Manuel Di Gangi

S5_L3

21 febbraio 2024

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection. E la seguente sul target

Windows 7:

- OS fingerprint.

A valle delle scansioni è prevista la produzione di un report contenente le seguenti info (dove disponibili): IP, Sistema Operativo, Porte Aperte, Servizi in ascolto con versione.

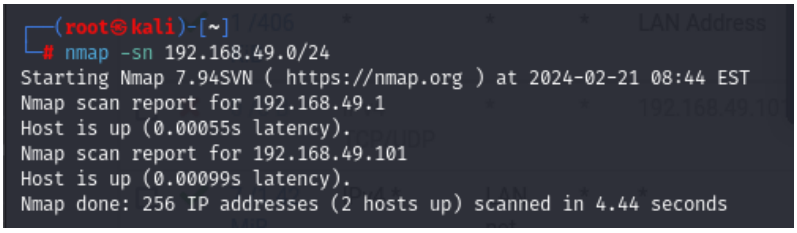
Quesito extra (al completamento dei quesiti sopra): Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Scansione della rete

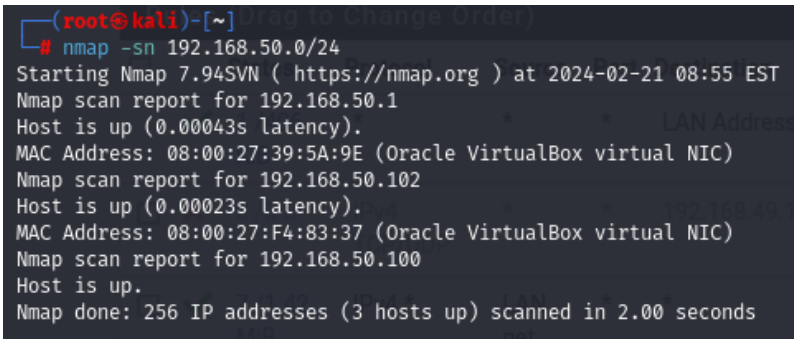
Indirizzi IP

Come prima operazione effettuiamo una scansione della rete alla ricerca dei nostri target

All'interno della prima rete individuiamo due dispositivi: il primo è l'interfaccia del gateway (nel nostro caso PFsense), il secondo è l'indirizzo della macchina di Metasploit, il nostro primo target.



Continuiamo la scansione sulla seconda rete, individuiamo tre dispositivi: il primo è sempre l'interfaccia del gateway, il secondo è la macchina Kali da dove stiamo operando in fine il terzo indirizzo appartiene alla macchina Windows, il secondo target.



Sistemi operativi, Porte aperte e Servizi in ascolto

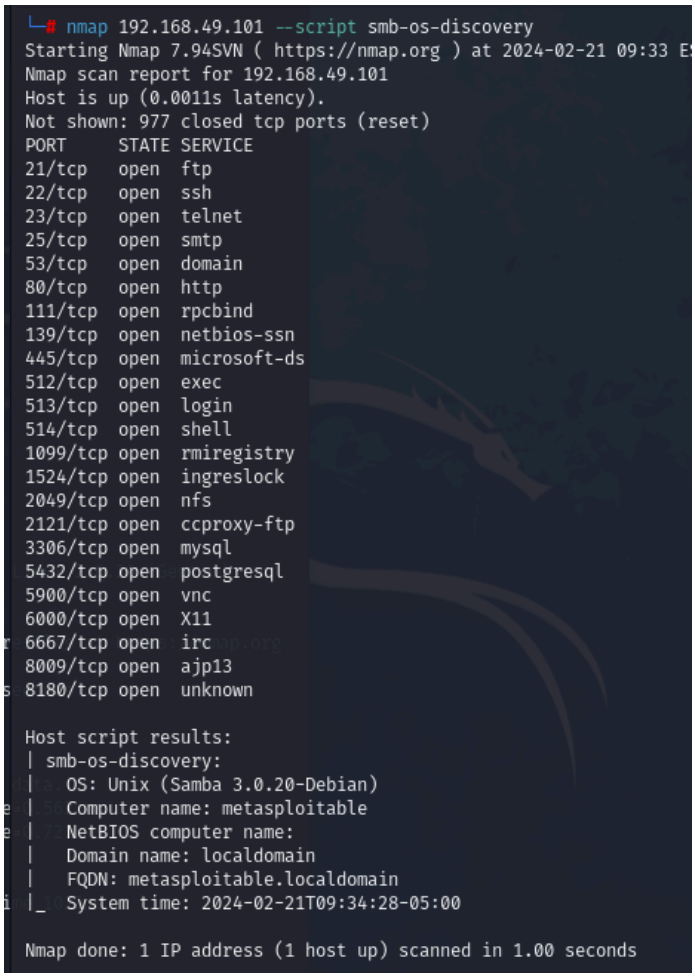
Lo step successivo è studiare il sistema operativo dei nostri target così da conoscere l'ambiente in cui ci andremo ad introdurre. Per accelerare la raccolta di informazioni anzichè eseguire le varie interrogazioni con i parametri -O -sT - sS eseguiamo lo script smb-os-discovery

Eseguendo lo script in figura per l'indirizzo **192.168.49.101** rileviamo che:

La macchina ha molte porte aperte fra cui rientrano anche delle porte **non sicure:**

- 21 FTP
- 23 TELNET
- 25 SMTP
- 53 DNS
- 80 HTTP
- 445 SMB

Sulla macchina gira un sistema operativo su base Unix nello specifico Samba 3.0.20-Deian



Tentando di contattare la macchina windows riceviamo le seguenti informazioni. Deduciamo che la sicurezza di windows è molto più alta di quella di Metasploit

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.50.102 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:45 EST
Nmap scan report for 192.168.50.102
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:F4:83:37 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds
```

Tuttavia interrogando la macchina su un gruppo ristretto di porte alla volta riusciamo a raccogliere le informazioni necessarie. Notiamo che tutte le porte sono filtrate dal firewall.

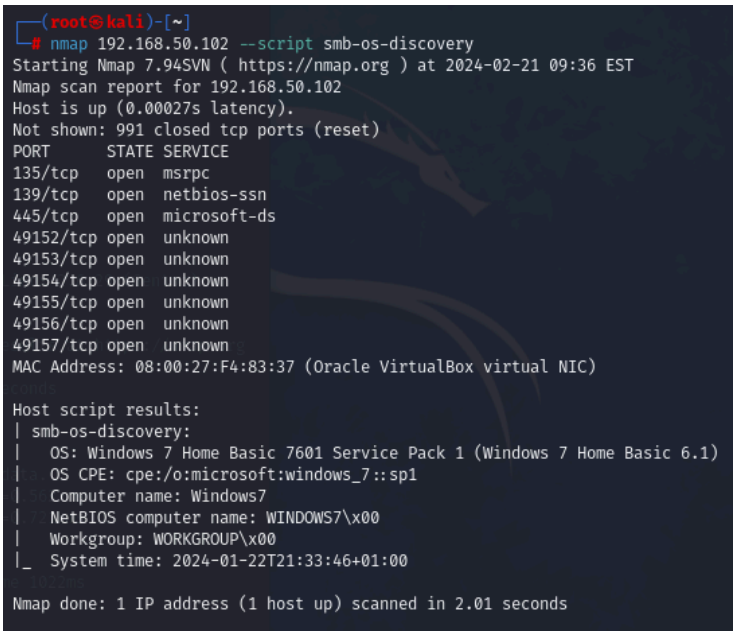
```
┌──(root㉿kali)-[~]
└─# nmap -sS -p 1-20 192.168.50.102 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:19 EST
Nmap scan report for 192.168.50.102
Host is up (0.00045s latency).

PORT   STATE    SERVICE
1/tcp  filtered tcpmux
2/tcp  filtered compressnet
3/tcp  filtered compressnet
4/tcp  filtered unknown
5/tcp  filtered rje
6/tcp  filtered unknown
7/tcp  filtered echo
8/tcp  filtered unknown
9/tcp  filtered discard
10/tcp filtered unknown
11/tcp filtered systat
12/tcp filtered unknown
13/tcp filtered daytime
14/tcp filtered unknown
15/tcp filtered netstat
16/tcp filtered unknown
17/tcp filtered qotd
18/tcp filtered msp
19/tcp filtered chargen
20/tcp filtered ftp-data
MAC Address: 08:00:27:F4:83:37 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
```

Disattivato il firewall riceviamo la seguente risposta:

Eseguendo il medesimo script all'indirizzo **192.168.50.102** rileviamo che:

La macchina ha delle porte aperte di cui molte sono alte e non conosciamo il relativo servizio.

Sulla macchina gira un sistema il sistema operativo Windows 7 Home basic



Per ottenere ulteriori sui **servizi attivi** eseguiamo il comando nmap con il parametro -sV, il quale ci ritorna la lista dei servizi attivi sulle macchine, la relativa porta e la versione del servizio.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:48 EST
Nmap scan report for 192.168.49.101
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.89 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:49 EST
Nmap scan report for 192.168.50.102
Host is up (0.00038s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:F4:83:37 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 77.97 seconds
```

Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Soluzione per proseguire le scansioni su Windows7

Precedentemente abbiamo come il risultato della scansione della porte non ci restituisse alcuna informazione utile dal momento che ci diceva che le mille porte tcp scansionate fossero in modalita “ignora”

```
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

Nella soluzione sopra abbiamo disattivato il firewall di windows per proseguire l'esercitazione, ma ciò non sarebbe possibile al di fuori del laboratorio didattico, o almeno non in questo modo. Per riuscire a proseguire la scansione potremmo:

- Tentare di effettuare un syn scan il quale è meno invasivo in quanto non completa il 3-way-handshake, rendendo le operazioni più rapide, e lasciando meno tracce.
- Timing template: è una modalità per controllare il tempo che passa tra l'invio di richieste successive, chiamata timing template. Si possono impostare 6 livelli di timing che vanno da 0 a 5. T0 e T1 sono comunemente utilizzati per bypassare gli IDS: in questa modalità gli scan sono piuttosto lenti e poco invasivi, e dunque diminuisce notevolmente la probabilità di essere intercettati
- Frammentare i pacchetti: frammentare l'header TCP su più pacchetti, in modo da rendere più difficile per un packet filter capire cosa sta succedendo.