Nmap: scansione di due macchine target

Nella prova di oggi useremo nmap per provare a scansionare due macchine target in ambiente virtuale, nel particolare lanceremo nmap da Kali bersagliando Metasploitable e Windows 7.

Innanzitutto, effettuiamo una scansione sulla sottorete dove si trovano le macchine per ricavarne gli indirizzi IP.

```
┌──(giuseppe㉿kali)-[~]
└─$ nmap -sn 192.168.50.*
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:17 CEST
Stats: 0:00:50 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 3 hosts. Timing: About 0.00% done
Nmap scan report for 192.168.50.100
Host is up (0.00011s latency).
Nmap scan report for 192.168.50.101
Host is up (0.00019s latency).
Nmap scan report for 192.168.50.102
Host is up (0.00027s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 59.92 seconds
```

Come possiamo notare, otteniamo in output tre diversi IP, appartenenti rispettivamente a Kali, Metasploitable e Windows 7. Ora che abbiamo gli IP dei target, possiamo approfondire la nostra indagine.

Per adesso, concentriamo l'indagine sul solo Metasploitable

Utilizzando il comando visibile nella prossima immagine, il quale richiama uno script, indaghiamo quale sia il sistema operativo presente sulla macchina.

```
┌──(giuseppe㉿kali)-[~]
└─$ nmap 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:12 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00016s 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  microsof0
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

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: 2023-10-25T09:13:09-04:00

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

Evidenziando la parte finale dello script, leggiamo non solo quale sistema è presente, Unix in questo caso, ma anche il nome della macchina e la presenza del software Samba per la comunicazione multi-piattaforma.

Procediamo poi evidenziando quali porte siano aperte. Possiamo ottenere tale risultato in diversi modi (quello preso ad esempio sulla sinistra usa -p-); spostiamo però l'attenzione sul comando -sS nell'immagine a destra: questo permette a nmap di "troncare" il 3-way handshake anticipatamente (mandando solo un pacchetto syn e interrompendo la sessione dopo aver ricevuto il pacchetto syn-ack), riducendo il rumore a livello del target e quindi riducendo anche la possibilità di essere scoperti dai meccanismi di sicurezza del target, oltre a ridurre il tempo necessario alla scansione.

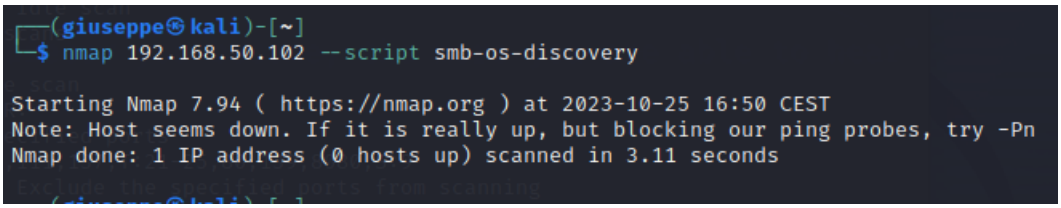
```
┌──(giuseppe㉿kali)-[~]
└─$ nmap -p- 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:38 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00030s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34421/tcp open  unknown
43689/tcp open  unknown
53504/tcp open  unknown
57180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.53 seconds
```

```
┌──(giuseppe㉿kali)-[~]
└─$ sudo nmap -sS  192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:51 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00013s 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: 08:00:27:7E:BE:F3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

Infine, andiamo ad esaminare nel dettaglio le porte e i relativi servizi, esaminandone anche la versione. Questo potrebbe permetterci di trovare delle vulnerabilità qualora uno dei servizi non dovesse essere aggiornato e presentare quindi una vecchia versione con vulnerabilità note.

```
┌──(giuseppe㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:41 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (conn-refused)
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://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 65.83 seconds
```

Come ultimo test, proviamo a ricavare quale OS sia in uso sulla seconda macchina target (che noi sappiamo essere Windows 7).



Notiamo subito come la ricerca sia stata inconcludente: non visualizziamo infatti neanche lo stato delle porte. Ciò avviene a causa del firewall, il quale blocca il protocollo ICMP e la scansione da parte del sistema attaccante, tanto che non abbiamo risultati anche inserendo il comando -Pn per aggirare il blocco ai ping.

A riporova di ciò infatti, se disattiviamo il firewall e riproviamo la scansione, noteremo come questa fornirà risultati indicando il sistema operativo della macchina.