

NMAP

Nmap è un programma di port scanning.

Usato per scansionare le porte di possibili macchine da attaccare.

Ora andiamo a vedere alcuni comandi per fare queste scansioni effettuate sulla macchina metasploit:

`nmap -sS ip -p [port range]`

```
(kali㉿kali)-[~]  
$ sudo su  
[sudo] password for kali:  
(root㉿kali)-[/home/kali]  
# nmap -sS 192.168.1.36 -p 1-1000  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:11 EDT  
Nmap scan report for 192.168.1.36  
Host is up (0.00017s latency).  
Not shown: 988 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  
MAC Address: 08:00:27:62:75:2C (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

Questo comando è sS è il comando stealth.

Quindi è uno command stealth, un comando che fa poco rumore e non completa il 3WH.

In parole povere si ferma al primo SYN.

Un comando leggermente più aggressivo è il comando:

`nmap -sT ip -p [port range]`

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.1.36 -p 1-1000
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:12 EDT
Nmap scan report for 192.168.1.36
Host is up (0.00020s latency).
Not shown: 988 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
MAC Address: 08:00:27:62:75:2C (Oracle VirtualBox virtual NIC)

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

A differenza di `-sS` questo comando completa il 3WH e fa molto più rumore del primo, ma il funzionamento è esattamente lo stesso.

La differenza è la velocità di esecuzione `-sT` è più rapida rispetto `-sS`.

Questo comando è detto anche comando TCP.

Il tcp è proprio SYN,SYN ACK, ACK.

Il comando più aggressivo che abbiamo su nmap è
`nmap -sV ip -p [port range]`

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.36 -p 1-1000
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:12 EDT
Nmap scan report for 192.168.1.36
Host is up (0.00011s latency).
Not shown: 988 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
MAC Address: 08:00:27:62:75:2C (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; 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 49.71 seconds
```

Questo tipo di comando oltre a chiudere il 3WH è un comando che mira a vedere anche le versioni utilizzate sulle porte aperte della macchina che stiamo scannerizzando. E' il comando che fa più rumore sulla macchina scansionata.

Come possiamo vedere appunto dall'immagine le versioni usate della porte sono ben specificate.

Ora andiamo a vedere un comando di script:
nmap ip --script smb-os-discovery

```
(root@kali)-[/home/kali]
# nmap 192.168.1.36 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:15 EDT
Nmap scan report for 192.168.1.36
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: 08:00:27:62:75:2C (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: 2022-08-03T08:26:58-04:00

Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

Questo comando ci permette di vedere oltre che le porte aperte anche le versione del sistema operativo usato dalla macchina scansionata.

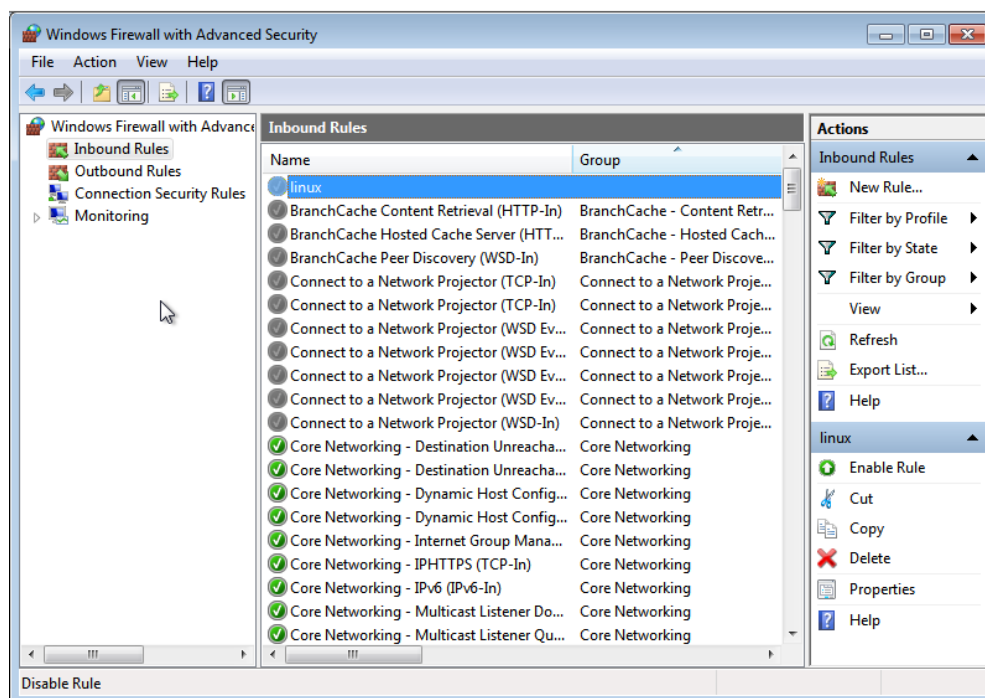
Ora cambiamo macchina e proviamo a fare le scansioni su un macchina windows, in questo caso abbiamo usato un windows 7.

Il comando lanciato è il comando di script usato precedentemente ma il firewall di windows non ci permette di fare la scansione.

```
(root@kali)-[/home/kali]
# nmap 192.168.1.100 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:32 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.1.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:95:DE:5A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.52 seconds
```

Quindi siamo andati sulla macchina windows 7 a cambiare le regole del firewall permettono alla macchina windows di parlare con linux.



A questo punto una volta cambiata la regola possiamo riprovare ad effettuare la scansione il risultato è completamente diverso.

```
(root@kali)-[/home/kali]
# nmap 192.168.1.100 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:24 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00024s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 08:00:27:95:DE:5A (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: federico-PC
|   NetBIOS computer name: FEDERICO-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-08-03T14:36:17+02:00

Nmap done: 1 IP address (1 host up) scanned in 17.67 seconds
```

Come possiamo notare ora una volta cambiata la regola del firewall abbiamo dei risultati diversi anche sulla macchina di windows.

