



Network Scanning con Nmap

Traccia:

Nell'esercizio di oggi pomeriggio vedremo da vicino nmap e i suoi comandi. Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchina sorgente con Wireshark.

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchina. E' molto importante in questa fase essere organizzati e strutturati. Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report Excel / altro che riporti in maniera chiara:

- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

L'esercizio di oggi richiede di eseguire un scanning su una macchina bersaglio e trovare eventuali vulnerabilità. In seguito sono riportati tutti i procedimenti e comandi che ci serviranno per poter effettuare lo scan.

Per prima cosa occorre sapere quali sono gli indirizzi IP di entrambe le macchine per poter controllare tramite comando “ping” i vari pacchetti in entrata ed in uscita.

The screenshot shows a terminal window with two panes. The left pane displays the output of the command `ifconfig`, listing network interfaces `eth0` and `lo`. The right pane displays the output of `ifconfig` from a host named `msfadmin@metasploitable`. Below these panes is another terminal window titled "kali@Kali ~" showing the results of a `ping` command to the IP address 192.168.128.2. The terminal shows 14 packets transmitted, 14 received, 0% packet loss, and a round-trip time of 13056ms.

```
(kali㉿Kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.128.3 netmask 255.255.255.0 broadcast 192.168.128.255
        inet6 fe80::b0aa:c1ff:fe34:7b47 prefixlen 64 scopeid 0x20<link>
            ether b2:aa:c1:34:7b:47 txqueuelen 1000 (Ethernet)
            RX packets 22 bytes 2508 (2.4 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 38 bytes 4940 (4.8 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr ba:54:3f:c1:0e:08
          inet addr:192.168.128.2  Bcast:192.168.128.255  Mask:255.255.255.0
          inet6 addr: fe00::b054:3fff:fe00:0/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:293 errors:0 dropped:0 overruns:0 frame:0
            TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:20760 (20.2 KB)  TX bytes:6034 (5.8 KB)
            Base address:0xc000 Memory:feb00000-febe0000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436  Metric:1
            RX packets:110 errors:0 dropped:0 overruns:0 frame:0
            TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:27753 (27.1 KB)  TX bytes:27753 (27.1 KB)

kali@Kali ~
File Azioni Modifica Visualizza Aiuto
zsh: corrupt history file /home/kali/.zsh_history
# ping 192.168.128.2
PING 192.168.128.2 (192.168.128.2) 56(84) bytes of data.
64 bytes from 192.168.128.2: icmp_seq=1 ttl=64 time=8.59 ms
64 bytes from 192.168.128.2: icmp_seq=2 ttl=64 time=2.02 ms
64 bytes from 192.168.128.2: icmp_seq=3 ttl=64 time=2.47 ms
64 bytes from 192.168.128.2: icmp_seq=4 ttl=64 time=3.54 ms
64 bytes from 192.168.128.2: icmp_seq=5 ttl=64 time=1.33 ms
64 bytes from 192.168.128.2: icmp_seq=6 ttl=64 time=1.68 ms
64 bytes from 192.168.128.2: icmp_seq=7 ttl=64 time=2.55 ms
64 bytes from 192.168.128.2: icmp_seq=8 ttl=64 time=2.61 ms
64 bytes from 192.168.128.2: icmp_seq=9 ttl=64 time=2.60 ms
64 bytes from 192.168.128.2: icmp_seq=10 ttl=64 time=1.75 ms
64 bytes from 192.168.128.2: icmp_seq=11 ttl=64 time=1.91 ms
64 bytes from 192.168.128.2: icmp_seq=12 ttl=64 time=1.87 ms
64 bytes from 192.168.128.2: icmp_seq=13 ttl=64 time=2.33 ms
64 bytes from 192.168.128.2: icmp_seq=14 ttl=64 time=1.86 ms
```
-- 192.168.128.2 ping statistics --
14 packets transmitted, 14 received, 0% packet loss, time 13056ms
rtt min/avg/max/mdev = 1.624/2.675/8.593/1.714 ms
```

Tramite comando “nmap -A -T4 (indirizzo IP), possiamo controllare tutte le porte presenti sulla macchina che vogliamo attaccare.

Con comandi “nmap (ip target) -sT oppure “nmap (ip target) -sS”, possiamo controllare più nello specifico quali porte tcp sono aperte, in modo da aver un quadro generale su dove poter agire per effettuare un possibile attacco.

```
(kali㉿Kali)-[~] $ nmap 192.168.128.2 -sT
Starting Nmap 7.93 (https://nmap.org) at 2022-11-10 16:23 CET
Nmap scan report for 192.168.128.2
Host is up (0.0002s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
1/tcp open ftp
2/tcp open ssh
3/tcp open telnet
5/tcp open smtp
9/tcp open domain
10/tcp open http
11/tcp open rpcbind
39/tcp open netbios-ssn
45/tcp open microsoft-ds
12/tcp open exec
13/tcp open login
14/tcp open shell
109/tcp open rmiregistry
524/tcp open ingreslock
2049/tcp open nfs
121/tcp open ccproxy-ftp
306/tcp open mysql
432/tcp open postgresql
900/tcp open vnc
2000/tcp open X11
667/tcp open irc
2009/tcp open ajp13
180/tcp open unknown
map done: 1 IP address (1 host up) scanned in 13.11 seconds

└─(root㉿Kali)-[/home/kali]
nmap 192.168.128.2 -sS
Starting Nmap 7.93 (https://nmap.org) at 2022-11-10 16:26 CET
Nmap scan report for 192.168.128.2
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
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: 0A:5E:12:E1:0E:08 (Unknown)

MAC Address: 0A:5E:12:E1:0E:08 (Unknown)
```

E per finire, tramite l'utilizzo di Wireshark, possiamo andare ad analizzare alcuni dei pacchetti e porte che sono vulnerabili, e quindi potenzialmente soggette ad attacchi.





