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

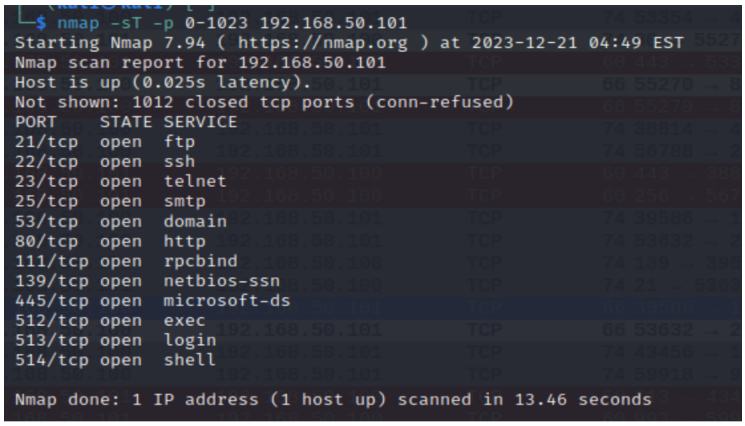
Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.
Per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report Excel / altro (tabella su word ad esempio) che riporti in maniera chiara:
- 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 previsi

Scansione TCP sulle porte well-known

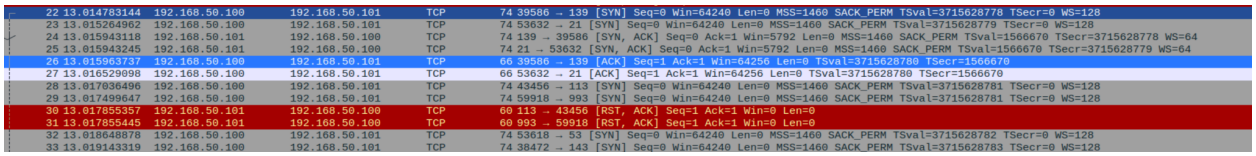
Per eseguire la scansione delle well-know port ho eseguito il comando `nmap -sT -p 0 1024 192.168.50.101` al fine di reperire i servizi TCP presenti sulla macchina Metaspoitable di indirizzo 192.168.50.101 nel range 0-1024 (well-known port).



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.



Come è possile 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-ANK (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

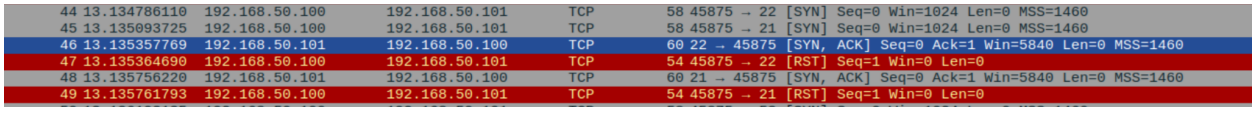
```
└─$ sudo nmap -sS -p 0-1023 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-21 05:35 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
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.



Come è possile 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

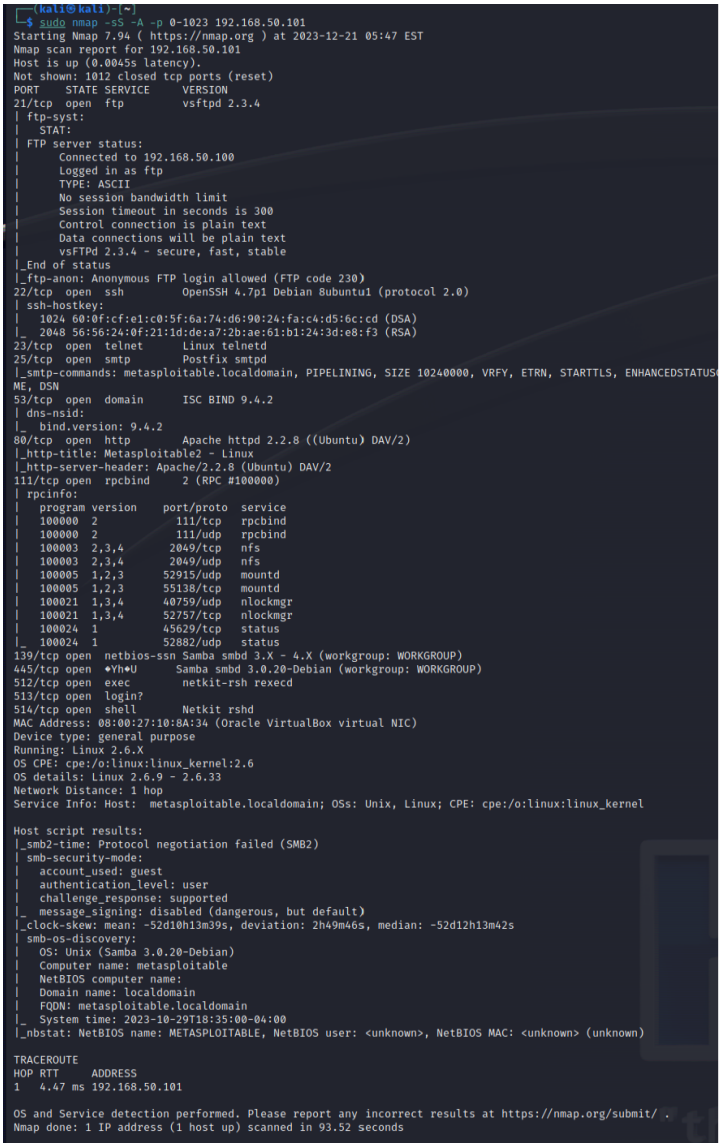
riga 48 - SYN-ACK), nmap non completa l'instauramento della connessione ed invia un pacchetto RST (riga 49) invece del pacchetto ACK inviato in precedenza.

Scansione con switch -A sulle porte well-known

L'opzione -A del comando switch premette di reperire informazioni di maggior dettaglio sui servizi individuati in seguito all 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



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