

Esercizio S5_L3

Rosario Giaimo

Ecco come eseguire le scansioni richieste utilizzando Nmap sui due diversi target

Scansioni sul target Metasploitable:

OS Fingerprinting:

```

File Actions Edit View Help
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
53/tcp open  domain
514/tcp open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  cccproxy-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: 08:00:27:25:D6:74 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
(kali㉿kali)-[~]
└─$ sudo nmap -T4 192.168.50.101
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-03-27 09:34 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00028s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
53/tcp    open  domain
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-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: 08:00:27:25:D6:74 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS: 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 14.49 seconds
(kali㉿kali)-[~]
└─$ 

```

```

File Macchina Visualizza Inserimento Dispositivi Auto
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.101
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.50.101
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:25:D6:74
          inet6 addr: fe80::a00:27ff:fe25:d674/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1023 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:67290 (65.7 KB) TX bytes:56134 (54.8 KB)
          Base address:0x0d10 Memory:f0200000-f0220000

lo      Link encap:Local Loopback
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40017 (39.0 KB) TX bytes:40017 (39.0 KB)

msfadmin@metasploitable:~$ 

```

Syn Scan:

```

File Actions Edit View Help
-- 192.168.50.101 ping statistics --
7 packets transmitted, 7 received, 0% packet loss, time 6133ms
rtt min/avg/max/mdev = 0.234/145.002/1013.308/354.484 ms, pipe 2
(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.1.100
(kali㉿kali)-[~]
└─$ ping 192.168.1.101
ping: connect: Network is unreachable
(kali㉿kali)-[~]
└─$ ping 192.168.1.101
ping: connect: Network is unreachable
(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.50.100
(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.595 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.268 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.239 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.529 ms
``C``

-- 192.168.50.101 ping statistics --
4 packets transmitted, 0 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.253/0.435/0.424/0.174 ms
(kali㉿kali)-[~]
└─$ sudo nmap -T4 192.168.50.101
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-03-27 09:31 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00024s 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  cccproxy-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: 08:00:27:25:D6:74 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
(kali㉿kali)-[~]
└─$ 

```

```

File Macchina Visualizza Inserimento Dispositivi Auto
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.101
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.50.101
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:25:D6:74
          inet6 addr: fe80::a00:27ff:fe25:d674/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1045 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1023 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:67290 (65.7 KB) TX bytes:56134 (54.8 KB)
          Base address:0x0d10 Memory:f0200000-f0220000

lo      Link encap:Local Loopback
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40017 (39.0 KB) TX bytes:40017 (39.0 KB)

msfadmin@metasploitable:~$ 

```

TCP Connect Scan:

```

kali㉿kali:~$ nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:40 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0001s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  rpopd
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1899/tcp  open  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6061/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:25:D6:74 (Oracle VirtualBox virtual NIC)

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

```

Per confrontare i risultati tra le scansioni Syn Scan e TCP Connect Scan, si possono osservare le differenze nelle risposte dei pacchetti. Syn Scan invia solo un pacchetto SYN per determinare se una porta è aperta o chiusa, mentre TCP Connect Scan stabilisce una connessione TCP completa, richiedendo quindi un maggior numero di pacchetti per ogni porta.

Version Detection:

```

kali㉿kali:~$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:41 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 7.9p1 Debian 10+deb10u1
23/tcp    open  telnet           vsftpd 3.0.4
25/tcp    open  smtp             vsftpd 3.0.4
53/tcp    open  domain           OpenSSH 7.9p1 Debian 10+deb10u1
80/tcp    open  http             OpenSSH 7.9p1 Debian 10+deb10u1
110/tcp   open  rpopd            OpenSSH 7.9p1 Debian 10+deb10u1
139/tcp   open  netbios-ssn      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  microsoft-ds     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec             netkit-rsh rexecd
513/tcp   open  login            netkit-rsh
514/tcp   open  shell            netkit-rsh
1899/tcp  open  rmiregistry      GNU GRMNPATH rmiregistry
2049/tcp  open  nfs              netkit-nfsd 2.4- (RPC #100003)
2121/tcp  open  cproxy-ftp      ProFTPD 1.3.5a
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)
6061/tcp  open  irc              Unprivileged IRC
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8180/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:25:D6:74 (Oracle VirtualBox virtual NIC)

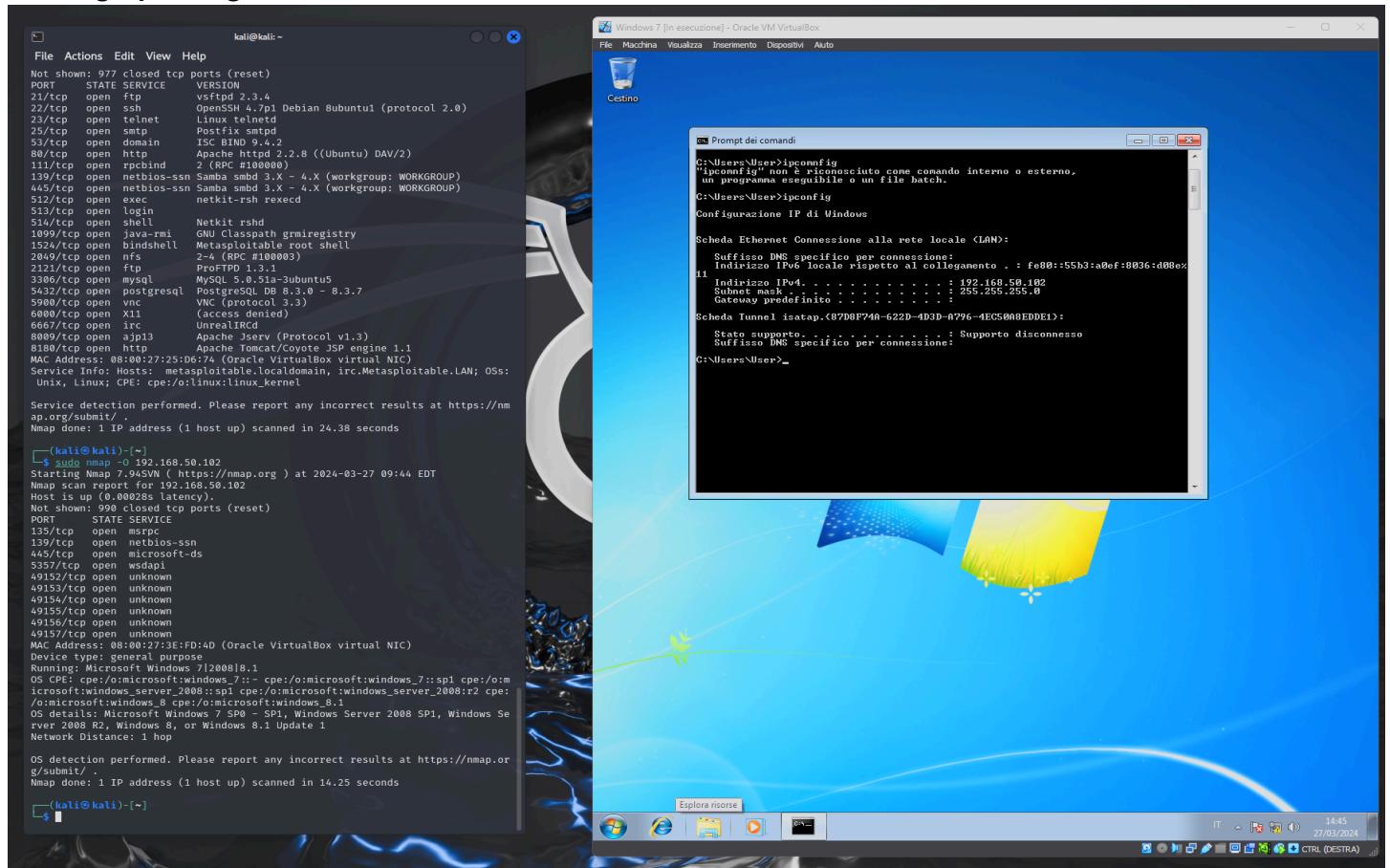
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 24.38 seconds

```

Scansione sul target Windows 7:

OS Fingerprinting:



Se la porta 990 non ha dato riscontri durante i test di scansione con Nmap e viene categorizzata come "filtrata", significa che Nmap non ha ricevuto né una risposta di apertura (SYN/ACK) né una risposta di chiusura (RST/ACK) dalla porta durante la scansione SYN. Questo scenario indica che la porta potrebbe essere bloccata da un firewall, filtro di rete o da qualche altra forma di protezione.

Per continuare a investigare sulla porta 990 e confermare se è effettivamente filtrata, è possibile eseguire altre azioni:

Scansione con altre tecniche: Utilizzare altre tecniche di scansione supportate da Nmap, come la scansione TCP Connect, la scansione UDP o la scansione completa dei servizi, per vedere se si ottiene un risultato diverso.

Analisi del firewall: Verificare le configurazioni del firewall sul target o lungo il percorso di rete per identificare se la porta 990 è stata bloccata volontariamente.

Utilizzo di strumenti di analisi del traffico: Utilizzare strumenti come Wireshark per analizzare il traffico di rete durante la scansione e vedere se ci sono segni di blocchi o filtri sulla porta 990.

Esame delle registrazioni di sistema: Controllare i registri di sistema del target per eventuali segni di attività di rete sulla porta 990 e per comprendere meglio il motivo per cui non si ottiene una risposta durante la scansione.

Analisi delle politiche di sicurezza: Verificare le politiche di sicurezza dell'ambiente target per determinare se ci sono regole o politiche che potrebbero influenzare l'accessibilità della porta 990.

