Floriana Feminò

10/11/2022

NMAP SCANNING

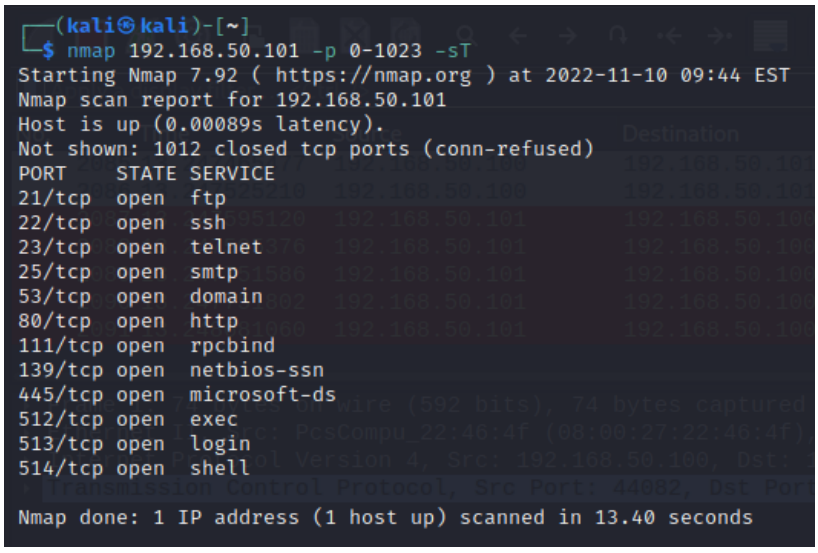
Riepilogo

SOURCE	TARGET	SCAN TYPE	RESULTS
192.168.50.100	192.168.50.101	TCP CONNECT SCAN	12 open well-known ports
192.168.50.100	192.168.50.101	TCP SYN SCAN	
192.168.50.100	192.168.50.101	AGGRESSIVE SCAN	

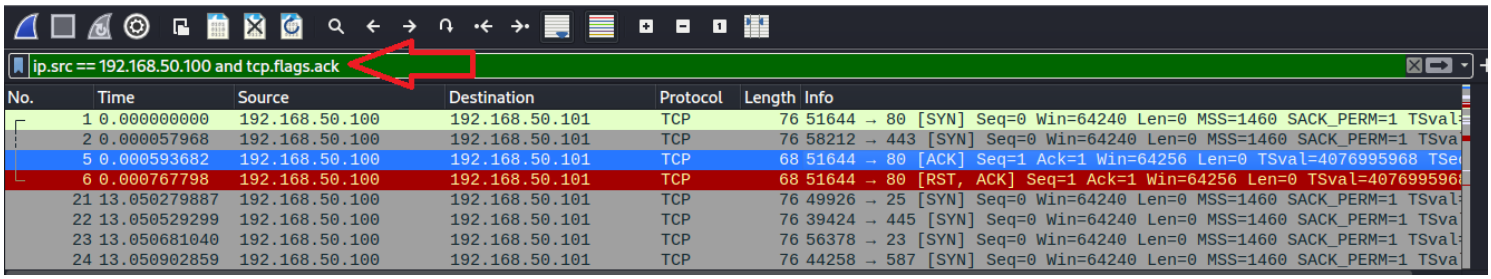
PORT	STATUS	SERVICE
21/tcp	Open	ftp
22/tcp	Open	Ssh
23/tcp	Open	telnet
25/tcp	Open	Smtp
53/tcp	Open	Domain
80/tcp	Open	http
111/tcp	Open	Rpcbind
139/tcp	Open	Netbios-ssn
445/tcp	Open	Microsoft-ds
512/tcp	Open	Exec
513/tcp	Open	Logic
514/tcp	Open	shell

1. TCP CONNECT SCAN

Avviamo la scansione delle porte well-known eseguendo il comando **nmap 192.168.50.101 -p 0-1023 -sT**



Analizzando il traffico TCP con Wireshark e applicando un filtro sul **source IP** ed uno sui **pacchetti ACK**, possiamo notare la presenza di pacchetti TCP con flag **ACK** inviati dalla macchina Kali 192.168.50.100 a Metasploitable 192.168.50.101, in quanto questo tipo di scansione completa tutti i passaggi del three-way handshake.



No.	Time	Source	Destination	Protocol	Length	Info
5	0,000593682	192.168.50.100	192.168.50.101	TCP	68	51644 > 80 [ACK] eq=1 Ack=1 Win=64256 Len=0 TSval=4076995968 TSecr=487210
33	13,05289871	192.168.50.100	192.168.50.101	TCP	68	49926 > 25 [ACK] eq=1 Ack=1 Win=64256 Len=0 TSval=4077009020 TSecr=488514
34	13,05291376	192.168.50.100	192.168.50.101	TCP	68	39424 > 44 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4077009020 TSecr=488514
35	13,05291872	192.168.50.100	192.168.50.101	TCP	68	56378 > 23 [ACK] eq=1 Ack=1 Win=64256 Len=0 TSval=4077009020 TSecr=488514
42	13,05509756	192.168.50.100	192.168.50.101	TCP	68	58452 > 13 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4077009022 TSecr=488515
61	13,05898314	192.168.50.100	192.168.50.101	TCP	68	59096 > 80 [ACK] eq=1 Ack=1 Win=64256 Len=0 TSval=4077009026 TSecr=488515
62	13,05899924	192.168.50.100	192.168.50.101	TCP	68	50880 > 53 [ACK] eq=1 Ack=1 Win=64256 Len=0 TSval=4077009026 TSecr=488515
66	13,05978926	192.168.50.100	192.168.50.101	TCP	68	49178 > 11 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4077009027 TSecr=488515
72	13,06093745	192.168.50.100	192.168.50.101	TCP	68	50742 > 22 [ACK] eq=1 Ack=1 Win=64256 Len=0 TSval=4077009028 TSecr=488515
73	13,06104522	192.168.50.100	192.168.50.101	TCP	68	53870 > 21 [ACK] eq=1 Ack=1 Win=64256 Len=0 TSval=4077009028 TSecr=488515
150	13,07655851	192.168.50.100	192.168.50.101	TCP	68	54556 > 51 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4077009044 TSecr=488517
329	13,09041006	192.168.50.100	192.168.50.101	TCP	68	49144 > 51 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4077009058 TSecr=488518
856	13,11858184	192.168.50.100	192.168.50.101	TCP	68	42076 > 51 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4077009086 TSecr=488521

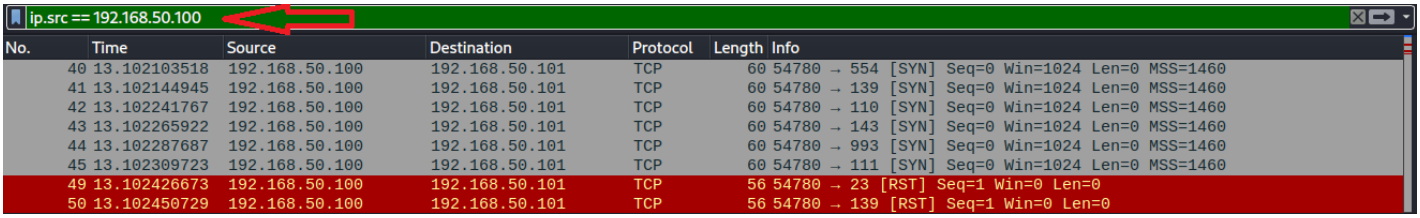
2. TCP SYN SCAN

Avviamo la scansione delle porte well-known eseguendo il comando **sudo nmap 192.168.50.101 -p 0-1023 -sS**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.101 -p 0-1023 -sS
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 10:01 EST
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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: 08:00:27:05:79:1F (Oracle VirtualBox virtual NIC)

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

Questo tipo di scansione è più leggera e non completa i passaggi del three-way handshake, in quanto la macchina con source IP 192.168.50.100 chiude la connessione inviando pacchetti con flag **RST.** Non viene inviato quindi nessun pacchetto ACK**.**



No.	Time	Source	Destination	Protocol	Length	Info
15	13,09889137	192.168.50.100	192.168.50.101	TCP	60	54780 > 19 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	13,0991182	192.168.50.100	192.168.50.101	TCP	60	54780 > 80 SYN] eq=0 Win=1024 Len=0 MSS=1460
17	13,09916103	192.168.50.100	192.168.50.101	TCP	60	54780 > 21 SYN] eq=0 Win=1024 Len=0 MSS=1460
18	13,09933649	192.168.50.100	192.168.50.101	TCP	60	54780 > 13 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	13,09937506	192.168.50.100	192.168.50.101	TCP	60	54780 > 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	13,09959425	192.168.50.100	192.168.50.101	TCP	60	54780 > 25 SYN] eq=0 Win=1024 Len=0 MSS=1460
24	13,09991715	192.168.50.100	192.168.50.101	TCP	56	54780 > 80 RST] eq=1 Win=0 Len=0
25	13,09994951	192.168.50.100	192.168.50.101	TCP	56	54780 > 21 RST] eq=1 Win=0 Len=0
29	13,1001394	192.168.50.100	192.168.50.101	TCP	56	54780 > 25 RST] eq=1 Win=0 Len=0
30	13,10111666	192.168.50.100	192.168.50.101	TCP	60	54780 > 58 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	13,10115551	192.168.50.100	192.168.50.101	TCP	60	54780 > 11 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	13,10117279	192.168.50.100	192.168.50.101	TCP	60	54780 > 44 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
33	13,10118761	192.168.50.100	192.168.50.101	TCP	60	54780 > 22 SYN] eq=0 Win=1024 Len=0 MSS=1460
38	13,10169758	192.168.50.100	192.168.50.101	TCP	56	54780 > 22 RST] eq=1 Win=0 Len=0
39	13,10191641	192.168.50.100	192.168.50.101	TCP	60	54780 > 23 SYN] eq=0 Win=1024 Len=0 MSS=1460
40	13,10210352	192.168.50.100	192.168.50.101	TCP	60	54780 > 55 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
41	13,10214495	192.168.50.100	192.168.50.101	TCP	60	54780 > 13 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42	13,10224177	192.168.50.100	192.168.50.101	TCP	60	54780 > 11 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

3. AGGRESSIVE SCAN

Avviamo la scansione delle porte well-known eseguendo il comando **nmap 192.168.50.101 -p 0-1023 -A**

Questo tipo di scansione, oltre alle informazioni sullo stato delle porte, analizza informazioni aggiuntive. In figura 2 possiamo ad esempio vedere che vengono anche rilevate le specifiche relative al **Sistema Operativo**.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.101 -p 0-1023 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 10:45 EST
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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)
```

Figura 1

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-11-10T10:46:33-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h30m01s, deviation: 3h32m08s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
```

Figura 2