



è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP.
- Sistema Operativo.
- Porte Aperte.
- Servizi in ascolto con versione.

IP

Per questa volta la macchina target è Metasploitable 2 , il quale IP è il seguente 192.168.43.101 , questa informazione è vitale per le operazioni che andremo a fare , essendo autorizzati non subiremo nessuna denuncia .

Sistema operativo

Per determinare il sistema operativo del target (OS Fingerprint), si usa il flag `-O`. Questo comando consente di identificare il sistema operativo cercando di riconoscere alcune caratteristiche specifiche del sistema target:

```

root@kali: /home/kali
File Actions Edit View Help
[sudo] password for kali:
root@kali: /home/kali
nmap -O 192.168.43.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:08 EDT
Nmap scan report for 192.168.43.101
Host is up (0.00029s 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:C5:3B:59 (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 1.56 seconds

```

È importante sapere che il rilevamento del sistema operativo è più preciso se Nmap riesce a trovare e analizzare porte aperte e chiuse.

Porte Aperte

Per effettuare la scansione delle porte aperte abbiamo diversi comandi che possiamo lanciare :

1) `nmap -sS`

Utilizza il comando SYN Scan per una scansione veloce e stealth

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -sS 192.168.43.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:10 EDT
Nmap scan report for 192.168.43.101
Host is up (0.000066s 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:C5:3B:59 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Questo metodo è molto utilizzato perché è veloce, discreta e consente di identificare le porte aperte senza stabilire una connessione TCP completa.

Piu' sicura perchè non finisce le 3 way handshake.

Servizi in ascolto con versione

Per rilevare i servizi in ascolto con le loro versioni su un target, si può utilizzare l'opzione -sV di Nmap. Questa opzione permette di identificare il tipo di servizio in ascolto su una porta e, quando possibile, la versione esatta del servizio.

Comando in questione :

1) nmap -sV

```

root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -sV 192.168.43.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:16 EDT
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 11:16 (0:00:02 remaining)
Nmap scan report for 192.168.43.101
Host is up (0.000061s latency).
Not shown: 777 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        OpenBSD or Solaris rlogind
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  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
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.94SVN%I=7%D=10/29%Time=6720FC38%P=x86_64-pc-linux-gnu%r
SF:(NULL,2B,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\
SF:li\\n");
MAC Address: 08:00:27:C5:3B:59 (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 64.11 seconds

```

