

Esercitazione W9D1 - Pratica 2

Nmap scan

Fabio Benevento - 20/12/2023

Traccia

Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchina 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 macchine sorgente con Wireshark.

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)

Implementazione

Di seguito sono illustrati nel dettaglio i risultati della scansione nei 3 casi previsti

Scansione TCP sulle porte well-known

Per eseguire la scansione delle well-know port ho eseguito il comando `nmap -sT -p 0 1024 192.168.50.101` al fine di reperire i servizi TCP presenti sulla macchina Metasploitable di indirizzo 192.168.50.101 nel range 0-1024 (well-known port).

```
$ nmap -sT -p 0-1023 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 04:49 EST
Nmap scan report for 192.168.50.101
Host is up (0.025s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

Di seguito è mostrato il report della scansione in forma tabellare.

Fonte	Nmap da Kali Linux - IP: 192.168.50.100
Target	Metasploitable - IP: 192.168.50.101
Tipo di scan	Nmap -sT -p 0 1024 (well-known port)
Numero servizi trovati	12
Porta	Servizio
21	ftp
22	ssh
23	telnet
25	smtp
53	domain
80	http
111	rpc-bind
139	netbios-ssn
445	microsoft-ds
512	exec
513	login
514	shell

Nella seguente figura è mostrato un estratto di cattura preso mediante Wireshark durante l'esecuzione del comando Nmap.

22	13.014783144	192.168.50.100	192.168.50.101	TCP	74	39586 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3715628778 TSecr=0 WS=128
23	13.015204962	192.168.50.100	192.168.50.101	TCP	74	53632 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3715628779 TSecr=0 WS=128
24	13.015943118	192.168.50.101	192.168.50.100	TCP	74	139 → 39586 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1566670 TSecr=3715628778 WS=64
25	13.015943245	192.168.50.101	192.168.50.100	TCP	74	21 → 53632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1566670 TSecr=3715628779 WS=64
26	13.015963737	192.168.50.100	192.168.50.101	TCP	66	39586 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3715628780 TSecr=1566670
27	13.016529098	192.168.50.100	192.168.50.101	TCP	66	53632 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3715628780 TSecr=1566670
28	13.017036496	192.168.50.100	192.168.50.101	TCP	74	43456 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3715628781 TSecr=0 WS=128
29	13.017499647	192.168.50.100	192.168.50.101	TCP	74	59918 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3715628781 TSecr=0 WS=128
30	13.017855357	192.168.50.101	192.168.50.100	TCP	60	113 → 43456 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	13.017855445	192.168.50.101	192.168.50.100	TCP	60	993 → 59918 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	13.018648876	192.168.50.100	192.168.50.101	TCP	74	53618 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3715628782 TSecr=0 WS=128
33	13.019143319	192.168.50.100	192.168.50.101	TCP	74	38472 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3715628783 TSecr=0 WS=128

Come è possibile notare il client, in questo caso Nmap, tenta di contattare una serie di porte sulla macchina target (Metasploitable - IP: 192.168.50.101) tentando di instaurare una connessione TCP mediante l'invio di un pacchetto SYN. Una di queste è la porta 21 (riga 23, SYN) al quale il client, essendo una porta aperta, risponde con un pacchetto SYN-ACK (riga 25). Nmap completa il three-way handshake per l'apertura del canale con l'invio di un pacchetto ACK (riga 27). Nel caso invece la porta non è aperta come per esempio la porta 113 (riga 28), il server risponde con un pacchetto di tipo RST-ACK (riga 30), concludendo l'handshake.

Scansione SYN sulle porte well-known

Per eseguire la scansione delle well-know port di tipo SYN ho in questo caso eseguito il comando `nmap -sS -p 0 1024 192.168.50.101`. Questo tipo di scansione è più leggera, veloce e meno invasiva in quanto Nmap non completa l'handshake con un ACK stabilendo una connessione ma chiude la richiesta con un pacchetto RST-ACK

```
└─$ sudo nmap -sS -p 0-1023 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 05:35 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
```

Il risultato della scansione è, com'è lecito aspettarsi analogo al precedente.

Di seguito è mostrato il report della scansione in forma tabellare.

Fonte	Nmap da Kali Linux - IP: 192.168.50.100
Target	Metasploitable - IP: 192.168.50.101
Tipo di scan	Nmap -sS -p 0 1024 (well-known port)
Numero servizi trovati	12
Porta	Servizio
21	ftp
22	ssh
23	telnet
25	smtp
53	domain
80	http
111	rpc-bind
139	netbios-ssn
445	microsoft-ds
512	exec
513	login
514	shell

Nella seguente figura è mostrato un estratto di cattura preso mediante Wireshark durante l'esecuzione del comando Nmap.

44	13.134786110	192.168.50.100	192.168.50.101	TCP	58 45875 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45	13.135093725	192.168.50.100	192.168.50.101	TCP	58 45875 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	13.135357769	192.168.50.101	192.168.50.100	TCP	60 22 → 45875 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
47	13.135364690	192.168.50.100	192.168.50.101	TCP	54 45875 → 22 [RST] Seq=1 Win=0 Len=0
48	13.135756220	192.168.50.101	192.168.50.100	TCP	60 21 → 45875 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
49	13.135761793	192.168.50.100	192.168.50.101	TCP	54 45875 → 21 [RST] Seq=1 Win=0 Len=0

Come è possibile notare in questa modalità, in seguito all'invio di un pacchetto SYN verso una determinata porta aperta, ad esempio la porta 21 (riga 45 - SYN e relativa risposta

riga 48 - SYN-ACK), nmap non completa l'instauramento della connessione ed invia un pacchetto RST (riga 49) invece del pacchetto ACK inviato in precedenza.

Scansione con switch -A sulle porte well-known

L'opzione -A del comando switch permette di reperire informazioni di maggior dettaglio sui servizi individuati in seguito alla scansione, tra le quali:

- Rilevamento del sistema operativo
- Rilevamento della versione dei servizi
- Analisi di vulnerabilità sui servizi esposti

L'immagine in figura mostra il risultato dello scan con l'opzione -A applicata

```
[kali@kali] (~)
$ sudo nmap -sS -A -p 0-1023 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 05:47 EST
Nmap scan report for 192.168.50.101
Host is up (0.0045s 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 60:0f:cfe1:c0:5f:6a:74:d6:00:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:bl: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, ENHANCEDSTATUS
ME, DSN
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_title: Metasploitable2 - Linux
|_http_server_header: Apache/2.2.8 (Ubuntu) DAV/2
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 52915/udp mountd
|_  100005 1,2,3 55138/tcp mountd
|_  100021 1,3,4 40759/udp nlockmgr
|_  100021 1,3,4 52757/tcp nlockmgr
|_  100024 1 45629/tcp status
|_  100024 1 52882/udp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  smb          Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?       Netkit rshd
514/tcp   open  shell        Netkit rshd
MAC Address: 08:00:27:10:8A:34 (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: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-times: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|_  account_used: guest
|_  authentication_level: user
|_  challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -52d10h13m39s, deviation: 2h49m46s, median: -52d12h13m42s
|_smb-os-discovery:
|_  OS: Unix (Samba 3.0.20-Debian)
|_  Computer name: metasploitable
|_  NetBIOS computer name:
|_  Domain name: localdomain
|_  FQDN: metasploitable.localdomain
|_  System time: 2023-10-20T18:35:00-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT ADDRESS
1 4.47 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 93.52 seconds
```

Di seguito è mostrato il report della scansione in forma tabellare.

Fonte	Nmap da Kali Linux - IP: 192.168.50.100	
Target	Metasploitable - IP: 192.168.50.101 - Linux 2.6.X	
Tipo di scan	Nmap -sS -p 0 1024 (well-known port)	
N. serv. trovati	12	
Porta	Servizio	Versione
21	ftp	vsftpd 2.3.4
22	ssh	OpenSSH 4.7p1
23	telnet	Linux telnetd
25	smtp	Postfix smtpd
53	domain	ISC BIND 9.4.2
80	http	Apache httpd 2.2.8
111	rpc-bind	2
139	netbios-ssn	Samba smbd 3.X - 4.X
445	microsoft-ds	Samba smbd 3.0.20-Debian
512	exec	netkit-rsh rexecd
513	login	
514	shell	netkit-rshd

E' possibile scaricare per questa scansione un report dettagliato in formato html dal seguente indirizzo

[Report dettagliato HTML](#)