Consenga S5-L3

Introduzione ad nmap

TRACCIA

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 le seguenti sul target Windows 7:

- OS fingerprint .

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, 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?

Scan sull'indirizzo di meta

IP: 192.168.50.101

PORTE: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180 con servizio tcp

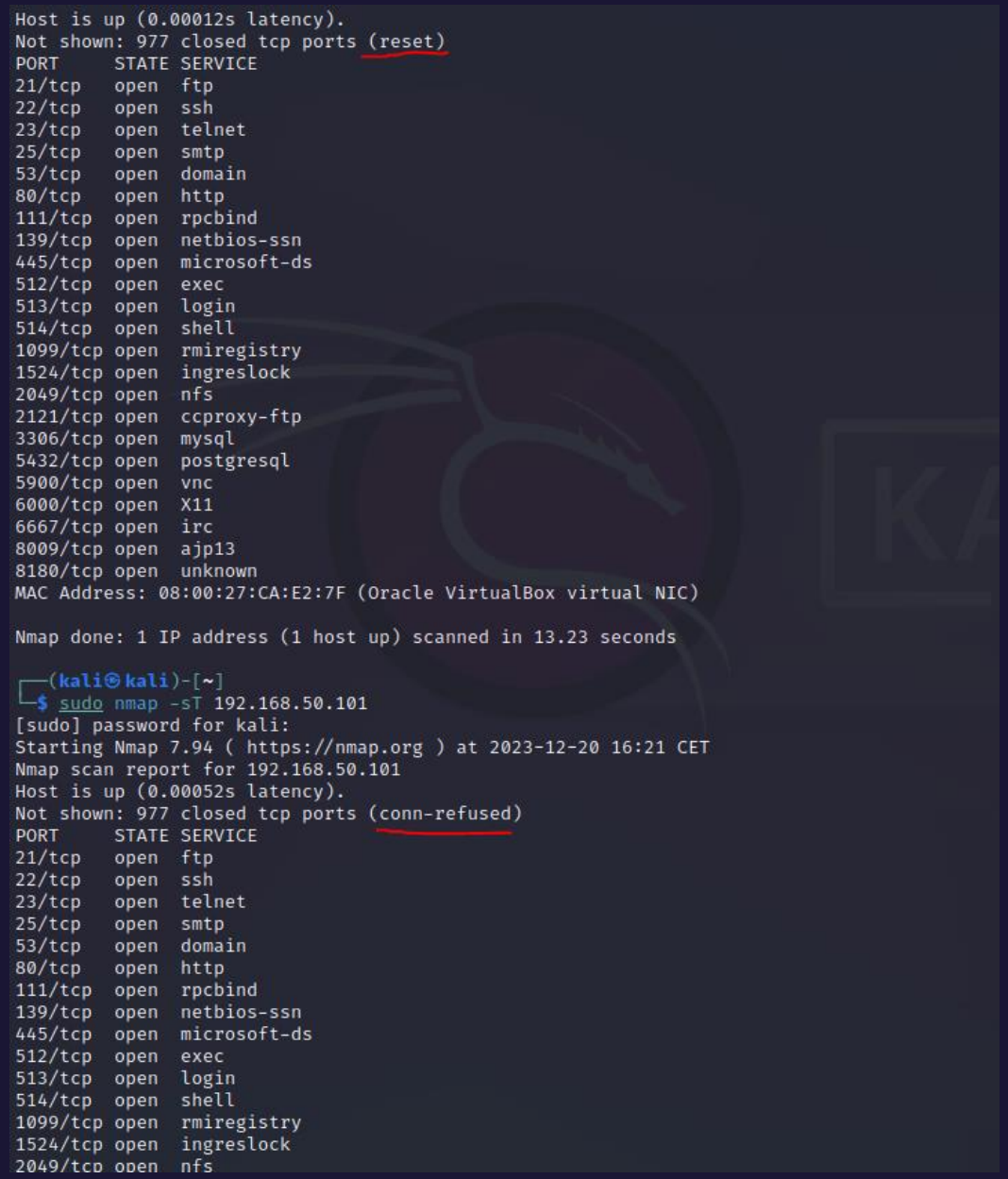
OS: Linux 2.6.X

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 15:48 CET
Nmap scan report for 192.168.50.101
Host is up (0.00048s 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:CA:E2:7F (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 14.74 seconds
```

Confronto tra Syn e TCP connect

Nella prima c'è un vero e proprio three-way-handshake essendo di tipo reset mentre nella seconda viene rifiutata la richiesta dal firewall (conn-refused)



Comando version detection

In questa slide le informazioni forniteci grazie all'esecuzione del comando -sV che ci illustra i servizi attivi sulle porte

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
sudo] password for kali:
tarting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:43 CET
map scan report for 192.168.50.101
ost is up (0.00011s latency).
ot shown: 977 closed tcp ports (reset)
ORT     STATE SERVICE     VERSION
1/tcp   open  ftp         vsftpd 2.3.4
2/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
3/tcp   open  telnet      Linux telnetd
5/tcp   open  smtp        Postfix smtpd
3/tcp   open  domain      ISC BIND 9.4.2
0/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
11/tcp  open  rpcbind     2 (RPC #100000)
39/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
45/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
12/tcp  open  exec        netkit-rsh rexecd
13/tcp  open  login?
14/tcp  open  shell       Netkit rshd
099/tcp open  java-rmi    GNU Classpath grmiregistry
524/tcp open  bindshell   Metasploitable root shell
049/tcp open  nfs         2-4 (RPC #100003)
121/tcp open  ftp         ProFTPD 1.3.1
306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
900/tcp open  vnc         VNC (protocol 3.3)
000/tcp open  X11         (access denied)
667/tcp open  irc         UnrealIRCd
009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
AC Address: 08:00:27:CA:E2:7F (Oracle VirtualBox virtual NIC)
ervice Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Lin
; CPE: cpe:/o:linux:linux_kernel

ervice detection performed. Please report any incorrect results at https://nmap.org/sub
t/ .
map done: 1 IP address (1 host up) scanned in 65.82 seconds
```

OS fingerprint su windows 7

```
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 16:57 CET
Nmap scan report for 192.168.50.102
Host is up (0.00067s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:97:1C:91 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Pal
mmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows
_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 c
pe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows
 Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0,
 Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP modu
le, VMware Player virtual NAT device
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 37.01 seconds
```

Si può notare come il firewall di win7 vada a bloccare la connessione, impedendoci di ricavare informazioni

OS fingerprint su windows 7

Si può bypassare questo problema andando a disattivare il firewall su win7 oppure aprire le porte in entrata e uscita UDP/TCP dalle impostazioni di esso

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 17:07 CET
Nmap scan report for 192.168.50.102
Host is up (0.00090s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:97:1C:91 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:wi
ndows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R
2, Windows 8, or Windows 8.1 Update 1
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 36.43 seconds
```

IP: 192.168.50.102

PORTE: 135, 139, 445, 49152-49157 con servizio tcp

OS: Microsoft Windows 7



FINE

Amedeo Natalizi