

Nama :

1. Abdillah Ibnu Mubarak / 1707051014
2. Muhammad Bella Buay Nunyai / 1707051018
3. Ramadhan Kurniawan Sanggam / 1707051030

Mata Kuliah Keamanan Komputer

TUGAS PENDAHULUAN

1. Sebutkan langkah dasar yang biasa dipakai untuk melakukan proses hacking !
 1. Reconnaissance dan footprinting
 2. Scanning dan probing
 3. Enumerasi
 4. Mendapatkan akses
 5. Eskalasi
 6. Membuat backdoor dan menyembunyikan jejak

2. Sebutkan cara penggunaan netstat dan option-option yang dipakai serta arti option tersebut ?

Jawab:

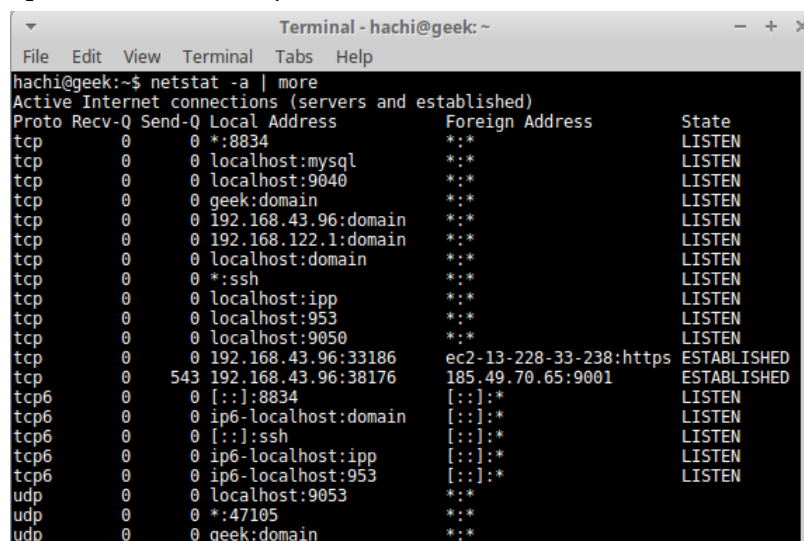
Kita download dahulu paket netstat nya dengan perintah ***apt-get install net-tools***

Lalu kita bisa option di netstat dengan perintah ***netstat -help***

Ada beberapa option di netstat yang sering digunakan

- Mendengarkan semua koneksi melalui port UDP dan TCP

Dengan perintah ***netstat -a | more***



```
hachi@geek:~$ netstat -a | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:8834                  *:*                     LISTEN
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 localhost:9040          *:*                     LISTEN
tcp        0      0 geek:domain             *:*                     LISTEN
tcp        0      0 192.168.43.96:domain    *:*                     LISTEN
tcp        0      0 192.168.122.1:domain    *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 localhost:953           *:*                     LISTEN
tcp        0      0 localhost:9050          *:*                     LISTEN
tcp        0      0 192.168.43.96:33186     ec2-13-228-33-238:https ESTABLISHED
tcp        0      0 543 192.168.43.96:38176  185.49.70.65:9001     ESTABLISHED
tcp6       0      0 [::]:8834               [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:domain    [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                 [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:953       [::]:*                  LISTEN
udp        0      0 localhost:9053          *:*                     LISTEN
udp        0      0 *:47105                 *:*                     LISTEN
udp        0      0 geek:domain             *:*                     LISTEN
```

- Mendengarkan semua koneksi melalui port TCP
Dengan perintah ***netstat -at***

```

Terminal - hachi@geek: ~
File Edit View Terminal Tabs Help
hachi@geek:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:8834                  *:*                     LISTEN
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 localhost:9040          *:*                     LISTEN
tcp        0      0 geek:domain             *:*                     LISTEN
tcp        0      0 192.168.43.96:domain    *:*                     LISTEN
tcp        0      0 192.168.122.1:domain    *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 localhost:953           *:*                     LISTEN
tcp        0      0 localhost:9050          *:*                     LISTEN
tcp        0      0 192.168.43.96:42478     ec2-52-36-130-57.:https TIME WAIT
tcp        0      0 192.168.43.96:56486     ec2-54-187-254-12:https TIME WAIT
tcp        0      0 192.168.43.96:41390     74.125.24.95:https     ESTABLISHED
tcp        0      0 192.168.43.96:36352     ec2-35-163-197-25:https TIME WAIT
tcp        0      0 192.168.43.96:36356     ec2-35-163-197-25:https TIME WAIT
tcp        0      0 192.168.43.96:44422     any-in-2678.1e100:https ESTABLISHED
tcp        0      0 192.168.43.96:40158     74.125.24.101:http     ESTABLISHED
tcp        0      0 192.168.43.96:59362     104.19.198.151:https   ESTABLISHED

```

- Menam

pilkan ip routing

Dengan perintah **netstat -r**

```

Terminal - hachi@geek: ~
File Edit View Terminal Tabs Help
hachi@geek:~$ netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default 192.168.43.1 0.0.0.0 UG 0 0 0 wlp2s0
link-local * 255.255.0.0 U 0 0 0 virbr0
192.168.43.0 * 255.255.255.0 U 0 0 0 wlp2s0
192.168.122.0 * 255.255.255.0 U 0 0 0 virbr0
hachi@geek:~$ 

```

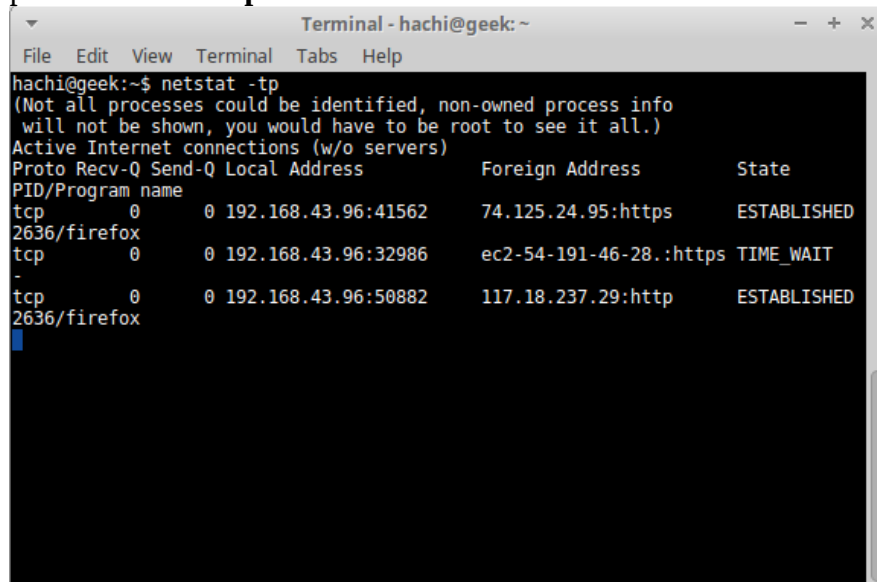
- Menampilkan IP v4 dan v6
Dengan perintah **netstat -g**

```

Terminal - hachi@geek: ~
File Edit View Terminal Tabs Help
hachi@geek:~$ netstat -g
IPv6/IPv4 Group Memberships
Interface RefCnt Group
-----
lo 1 all-systems.mcast.net
wlp2s0 1 224.0.0.251
wlp2s0 1 all-systems.mcast.net
virbr0 1 224.0.0.251
virbr0 1 all-systems.mcast.net
lo 1 ip6-allnodes
lo 1 ff01::1
wlp2s0 1 ff02::fb
wlp2s0 1 ff02::1:ff42:36bd
wlp2s0 1 ip6-allnodes
wlp2s0 1 ff01::1
virbr0 1 ip6-allnodes
virbr0 1 ff01::1
virbr0-nic 1 ip6-allnodes
virbr0-nic 1 ff01::1
hachi@geek:~$ 

```

- Menampilkan service dengan PID yang berjalan
Dengan perintah **netstat -tp**



```

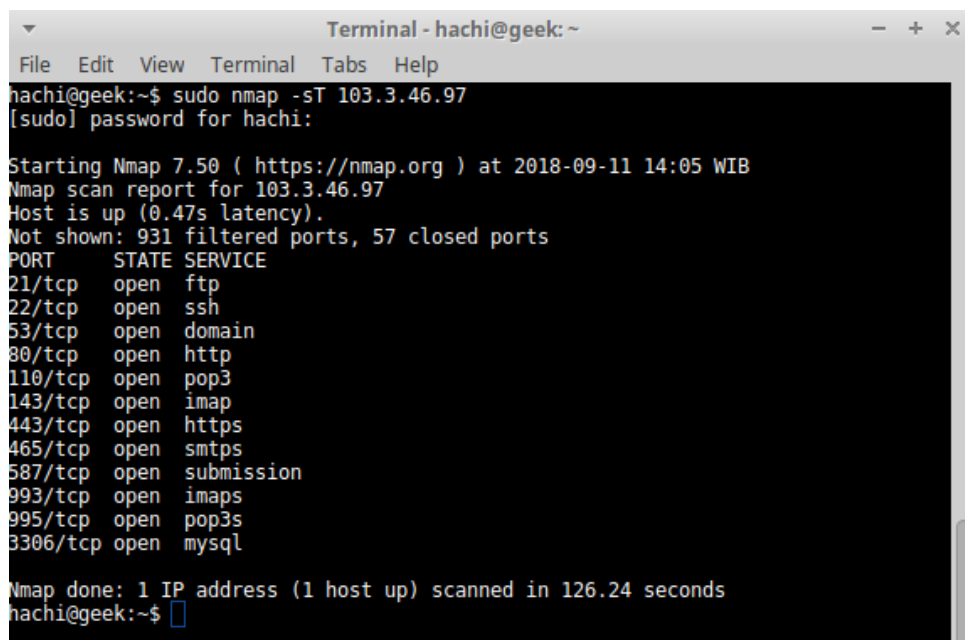
hachi@geek:~$ netstat -tp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 192.168.43.96:41562     74.125.24.95:https      ESTABLISHED
2636/firefox
tcp        0      0 192.168.43.96:32986     ec2-54-191-46-28.:https TIME_WAIT
-
tcp        0      0 192.168.43.96:50882     117.18.237.29:http      ESTABLISHED
2636/firefox

```

Mungkin menurut kami itu saja command menggunakan netstat yang berguna, kalau kalian ingin tau lebih lagi tentang command nya dengan perintah **man netstat**

3. Sebutkan cara pemakaian software nmap dengan menggunakan tipe scanning:

- TCP Connect scan
Dengan perintah **sudo nmap -sT 103.3.46.97** kita coba pada website fmipa.unila.ac.id untuk menscan port sasaran langsung



```

hachi@geek:~$ sudo nmap -sT 103.3.46.97
[sudo] password for hachi:

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 14:05 WIB
Nmap scan report for 103.3.46.97
Host is up (0.47s latency).
Not shown: 931 filtered ports, 57 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 126.24 seconds
hachi@geek:~$

```

- TCP SYN Scan
Dengan perintah **sudo nmap -sS 103.3.46.97** berguna untuk scan default pada nmap

```
Terminal - hachi@geek: ~
File Edit View Terminal Tabs Help
hachi@geek:~$ sudo nmap -sS 103.3.46.97

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 14:18 WIB
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 103.3.46.97, 16) => Network is unreachable
Offending packet: TCP 192.168.100.17:58206 > 103.3.46.97:6547 S ttl=48 id=55108 iplen=44 seq=1580683970 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 103.3.46.97, 16) => Network is unreachable
Offending packet: TCP 192.168.100.17:58207 > 103.3.46.97:6547 S ttl=39 id=44793 iplen=44 seq=1580618435 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 103.3.46.97, 16) => Network is unreachable
Offending packet: TCP 192.168.100.17:58208 > 103.3.46.97:6547 S ttl=56 id=33847 iplen=44 seq=1580552896 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 103.3.46.97, 16) => Network is unreachable
Offending packet: TCP 192.168.100.17:58202 > 103.3.46.97:7100 S ttl=48 id=50782 iplen=44 seq=1580421830 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 103.3.46.97, 16) => Network is unreachable
Offending packet: TCP 192.168.100.17:58203 > 103.3.46.97:7100 S ttl=52 id=22556 iplen=44 seq=1580356295 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 103.3.46.97, 16) => Network is unreachable
```

- TCP FIN scan

Dengan perintah **sudo nmap -sF 103.3.46.97** berguna untuk mengirim kan paket FIN ke port sasaran

```
Terminal - hachi@geek: ~
File Edit View Terminal Tabs Help
21/tcp open ftp
22/tcp open ssh
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
3306/tcp open mysql

Nmap done: 1 IP address (1 host up) scanned in 534.48 seconds
hachi@geek:~$ sudo nmap -sF 103.3.46.97
[sudo] password for hachi:

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 14:36 WIB
Nmap scan report for 103.3.46.97
Host is up (0.026s latency).
All 1000 scanned ports on 103.3.46.97 are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 28.78 seconds
hachi@geek:~$
```

- TCP Xmas Tree scan

Dengan perintah **sudo nmap -sX 103.3.46.97** berguna untuk mengirim paket FIN, URG dan PUSH ke paket sasaran

```
hachi@geek:~$ sudo nmap -sX 103.3.46.97

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 14:39 WIB
Nmap scan report for 103.3.46.97
Host is up (0.010s latency).
All 1000 scanned ports on 103.3.46.97 are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 29.18 seconds
hachi@geek:~$
```

- TCP null scan

Dengan perintah **sudo nmap -sN 103.3.46.97** berguna untuk membuat off semua flag dan mengirim balik paket RST untuk semua port yang tertutup

```
hachi@geek:~$ sudo nmap -sN 103.3.46.97

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 14:43 WIB
Nmap scan report for 103.3.46.97
Host is up (0.0088s latency).
All 1000 scanned ports on 103.3.46.97 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 29.38 seconds
hachi@geek:~$
```

- TCP ACK scan

Dengan perintah **sudo nmap -sA 103.3.46.97** berguna untuk memetakan set aturan firewall

```
hachi@geek:~$ sudo nmap -sA 103.3.46.97

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 14:45 WIB
Nmap scan report for 103.3.46.97
Host is up (0.015s latency).
Not shown: 999 filtered ports
PORT      STATE      SERVICE
80/tcp    unfiltered http

Nmap done: 1 IP address (1 host up) scanned in 27.54 seconds
hachi@geek:~$
```

- TCP Windows scan

Dengan perintah **sudo nmap -s**

- TCP RPC scan

Dengan perintah Teknik ini spesifik hanya pada system UNIX dan digunakan untuk mendeteksi dan mengidentifikasi port RPC (Remote Procedure Call) dan program serta normor versi yang berhubungan dengannya.

- UDP scan

Dengan perintah **sudo nmap -sU 103.3.46.97** berguna untuk mengirimkan paket UDP ke port sasaran

```
hachi@geek:~$ sudo nmap -sU 103.3.46.97

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 15:17 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 53.25 seconds
hachi@geek:~$
```

- OS fingerprinting

Dengan perintah **sudo nmap -O 103.3.46.97** berguna untuk mendeteksi OS yang digunakan

```
hachi@geek:~$ sudo nmap -O 103.3.46.97

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 15:20 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 54.10 seconds
hachi@geek:~$
```

4. Bagaimana cara mematikan dan menghidupkan service yang ada

Jawab:

Untuk mematikan service pada nessus digunakan perintah **/etc/init.d/nessusd stop**

Untuk menghidupkan service pada nessus digunakan perintah **/etc/init.d/nessusd start**

5. Sebutkan cara pemakaian software nessus untuk melihat kelemahan sistem jaringan kita !

Jawab:

Pastikan download nessus terlebih dahulu

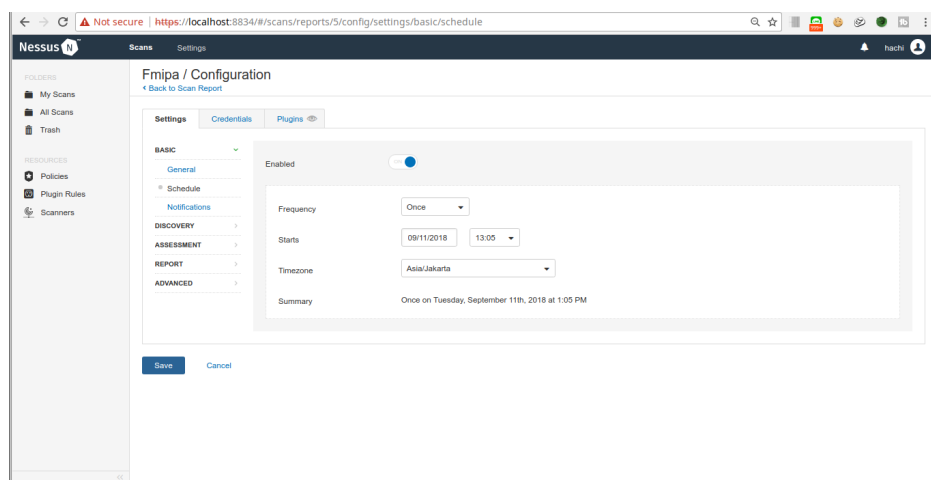
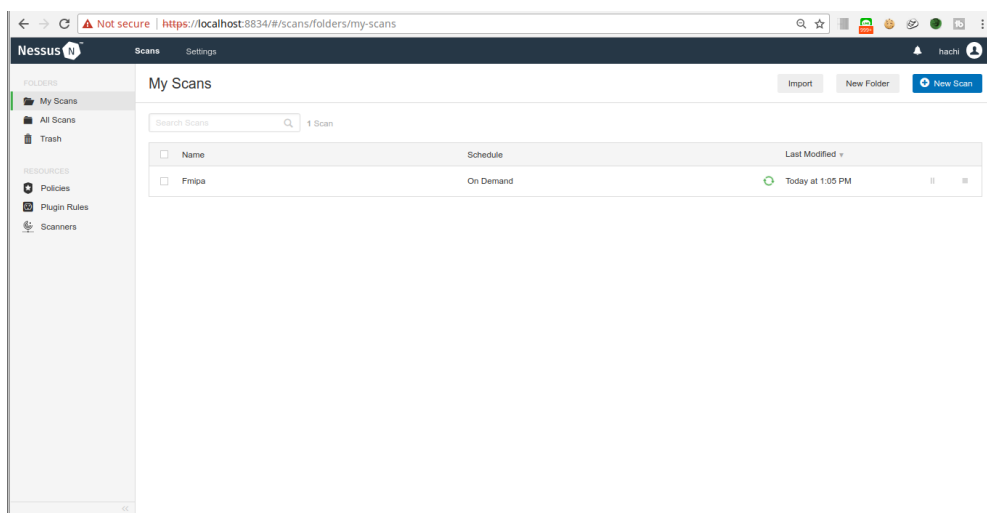
Apabila sudah terinstall pastikan running di pc kita nessus nya dengan perintah **/etc/init.d/nessusd start**

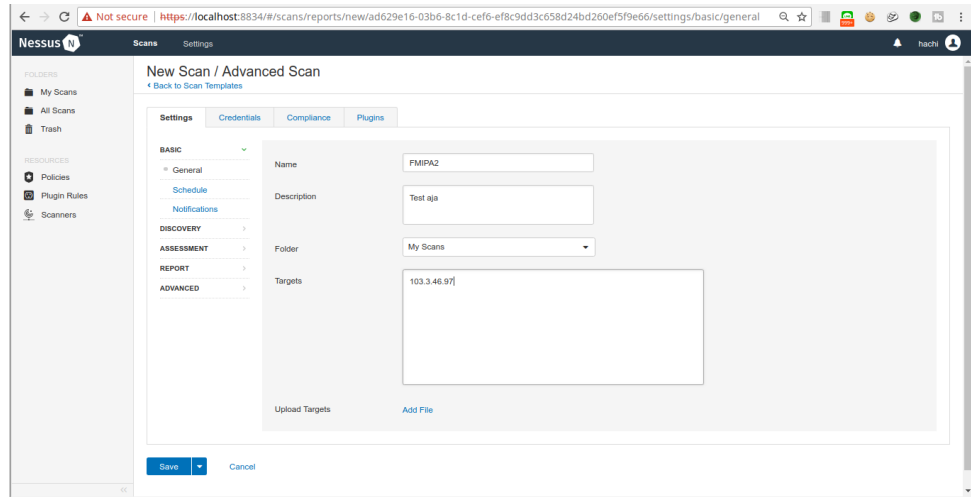
Lalu jalankan nessus agar bisa berjalan di browser recommend make google chrome

Kita mencari tahu dahulu ip website fmipa.unila.ac.id didapatkan ip nya

Buka nessus nya diweb <https://localhost:8834/>

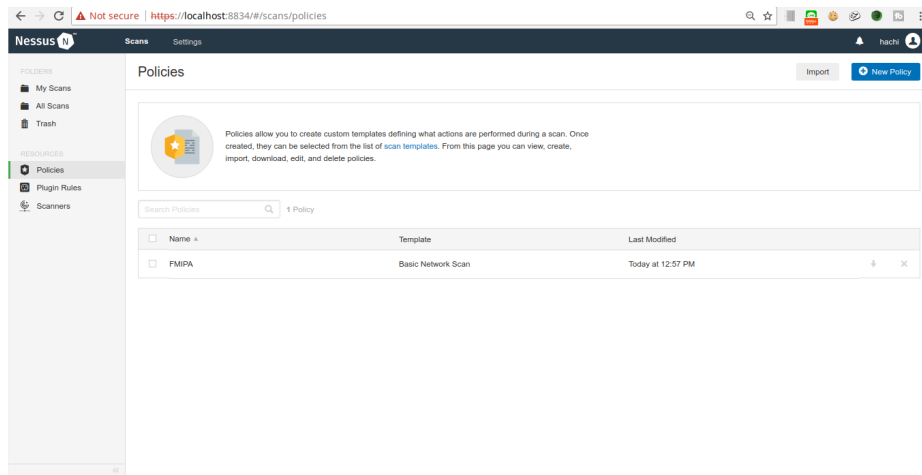
Kalau sudah new scan sesuaikan dengan ip kita dan apa yang mau discan, kita buat contoh nya FMIPA



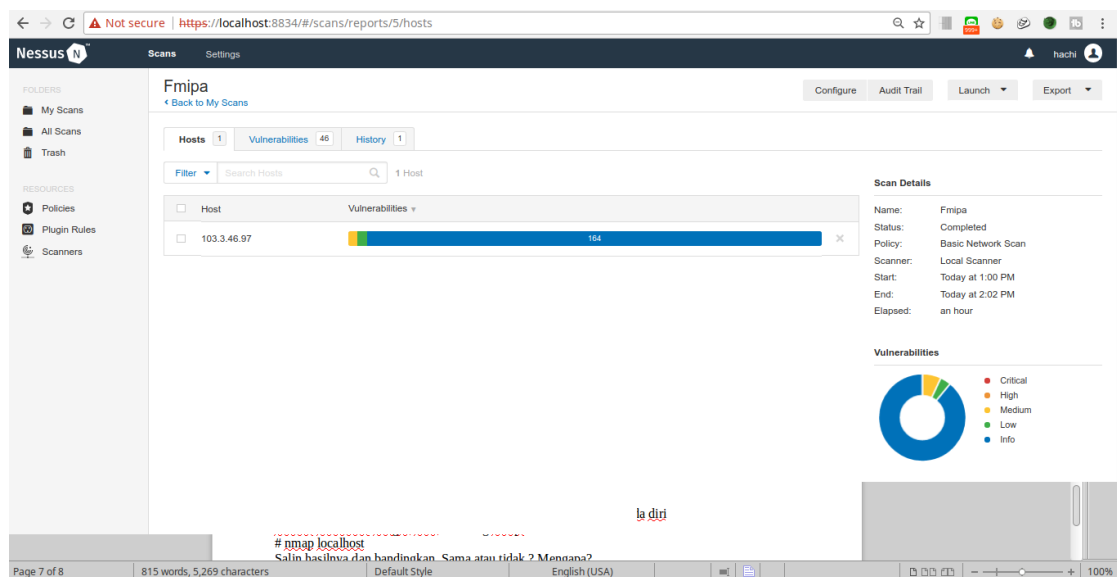


Setting schedule waktu nya

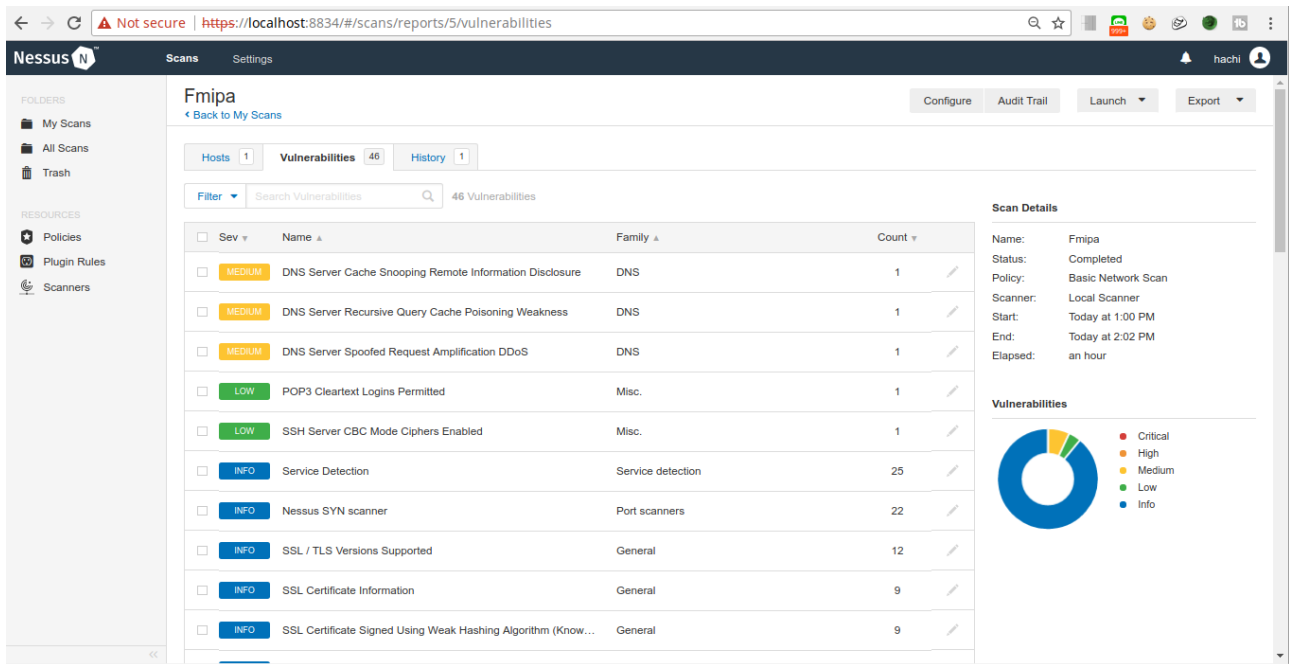
Terus add policies pilih basic network scan



Kita tunggu hingga proses selesai



Kita dapatkan website tersebut mempunyai vuln atau kelemahan pada beberapa bagian



6. Lakukan analisa paket nessus dan bandingkan dengan yang dilakukan nmap.

Jawab:

Kita bisa lihat di nessus terdapat vuln dibeberapa bagian kita bisa tahu juga vuln nya dibagian apa, sedangkan di nmap hanya mengecek koneksi nya saja tidak secara spesifik seperti di nessus

PERCOBAAN

1. Melihat status service yang aktif di local komputer

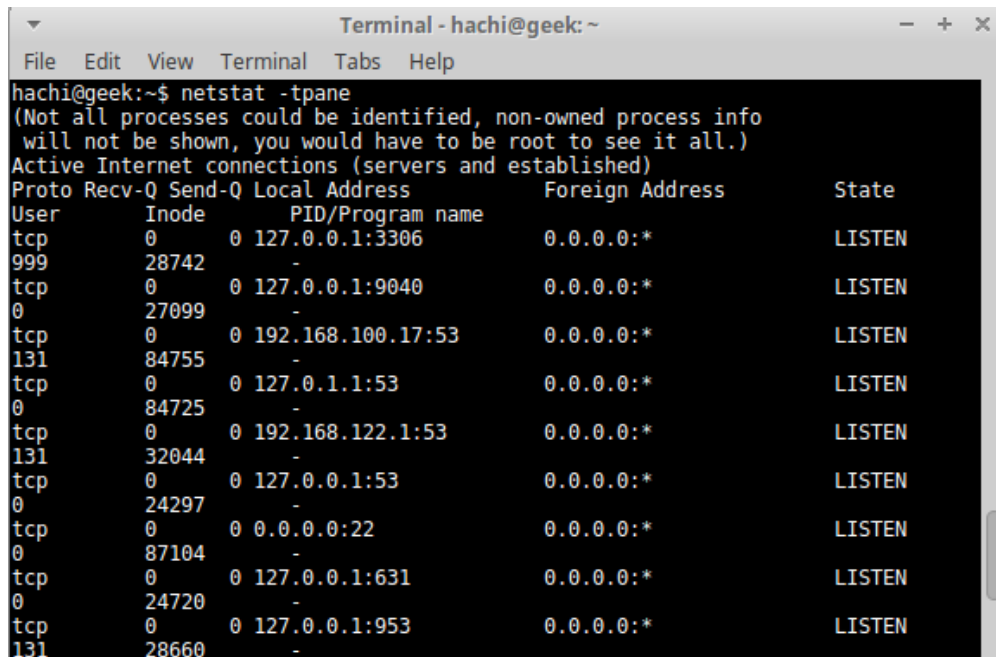
Gunakan command `netstat -tpane` dan `netstat -tupane` bandingkan hasilnya .

Lakukan beberapa option `netstat` untuk mengetahui hanya tcp atau udp saja yang terlihat

Lakukan pula options – options yang lain

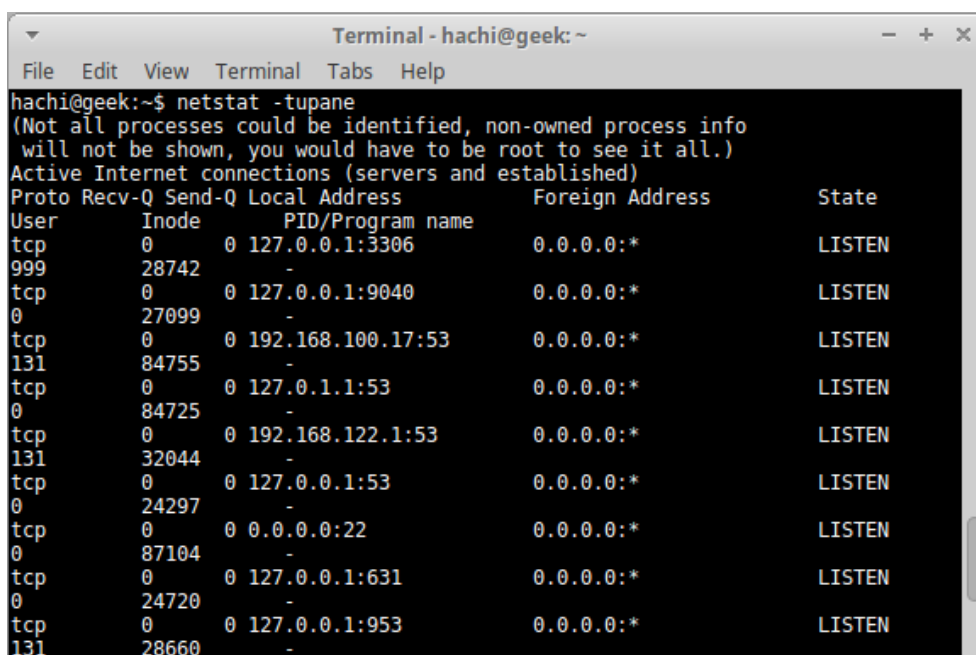
Jawab:

Menggunakan perintah **`netstat -tpane`** berguna mengecek berdasarkan protocol tcp



```
hachi@geek:~$ netstat -tpane
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
User      Inode  PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
999       28742  -
tcp        0      0 127.0.0.1:9040          0.0.0.0:*               LISTEN
0         27099  -
tcp        0      0 192.168.100.17:53       0.0.0.0:*               LISTEN
131       84755  -
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
0         84725  -
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN
131       32044  -
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
0         24297  -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
0         87104  -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
0         24720  -
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
131       28660  -
```

Menggunakan perintah **`netstat -tupane`** berguna mengecek berdasarkan protocol tcp dan udp



```
hachi@geek:~$ netstat -tupane
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
User      Inode  PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
999       28742  -
tcp        0      0 127.0.0.1:9040          0.0.0.0:*               LISTEN
0         27099  -
tcp        0      0 192.168.100.17:53       0.0.0.0:*               LISTEN
131       84755  -
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
0         84725  -
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN
131       32044  -
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
0         24297  -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
0         87104  -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
0         24720  -
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
131       28660  -
```

Kita juga bisa menggunakan parameter **`netstat -at`** untuk mengecek berdasarkan protokol TCP

Kita juga bisa menggunakan parameter **netstat -au** untuk mengecek berdasarkan protokol UDP

2. Pastikan nmap dan wireshark terinstal pada komputer anda, jika belum lakukan instalasi

- Jalankan wireshark pada komputer target lalu lakukan command nmap pada komputer sumber, analisa hasil dan perilaku data yang dikirim ke jaringan oleh masing- masing nmap.

- Pastikan koneksi terhubung dengan baik antara komputer sumber dan target, gunakan perintah ping.

Misal beberapa perintah nmap berikut

`nmap -sT -v Nama_IP_Target`

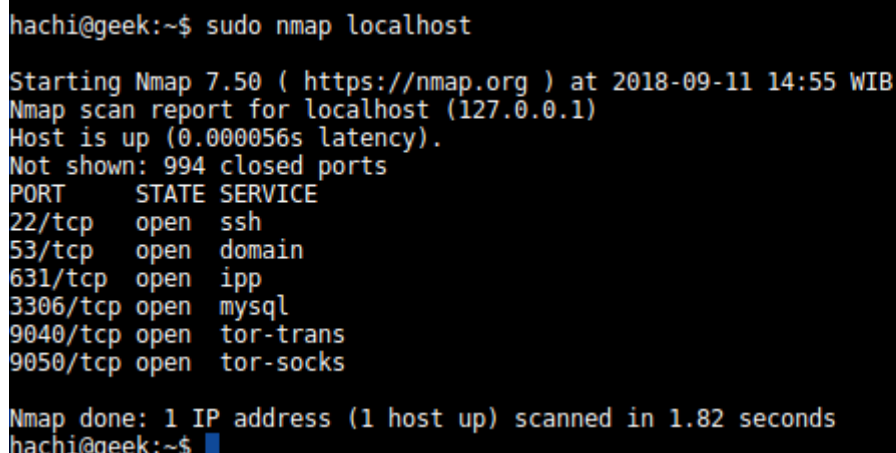
`nmap -sS -v Nama_IP_Target nmap -O -v Nama_IP_Target`

`nmap -sF -v Nama_IP_Target`

- Mintalah pada komputer yg discan untuk menjalankan scanning pada diri sendiri. Cocokkan dengan hasil scanning nmap.

nmap localhost

Salin hasilnya dan bandingkan. Sama atau tidak ? Mengapa?



```
hachi@geek:~$ sudo nmap localhost

Starting Nmap 7.50 ( https://nmap.org ) at 2018-09-11 14:55 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000056s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
631/tcp    open  ipp
3306/tcp   open  mysql
9040/tcp   open  tor-trans
9050/tcp   open  tor-socks

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
hachi@geek:~$
```

- Jalankan nmap dengan beberapa option yang berdasarkan tipe-tipe scanning yang ada (FIN scan, TCP Xmas Tree scan, TCP null scan, TCP ACK scan, TCP Windows scan, TCP RPC scan, UDP scan, OS fingerprinting) dan analisa perilaku data yang dikirim dengan wireshark

The image shows a Wireshark packet capture window titled '*wlp2s0'. The 'Filter' bar is set to 'icmp'. The packet list shows various protocols including DNS, ICMPv6, MDNS, NTP, and SSDP. The packet details pane shows the selected packet (No. 103) as an Internet Protocol Version 4 packet from 192.168.2.101 to 103.19.177.177. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1694	279.173657597	192.168.2.101	202.12.31.53	DNS	87	Standard query 0x31e0 A www.google.co.id OPT
1695	279.970813841	192.168.2.101	192.26.92.30	DNS	86	Standard query 0x90ad A ssl.gstatic.com OPT
1696	279.974014928	192.168.2.101	103.19.177.177	DNS	76	Standard query 0xcd10 A www.google.co.id
1697	280.170488442	192.168.2.101	8.8.8.8	DNS	75	Standard query 0x67cf A ssl.gstatic.com
1698	280.171133577	192.168.2.101	8.8.8.8	DNS	76	Standard query 0x2ea8 A www.google.co.id
638	91.572405778	fe80::d8c4:74d2:b8e...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
639	91.586351129	fe80::d8c4:74d2:b8e...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
640	91.588384132	fe80::d8c4:74d2:b8e...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
641	91.593788975	fe80::d8c4:74d2:b8e...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
644	91.984831046	fe80::d8c4:74d2:b8e...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
915	140.956315283	fe80::9203:25ff:fe6...	ff02::1:ff3a:975c	ICMPv6	86	Neighbor Solicitation for fe80::982c:dddc:2c3a:975c from 90:03:25:64:b3:74
1464	231.480134706	fe80::4213:a5b1:f1d...	ff02::fb	MDNS	203	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question PTR _ipps...
1466	232.847550101	192.168.2.101	224.0.0.251	MDNS	183	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question PTR _ipps...
452	66.425407772	192.168.2.101	91.189.94.4	NTP	90	NTP Version 4, client
688	98.675143776	192.168.2.101	91.189.94.4	NTP	90	NTP Version 4, client
1027	162.925251677	192.168.2.101	91.189.94.4	NTP	90	NTP Version 4, client
1093	173.230346121	192.168.2.101	91.189.89.198	NTP	90	NTP Version 4, client
1155	183.425516481	192.168.2.101	91.189.91.157	NTP	90	NTP Version 4, client
1228	193.675523834	192.168.2.101	91.189.89.199	NTP	90	NTP Version 4, client
32	5.219192891	192.168.2.200	239.255.255.250	SSDP	308	NOTIFY * HTTP/1.1
33	5.225595203	192.168.2.200	239.255.255.250	SSDP	308	NOTIFY * HTTP/1.1
34	5.279477630	192.168.2.200	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
35	5.282088620	192.168.2.200	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1

Bisa dilihat dari file wireshark tersebut bahwa pada protocol icmp ada proses pengiriman data

3. Pastikan nessus terinstal pada komputer anda, lakukan instalasi.

Berikut beberapa langkah instalasi nessus

Kita bisa menggunakan perintah **sudo apt-get install nessus**

Lalu jalan kan nessus dengan perintah **/etc/init.d/nessusd start**

LAPORAN RESMI

1. Berikan kesimpulan hasil praktikum yang anda lakukan.

Jawab:

Menurut kesimpulan dari kami yaitu, jika kita menggunakan nmap kita hanya menscan berdasarkan parameter yang berikan antara lain port yang terbuka, terus OS yang digunakan, beda dengan nessus nessus menscan secara keseluruhan bisa mengetahui kelemahan dari ip tersebut secara spesifik walaupun berat saat digunakan dan lama saat proses scanning tapi ini rekomend tools yang digunakan untuk mencari tau kelemahan sistem yang kita gunakan

2. Sebutkan option atau bentuk-bentuk scanning yang bisa dilakukan nmap

Jawab:

- TCP Connect scan
Dengan perintah **sudo nmap -sT 103.3.46.97** kita coba pada website fmipa.unila.ac.id untuk menscan port sasaran langsung
- TCP SYN Scan
Dengan perintah **sudo nmap -sS 103.3.46.97** berguna untuk scan default pada nmap
- TCP FIN scan
Dengan perintah **sudo nmap -sF 103.3.46.97** berguna untuk mengirim kan paket FIN ke port sasaran
- TCP Xmas Tree scan
Dengan perintah **sudo nmap -sX 103.3.46.97** berguna untuk mengirim paket FIN, URG dan PUSH ke paket sasaran

- TCP null scan
Dengan perintah **sudo nmap -sN 103.3.46.97** berguna untuk membuat off semua flag dan mengirim balik paket RST untuk semua port yang tertutup
- TCP ACK scan
Dengan perintah **sudo nmap -sA 103.3.46.97** berguna untuk memetakan set aturan firewall
- TCP Windows scan
Dengan perintah **sudo nmap -s**
- TCP RPC scan
Dengan perintah Teknik ini spesifik hanya pada system UNIX dan digunakan untuk mendeteksi dan mengidentifikasi port RPC (Remote Procedure Call) dan program serta normor versi yang berhubungan dengannya.
- UDP scan
Dengan perintah **sudo nmap -sU 103.3.46.97** berguna untuk mengirimkan paket UDP ke port sasaran
- OS fingerprinting
Dengan perintah **sudo nmap -O 103.3.46.97** berguna untuk mendeteksi OS yang digunakan

3. Cari di internet beberap tools scanning yang ada dan bagaimana cara pemakaian dan hasilnya?

Jawab:

- Nikto cara penggunaan nya dengan perintah **nikto -h ipaddress**
- ZAP cara penggunaan nya hanya memasukan website dan ip address nya saja pada kolom search