CONSEGNA S5/L3

di Giuseppe Lupoi

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 .

TRACCIA – TECNICHE DI SCANSIONE CON NMAP

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?

Comincerò esponendo le scansioni sul target Metasploitable

OS fingerprint

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 08:39 EST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8180/tcp open  unknown
MAC Address: CA:01:D0:D2:AF:9A (Unknown)
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/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

Version Detection

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 08:42 EST
Nmap scan report for 192.168.50.101
Host is up (0.00047s latency).
Not shown: 982 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
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
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8180/tcp open  tcpwrapped
MAC Address: CA:01:D0:D2:AF:9A (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni
x, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.05 seconds
```

L’unica differenza che ho scovato tra le due scansioni è nel messaggio di output nella riga **“Not shown: 982 closed tcp ports”** dove tra parentesi riceviamo:
da **TCP (conn-refused)**, mentre nel **SYN (reset)**

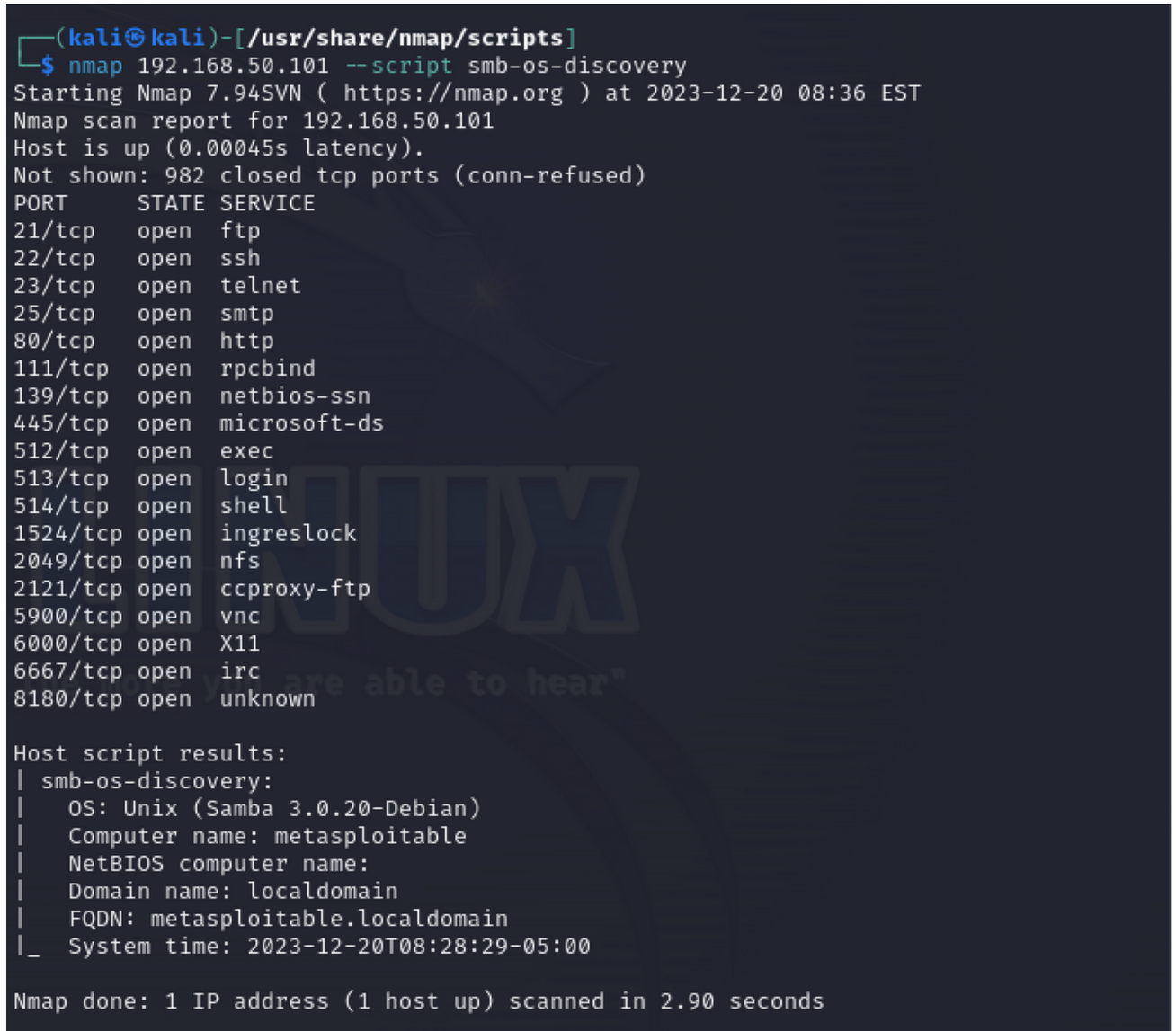
TCP Connect

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 08:41 EST
Nmap scan report for 192.168.50.101
Host is up (0.00089s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8180/tcp open  unknown
MAC Address: CA:01:D0:D2:AF:9A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Syn Scan

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 08:41 EST
Nmap scan report for 192.168.50.101
Host is up (0.00047s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8180/tcp open  unknown
MAC Address: CA:01:D0:D2:AF:9A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Ho voluto provare anche lo script Samba per vedere che tipo di output ricevevo



REPORT METASPLOITABLE

Riguardo i dati e le informazioni acquisite dalle scansioni possiamo affermare che:

- Indirizzo IP Target: 192.168.50.101
- Sistema operativo: Unix
- Porte aperte: 21, 22, 23, 25, 80, 111, 139, 445, 512, 513, 514, 1524, 2049, 2121, 5900, 6000, 6667, 8180 // TCP
- Servizi attivi / relativa versione:

ftp/vsftpd 2.3.4,
telnet/Linux telnetd
http/Apache httpd 2.2.8
netbios-ssn/Samba smbd 3.X 4.X
login/-
bindshell/Metasploitable rooot shell
ftp/ProFTPD 1.3.1
X11/(access denied)
tcpwrapped/-

ssh/OpenSSH 4.7p1 Debian 8ubuntu1
smtp/Postfix smtpd
rpcbind/2(RPC #100000)
exec/netkit-rsh rexecd
shell/Netkit rshd
nfs/2-4 (RPC #100003)
vnc/VNC (protocol 3.3)
irc/UnrealIRCd

Ed infine la scansione sul target Windows7

OS fingerprint

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-21 14:15 EST
Nmap scan report for 192.168.50.102
Host is up (0.0074s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
554/tcp  open  rtsp
7070/tcp open  realserver
Warning: OSScan results may be unreliable because we could not find at least 1 ope
n and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.01 seconds
```

REPORT WINDOWS7

Riguardo i dati e le informazioni acquisite nella scansione della pagina precedente possiamo affermare che:

- L’host risulta attivo
- Esistono 998 porte TCP filtrate

Porte scansionate:

- 554 // TCP con servizio attivo **rtsp**
- 7070 // TCP con servizio attivo **realserver**

IN CUNCUSIONE AL QUESITO EXTRA:

Dopo la scansione OS Fingerprint effettuata su Win7 notiamo da subito la differenza con Metasploitable in quanto su Windows la scansione ci fornisce molte meno informazioni sul target.

Questo potrebbe essere dovuto al fatto che Win7 da impostazioni predefinite ha antivirus e firewall attivi che impedisco e bloccano la ricezione di pacchetti non autorizzati.

Come soluzione per ovviare queste difese si potrebbero disattivare quei servizi che appunto bloccano il traffico non autorizzato.