

Esercizio nmap/Wireshark

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:

- Host discovery (sulla propria rete LAN)
- 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 macchine sorgente (Kali) 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 macchine. 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 (tabella su word ad esempio) 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)

-Host discovery rete Lan

Una volta settate le machine (linux/metasploit) con rispettivi ip:192.168.50.100/182.168.50.101, possiamo avviare nmap e inserendo il comando (nmap -sn 192.168.50./24), difatti una volta avviato tale comando nmap riconosce i 2 host.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sn 192.168.50.0/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 13:17 EDT  
Nmap scan report for 192.168.50.100  
Host is up (0.0013s latency).  
Nmap scan report for 192.168.50.101  
Host is up (0.0013s latency).  
Nmap done: 256 IP addresses (2 hosts up) scanned in 31.56 seconds  
  
(kali@kali)-[~]  
$
```

Scansione TCP sulle porte well-know

Una volta effettuato il seguente comando su nmap `-sT -p 0-1023 192.168.50.101` appaiono dei risultati riguardanti porte well-know.

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

-Scansione SYN sulle porte well-know

Come nel precedente scansione effettuiamo il seguente comando su nmap (`nmap -sS -p 0-1023 192.168.50.101`) sulle porte well-know SYN

```
(root@kali)-[~]  
# nmap -sS -p 0-1023 192.168.50.101  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 14:24 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00055s latency).  
Not shown: 1012 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  
MAC Address: 08:00:27:AD:D4:71 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 17.28 seconds
```

-Scansione con switch <<-A>> sulle porte well-know

Con il comando (nmap -A -p 0-1023 192.168.50.101)

```
(root@kali)-[~]
# nmap -A -p 0-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 14:35 EDT
Stats: 0:02:59 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 14:38 (0:00:15 remaining)
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 57.41% done; ETC: 14:38 (0:00:00 remaining)
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 14:38 (0:00:00 remaining)
Stats: 0:03:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.43% done; ETC: 14:38 (0:00:01 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.50.100
|   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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp open  telnet?
25/tcp open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
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)
| rpcinfo:
|   program version    port/proto  service
|   100000   2             111/tcp     rpcbind
|   100000   2             111/udp     rpcbind
|   100003   2,3,4         2049/tcp    nfs
|   100003   2,3,4         2049/udp    nfs

```

```

|   100005   1,2,3         52666/udp   mountd
|   100005   1,2,3         56607/tcp   mountd
|   100021   1,3,4         55251/tcp   nlockmgr
|   100021   1,3,4         60041/udp   nlockmgr
|   100024   1             33578/udp   status
|_  100024   1             39630/tcp   status
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?
513/tcp open  login?
514/tcp open  shell?
MAC Address: 08:00:27:AD:D4:71 (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h39m56s, deviation: 2h49m43s, median: -20m04s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable

```

```
| NetBIOS computer name:  
| Domain name: localdomain  
| FQDN: metasploitable.localdomain  
|_ System time: 2023-05-18T14:18:04-04:00  
| smb-security-mode:  
|   account_used: <blank>  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)  
|_ smb2-time: Protocol negotiation failed (SMB2)  
  
TRACEROUTE  
HOP RTT    ADDRESS  
1   1.11 ms 192.168.50.101  
  
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 327.79 seconds  
  
(root@kali)-[~]  
#
```

Evidenziare la differenza tra la scansione tra TCP/SYN

Utilizzando wireshark un software che intercetta il traffico dati in questo caso della macchina (virtuale) linux, avviamo una connessione TCP creando una comunicazione tra server ed client.

Creando così il three way handshake che scambia la sincronizzazione di scambio e riconoscimento dei pacchetti.

Inserendo il seguente filtro `tcp.port == || upd.port`

==80) come da foto si stabilizza la comunicazione tra SYN,SYN/ACK e ACK

334	5.227484832	192.168.50.100	192.168.50.101	TCP	74 42826 → 80	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2863315334 TSecr=0 WS=128
343	5.235625807	192.168.50.101	192.168.50.100	TCP	74 80 → 42826	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=116624 TSecr=28
344	5.236108439	192.168.50.100	192.168.50.101	TCP	66 42826 → 80	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2863315343 TSecr=116624

Diversamente dal TCP la scansione SYN non porta al termine il three way handshake e di conseguenza avviene lo scambio con SYN,SYN/ACK ed RST non porta la termine la connessione con RST

875	23.410261246	192.168.50.100	192.168.50.101	TCP	74 57082 → 80	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2863333517 TSecr=0 WS=128
877	23.410712221	192.168.50.101	192.168.50.100	TCP	74 80 → 57082	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=118442 TSecr=28
602	6.493095045	192.168.50.100	192.168.50.101	TCP	66 42834 → 80	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2863316600 TSecr=116750

Scansione TCP

Fonte dello scan:192.168.50.100

Target dello scan:192.168.50.101

Tipo di scan: -sT -p 0-1023 192.168.50.101

Risultati ottenuti: 12 risultati

Scansione SYN

Fonte dello scan:192.168.50.100

Target dello scan:192.168.50.101

Tipo di scan: -sS -p 0-1023 192.168.50.101

Risultati ottenuti:12 risultati

Scansione con switch < ← A >>

Fonte dello scan: 192.168.50.100

Target dello scan: 192.168.50.101

Tipo di scan: -A -p 0-1023 192.168.50.101

Risultati ottenuti: 12 risultati

