CYBER SECURITY & ETHICAL HACKING

ENUMERAZIONE SERVIZI E SCANSIONE

‘NMPA’ e’ il commando per avviare Nmpa
‘- O’ e’ l’opzione che indica a Nmpa di eseguire il rilevamento del sistema operativo. Nmap inizierà a eseguire la scansione del sistema operativo di Metasploitable e fornirà i risultati una volta completato il processo di scansione.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.26
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 08:02 EST
Nmap scan report for Host-006.home (192.168.1.26)
Host is up (0.00036s 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: 08:00:27:9D:45:9D (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.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
```

Nmpa –sT
Questa opzione di scansione è una forma di scansione standard che coinvolge il tentativo di connettersi a ciascuna porta del target. Se la connessione viene stabilita, Nmap determina che la porta è aperta.
È più affidabile ma più lenta rispetto ad altri tipi di scansione, in quanto stabilisce effettivamente una connessione TCP completa con ogni porta che si intende testare.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.26
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 08:03 EST
Nmap scan report for Host-006.home (192.168.1.26)
Host is up (0.00022s 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: 08:00:27:9D:45:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Nmpa -sS
La scansione SYN coinvolge l'invio di pacchetti SYN ai porti del target. Se il porto risponde con un pacchetto SYN/ACK, viene considerato come "aperto"; se riceve un pacchetto di reset (RST), è considerato "chiuso".
È più veloce della scansione TCP Connect, ma potrebbe non essere così accurata, poiché non completa la connessione.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.26
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 08:04 EST
Nmap scan report for Host-006.home (192.168.1.26)
Host is up (0.00017s 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: 08:00:27:9D:45:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Nmpa –sV
Questa opzione consente a Nmap di individuare le versioni dei servizi che operano sulle porte aperte. Ad esempio, può identificare la versione specifica di un server web o di un servizio FTP in esecuzione su una determinata porta.
Utile per ottenere informazioni dettagliate sui servizi in esecuzione sul target, aiutando a comprendere meglio le vulnerabilità specifiche associate a versioni specifiche di software.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.26
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 08:04 EST
Nmap scan report for Host-006.home (192.168.1.26)
Host is up (0.00016s 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?
513/tcp  open  login?
514/tcp  open  tcpwrapped
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  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:9D:45:9D (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linu
x; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 63.40 seconds
```