Report Nmap

METASPLOITABLE

IP: 192.168.32.101

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:37 GMT
Nmap scan report for 192.168.32.101
Host is up (0.00078s latency).
MAC Address: B6:44:54:D7:C0:FE (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds
```

OS: Metasploitable

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:45 GMT
Nmap scan report for 192.168.32.101
Host is up (0.00048s 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: B6:44:54:D7:C0:FE (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

Ricerca del sistema operativo con script:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.32.101 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:02 GMT
Nmap scan report for 192.168.32.101
Host is up (0.00082s 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  microsof0
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: B6:44:54:D7:C0:FE (Unknown)

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: 2023-12-20T06:02:33-05:00
```

Rispettivamente SYN e TCP:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sS 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:54 GMT
Stats: 0:02:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 10:56 (0:00:00 remaining)
Nmap scan report for 192.168.32.101
Host is up (0.00077s 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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: B6:44:54:D7:C0:FE (Unknown)
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.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 139.32 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 10:47 GMT
Nmap scan report for 192.168.32.101
Host is up (0.0013s 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: B6:44:54:D7:C0:FE (Unknown)

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

Si può notare che il nella ricerca SYN Scan chiude la comunicazione con reset, mentre nello TCP chiude la connessione alle porte chiuse con conn-refuse.
Inoltre si può notare che la version detection è stata già fatta sulla SYN scan, rilevando così le versioni sulle porte attive.

WINDOWS

Risulta impossibile raggiungere l'host perchè attivi firewall, attraverso il comando -Pn però possiamo vedere che l'IP inserito corrisponde ad un dispositivo attivo sulla rete:

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.105
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:53 GMT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 50.00% done; ETC: 11:53 (0:00:02 remaining)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn 192.168.32.105
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:55 GMT
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.50% done; ETC: 11:56 (0:00:16 remaining)
Nmap scan report for 192.168.32.105
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.32.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: A6:7C:83:03:95:E8 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 34.61 seconds
```

il firewall su Windows

Controlliamo OS della macchina Windows con IP: 192.168.32.105

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.32.105 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:04 GMT
Nmap scan report for 192.168.32.105
Host is up (0.0056s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsof0
5357/tcp open  wsdapi
MAC Address: A6:7C:83:03:95:E8 (Unknown)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7600 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: Fede-PC
|   NetBIOS computer name: FEDE-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-12-20T12:07:59-08:00

Nmap done: 1 IP address (1 host up) scanned in 18.33 seconds
```

Poi andiamo a cercare le porte aperte TCP con la loro relativa versione per completezza:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sT 192.168.32.105
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-20 11:25 GMT
Nmap scan report for 192.168.32.105
Host is up (0.0059s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: A6:7C:83:03:95:E8 (Unknown)
Service Info: Host: FEDE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 28.76 seconds
```