Scansioni su Metasploitable e W7

Obiettivi dell'esercizio di oggi

Su Meta:
- OS fingerprint
- Syn Scan
- TCP Connect
- Version detection

Su Windows 7:
- Os fingerprint
- spiegazione del risultato ottenuto: proporre una soluzione per continuare le scansioni

Hint:

Mentre il comando nmap -oN report1.txt IP" scansiona l'indirizzo IP specificato e crea un file di output chiamato "report1.txt" nella directory corrente

Mapping di rete

Dopo aver settato sulla stessa rete le 3 macchine che ci serviranno (Kali, Meta e W7) assicuriamoci che pinghino. Una semplificazione del comando ping è "fping -a" che pinga automaticamente tutti gli host attivi.

```
┌──(kali㉿kali)-[~]
└─$ fping -a -g 192.168.50.101 192.168.50.110
192.168.50.101
192.168.50.102
ICMP Host Unreachable from 192.168.50.100 for ICMP Echo sent to 192.168.50.104
```

Il comando fping -a -g seguito dall intervallo di indirizzi su cui ho effettuato il check, mi conferma che la macchina kali sta pingando con meta (192.168.50.101) e con win7 (192.168.50.102). Sugli altri indirizzi mi da "host unreachable".

Tale operazione di ping sweep è eseguibile anche con nmap, come di seguito:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 09:26 EST
Nmap scan report for 192.168.50.100
Host is up (0.000043s latency).
Nmap scan report for 192.168.50.101
Host is up (0.00092s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.91 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.102/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 09:27 EST
Nmap scan report for 192.168.50.100
Host is up (0.00032s latency).
Nmap scan report for 192.168.50.101
Host is up (0.021s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 20.06 seconds
```

Infine è possibile creare un File contenente -solo- gli indirizzi IP che si vogliono provare a pingare e dare poi il seguente comando:

```
┌──(kali㉿kali)-[~]
└─$ nano File_ip.txt

┌──(kali㉿kali)-[~]
└─$ nmap -sn -iL File_ip.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 10:03 EST
Nmap scan report for 192.168.50.100
Host is up (0.00013s latency).
Nmap scan report for 192.168.50.101
Host is up (0.0017s latency).
Nmap done: 3 IP addresses (2 hosts up) scanned in 14.21 seconds
```

OS fingerprint

Dopo aver recuperato informazioni sul target e sulla mappa di rete, procediamo con la fase di OS fingerprint, necessaria per l'identificazione del sistema operativo di un nodo su una rete.

Di seguito la scansione **su Metasploitable:**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 10:24 EST
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 977 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
```

```
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:4C:DA:22 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.78 seconds
```

Dalla stessa ricaviamo che l'host è un sistema operativo Linux con un kernel compreso tra la versione 2.6.9 e 2.6.33. La scansione ha rilevato una serie di porte TCP aperte sul sistema, che includono i servizi SSH, FTP, Telnet, SMTP, HTTP, NetBIOS ecc... Il nome del dispositivo non è stato fornito nella scansione, ma l'indirizzo MAC indica che si tratta di una macchina virtuale VirtualBox con una scheda di rete virtuale.
A questo punto procedo con la scansione Os fingerprint **su Windows 7:**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 10:25 EST
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:36:38:D5 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.74 seconds
```

In questo caso, la scansione ha rilevato che tutte le 1000 porte TCP disponibili sono state ignorate e non hanno prodotto risposta, nè fornito i servizi attivi sulle stesse. Avevo pensato che questo potesse esser causato dalla configurazione del firewall di win7 che ha bloccato le scansioni sulle porte, ma mandando i comandi nmap -pn -o e -osguess non ho ottenuto nessuna informazione aggiuntiva. Una soluzione potrebbe essere quella di provare a modificare la configurazione del firewall di win7 o di eseguire le scansioni mirate su porte UDP, HTTP o DNS.

Syn Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -oN syn.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 12:09 EST
Nmap scan report for 192.168.50.101
Host is up (0.00039s latency).
Not shown: 977 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

```
8180/tcp open  unknown
MAC Address: 08:00:27:4C:DA:22 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

Tcp Connect

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -oN tcp.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 12:48 EST
Nmap scan report for 192.168.50.101
Host is up (0.00097s latency).
Not shown: 977 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:4C:DA:22 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

L'output delle due scansioni elenca tutte le porte TCP aperte e il servizio associato su Meta.
La differenza tra la scansione TCP e la Syn Scan, a giudicare dagli output è il formato e la formattazione dei risultati.
Tuttavia, entrambi i comandi forniscono informazioni utili sulle porte aperte e sui servizi in esecuzione sulla macchina scansionata. È possibile utilizzare queste informazioni per verificare la sicurezza della rete, identificare eventuali servizi vulnerabili e indirizzi IP non autorizzati.

Version detection

La scansione è parimenti eseguibile digitando il comando nmap -sV 192.168.50.101, codice che fornirà in aggiunta la versione del servizio, come di seguito:

```
Nmap scan report for 192.168.50.101
Host is up (0.00034s 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
MAC Address: 08:00:27:4C:DA:22 (Oracle VirtualBox virtual NIC)
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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.77 seconds
```