ESERCITAZIONE n°W11D1

Tecniche di scansione con Nmap

SCANSIONE
nmap -O ipotizza il sistema operativo

```
└─$ sudo nmap -O 192.168.32.11
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 14:37 EST
Nmap scan report for 192.168.32.11
Host is up (0.00023s 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: 08:00:27:80:C2:66 (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
```

SCANSIONE
nmap --script smb-os-discovery ipotizza il SO utilizzando il protocollo SMB

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.32.11 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org       24-01-16 14:54 EST
Nmap scan report for 192.168.32.11
Host is up (0.00011s 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: 08:00:27:80:C2:66 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-01-16T14:54:12-05:00

Nmap done: 1 IP address (1 host up) scanned in 13.36 seconds
```

SCANSIONE
nmap -sS scansiona l'IP senza concludere il 3HS ma essendo la scansione sulla stessa rete il risultato è lo stesso

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.32.11 -oN report1sS
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org       24-01-17 13:47 EST
Nmap scan report for 192.168.32.11
Host is up (0.00033s 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: 08:00:27:80:C2:66 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```