M3-W11D1

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

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

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
Descrizione dei servizi

https://www.poftut.com/nmap-output/

nmap -oN report1 IP

OS fingerprint

```
└─$ sudo nmap -O  192.168.50.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21
14:05 EST
Nmap scan report for 192.168.50.100
Host is up (0.0034s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
```

```
sudo nmap -O  192.168.50.100
```

Syn Scan:	
└─$ sudo nmap -sS 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-21 14:12 EST Nmap scan report for 192.168.50.100 Host is up (0.041s 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 Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds	sudo nmap -sT 192.168.50.100

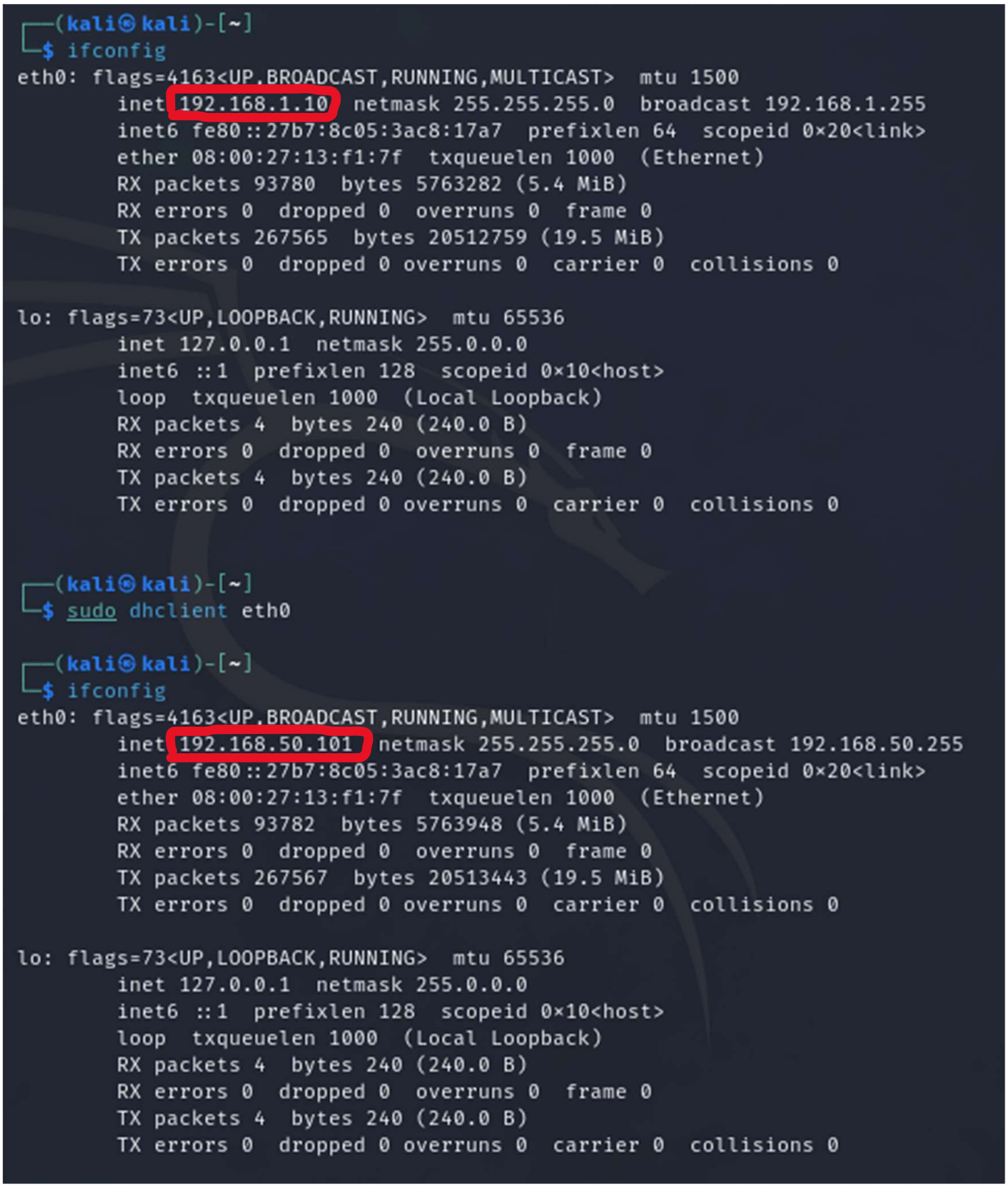
TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN	
└─$ sudo nmap -sT 192.168.50.100 Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-21 14:10 EST Nmap scan report for 192.168.50.100 Host is up (0.027s latency). Not shown: 977 closed tcp ports (conn-refused) PORT STATE 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 Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds	sudo nmap -sT 192.168.50.100

-Version detection

```
└─$ sudo nmap -sV 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21
14:14 EST
Nmap scan report for 192.168.50.100
Host is up (0.11s 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  ccproxy-ftp?
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 175.30 seconds
```

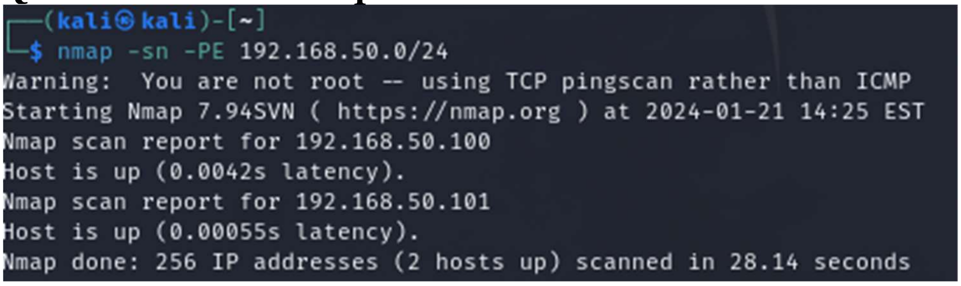
sudo nmap -sV 192.168.50.100

Adesso le due macchine sono nella stessa rete, vediamo se cambia qualcosa:



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::27b7:8c05:3ac8:17a7  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:13:f1:7f  txqueuelen 1000  (Ethernet)
        RX packets 93780  bytes 5763282 (5.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 267565  bytes 20512759 (19.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ sudo dhclient eth0

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.101  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::27b7:8c05:3ac8:17a7  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:13:f1:7f  txqueuelen 1000  (Ethernet)
        RX packets 93782  bytes 5763948 (5.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 267567  bytes 20513443 (19.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Qui scansione la rete per trovare la macchina vulnerabile



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.50.0/24
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 14:25 EST
Nmap scan report for 192.168.50.100
Host is up (0.0042s latency).
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 28.14 seconds
```

-Sistema Operativo - Porte Aperte - Servizi in ascolto con versione - Descrizione dei servizi

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -sTV 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 14:33 EST
Nmap scan report for 192.168.50.100
Host is up (0.0014s 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  unknown

MAC Address: 08:00:27:40:10:30 (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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 189.96 seconds
```

Cybersecurity Analyst 2023