

## Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

-OS fingerprint

Una scansione TCP che ha come obiettivo quello di identificare il OS del target.

Il sistema target viene analizzato in base all'ispezione dei pacchetti di risposta ricevuti, la determinazione del OS viene stabilita in base a TTL e alla grandezza della finestra TCP (che rappresenta in numero di byte che il sistema necessita di ricevere in input prima di rispondere ad un messaggio ricevuto).

Questa scansione è fondamentale in quanto conoscendo il OS del target, sapremo di conseguenza i suoi punti deboli.

```
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: 08:00:27:48:A0:5E (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
```

Vediamo come il comando nmap -o IP target restituisce in output N di porte chiuse, le porte (TCP) aperte con i loro relativi servizi, MAC address, OS e la sua versione di aggiornamento.

## Syn Scan:

Scansione poco invasiva difficilmente tracciabile in quanto non si basa sulla connessione 3 way-handshake , utilizzando il protocollo RST/ACK evitando così di 1 creare un ponte di comunicazione tra i 2 sistemi coinvolti , di conseguenza 2 evita che il sistema attaccante venga loggato (e quindi lasci il segno di un suo passaggio) sulle porte scansionate del target.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-19 19:44 UTC
Nmap scan report for 192.168.1.95
Host is up (0.00012s 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: 08:00:27:48:A0:5E (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

Vediamo come l'output del comando `nmap -sS IP target` restituisca come risultato Porte i loro relativi servizi e l'indirizzo MAC

TCP connect: `nmap -sT IP target`

```

Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-19 19:46 UTC
Nmap scan report for 192.168.1.95
Host is up (0.00026s 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
MAC Address: 08:00:27:48:A0:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

```

Come vediamo le differenze tra Syn scan e TCP connect come output sono identiche

La differenza sostanziale si può verificare tramite dei sniffer come Wireshark,

lo TCP scan crea, anche se per breve tempo, dei canali di comunicazione (3 way handshake) con le porte che analizza. Di conseguenza è una scansione facilmente rilevabile non solo durante la sua esecuzione, ma anche in un secondo momento controllando i log delle porte scansionate (del target).

Version detection: `nmap -sV`

Scansione lenta e pesante ma precisa. Fornisce come output non solo le porte aperte con i loro relativi servizi ma anche la versione dei software che le gestiscono e informazioni dettagliate sul OS utilizzato dal target

```

Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-19 19:47 UTC
Nmap scan report for 192.168.1.95
Host is up (0.00014s 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?	
25/tcp	open	smtp?	
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?	
513/tcp	open	login?	
514/tcp	open	shell?	
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?	
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

```

MAC Address: 08:00:27:48:A0:5E (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 193.21 seconds

```

IP/OS

Host: Kali GNU/Linux 2024.1

Target: Metasploitable Linux 2.6.x

192.168.1.100

192.168.1.95

OS protetto da un firewall

Nessuna porta scansionata

Target: : Metasploitable Linux 2.6.x

192.168.1.95

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?	
25/tcp	open	smtp?	
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?	
513/tcp	open	login?	
514/tcp	open	shell?	
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?	
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

Descrizione dei servizi:

ftp : File Transfer Protocol : protocollo di livello applicativo per il trasferimento di file basata su TCP e con architettura di tipo client-server

ssh: Secure Shell protocollo che permette di stabilire una sessione remota cifrata tramite interfaccia a riga di comando con un altro host di una rete informatica.

telnet : è un protocollo di rete, utilizzato tramite interfaccia a riga di comando per fornire all'utente sessioni di login remoto.

Smtp: è un protocollo per la trasmissione di email.

Domain: Domain Name System indica un Sistema utilizzato per assegnare nomi ai nodi delle reti

http : protocollo di livello applicativo usato come principale sistema per la trasmissione d'informazione sul web

rpcbind : un meccanismo per la gestione di applicazioni client/server

netbios-ssn: protocollo di livello sessione e riferito ad un API per comunicazioni sulla rete locale

exec: è una funzione di sistema presente nelle librerie standard del C del progetto GNU

Java-rmi : è una tecnologia che consente a processi java distribuiti di comunicazione