PRAKTIKUM 3 – NETWORK SCANNING

Peralatan

Mesin attacker menggunakan Kali linux, sedangkan target menggunakan mesin metasploit 2 dengan distro debian. IP Attacker: 192.168.1.6 sedangkan target 192.168.1.11.

Praktikum 1 – NMAP

Melakukan scanning pertama dengan NMAP

Ketika pertama kali berada di network target, kita perlu tahu host apa saja yang aktif. Perintah yang dapat digunakan adalah:

```
nmap -sP 192.168.1.1-12
```

```
root@kali:/home/indi6oblin# nmap -sP 192.168.1.1-12
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-10 05:51 EDT
Nmap scan report for 192.168.1.1
Host is up (0.047s latency).
MAC Address: 24:D3:F2:EB:7D:32 (zte)
Nmap scan report for redminote5-redmi (192.168.1.2)
Host is up (0.082s latency).
MAC Address: 9C:2E:A1:13:81:50 (Xiaomi Communications)
Nmap scan report for 192.168.1.3
Host is up (0.0045s latency).
MAC Address: 28:3F:69:04:6E:83 (Sony Mobile Communications)
Nmap scan report for 192.168.1.5
Host is up (0.014s latency).
MAC Address: 58:5F:F6:09:33:21 (zte)
Nmap scan report for android-972df36960bbd50e (192.168.1.7)
Host is up (0.011s latency).
MAC Address: A0:E4:53:FA:A0:76 (Sony Mobile Communications)
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.0013s latency).
MAC Address: E8:2A:44:F1:69:05 (Liteon Technology)
Nmap scan report for 192.168.1.10
Host is up (0.10s latency).
MAC Address: 24:4B:03:36:8E:84 (Samsung Electronics)
Nmap scan report for 192.168.1.11
Host is up (0.0017s latency).
MAC Address: 08:00:27:C6:FC:63 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.1.6)
Host is up.
Nmap done: 12 IP addresses (9 hosts up) scanned in 6.85 seconds
root@kali:/home/indi6oblin#
```

Perintah diatas digunakan untuk mencari tahu host yang aktif dari range 1 hingga 12. Lalu kita mencoba mentargetkan host dengan IP 192.168.1.11.

Mendeteksi Port Terbuka

Dalam hal ini scanning nmap dengan menggunakan tipe Connect Scan (-sT) pada semua ip 192.168.1.11, dengan memberi perintah:

```
nmap -sT 192.168.1.11
```

```
root@kali:/home/indi6oblin# nmap -sT 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-10 05:30 EDT
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.0015s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C6:FC:63 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.99 seconds
root@kali:/home/indi6oblin#
```

Jelaskan hasil yang didapat dari perintah tersebut berdasarkan hasil yang tampil?

Deteksi Informasi OS

Nmap adalah pilihan yang cocok untuk banyak orang untuk mendeteksi remote OS. -A memberi tahu Nmap untuk menemukan dan menampilkan informasi OS tentang host yang kita uji.

```
nmap -A 192.168.1.11
```

```
root@kali:/home/indi6oblin# nmap -A 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-10 05:34 EDT
Nmap scan report for 192.168.1.11
Host is up (0.0012s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.6
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
```

```
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake,
LongColumnFlag, Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: 3Otx~3!J1S3A-]o6]Sf+
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2020-10-10T09:35:19+00:00; +1s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
```

```
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:10:38
|   source ident: nmap
|   source host: F6F5BCAE.78DED367.FFFA6D49.IP
|_  error: Closing Link: ypyhjngse[192.168.1.6] (Quit: ypyhjngse)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:C6:FC:63 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix,
Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2020-10-10T05:35:11-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
TRACEROUTE
HOP RTT     ADDRESS
1   1.22 ms 192.168.1.11
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.81 seconds
```

Analisis hasil yg didapat dari perintah tersebut? Informasi apa saja yang anda anggap berguna sebagai attacker?

Lakukan lagi dengan perintah yang berbeda,

```
nmap -O 192.168.1.11
```

```
root@kali:/home/indi6oblin# nmap -O 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-10 05:45 EDT
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00084s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C6:FC:63 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
root@kali:/home/indi6oblin#
```

Apa perbedaan dengan perintah sebelum nya? Jika kita ingin tahu secara cepat mengenai informasi OS, perintah mana yg kita gunakan?

Praktikum 2 – HPING

Melakukan scanning port pada host

Dengan menscan port taget host, kita dapat mengetahui port-port yang terbuka pada target host.. Berikut ini adalah contoh dari port scanning :

```
# hping3 192.168.1.11 -S -p ++20
```

```
root@kali:/home/indi6oblin# hping3 192.168.1.11 -S -p ++20
HPING 192.168.1.11 (eth0 192.168.1.11): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=20 flags=RA seq=0 win=0 rtt=4.4 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=21 flags=SA seq=1 win=5840 rtt=3.2 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=5840 rtt=2.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=23 flags=SA seq=3 win=5840 rtt=2.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=24 flags=RA seq=4 win=0 rtt=8.7 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=25 flags=SA seq=5 win=5840 rtt=7.9 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=26 flags=RA seq=6 win=0 rtt=7.7 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=27 flags=RA seq=7 win=0 rtt=7.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=28 flags=RA seq=8 win=0 rtt=6.0 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=29 flags=RA seq=9 win=0 rtt=5.8 ms
len=46 ip=192.168.1.11 ttl=64 DF id=0 sport=30 flags=RA seq=10 win=0 rtt=6.0 ms
^C
--- 192.168.1.11 hping statistic ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max = 2.0/5.5/8.7 ms
root@kali:/home/indi6oblin#
```

Analisi hasil diatas, apa informasi yang bisa kita dapatkan?

Lalu lakukan kembali dengan perintah berikut,

```
# hping3 –scan 1-100 -S 192.168.1.11
```

```
root@kali:/home/indi6oblin# hping3 -a 10.10.10.10 -S 192.168.1.11 -s 50 -p 80 -c 4
HPING 192.168.1.11 (eth0 192.168.1.11): S set, 40 headers + 0 data bytes

--- 192.168.1.11 hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:/home/indi6oblin# hping3 --scan 1-100 -S 192.168.1.11
Scanning 192.168.1.11 (192.168.1.11), port 1-100
100 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp        : .S..A...  64     0  5840    46
   22 ssh        : .S..A...  64     0  5840    46
   23 telnet     : .S..A...  64     0  5840    46
   25 smtp       : .S..A...  64     0  5840    46
   53 domain     : .S..A...  64     0  5840    46
   80 http       : .S..A...  64     0  5840    46
All replies received. Done.
```

Apa perbedaan dengan perintah sebelumnya?

Lalu tambahkan option -V pada perintah sebelumnya,

```
root@kali:/home/indi6oblin# hping3 --scan 1-100 -S 192.168.1.11 -V
using eth0, addr: 192.168.1.6, MTU: 1500
Scanning 192.168.1.11 (192.168.1.11), port 1-100
100 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
    1 tcpmux     : ..R.A... 64     0     0    46
    2 nbp        : ..R.A... 64     0     0    46
    3            : ..R.A... 64     0     0    46
    4 echo       : ..R.A... 64     0     0    46
    5            : ..R.A... 64     0     0    46
    6 zip        : ..R.A... 64     0     0    46
    7 echo       : ..R.A... 64     0     0    46
    8            : ..R.A... 64     0     0    46
    9 discard    : ..R.A... 64     0     0    46
   10            : ..R.A... 64     0     0    46
   11 systat     : ..R.A... 64     0     0    46
   12            : ..R.A... 64     0     0    46
   13 daytime    : ..R.A... 64     0     0    46
   14            : ..R.A... 64     0     0    46
   15 netstat    : ..R.A... 64     0     0    46
   16            : ..R.A... 64     0     0    46
   17 qotd       : ..R.A... 64     0     0    46
   18            : ..R.A... 64     0     0    46
   19 chargen    : ..R.A... 64     0     0    46
   20 ftp-data   : ..R.A... 64     0     0    46
   21 ftp        : .S..A... 64     0  5840    46
   22 ssh        : .S..A... 64     0  5840    46
   23 telnet     : .S..A... 64     0  5840    46
   24            : ..R.A... 64     0     0    46
   25 smtp       : .S..A... 64     0  5840    46
```

Apa fungsi dari penambahan -V tersebut?

Inverse mapping

Inverse mapping dilakukan untuk mengetahui host yang aktif atau tidak. Berikut ini adalah contoh dari inverse mapping.

```
# hping3 192.168.1.11 -R
```

```
root@kali:/home/indi6oblin# hping3 192.168.1.11 -R
HPING 192.168.1.11 (eth0 192.168.1.11): R set, 40 headers + 0 data bytes
^C
```

Apa maksud dari hasil diatas?