

## HOMEWORK 31/05/2023

### 1) OS FINGERPRINT METASPLOITABLE CON `sudo nmap -O 192.168.50.101`

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 07:37 EDT
Nmap scan report for 192.168.50.101
Host is up (0.014s 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: 08:00:27:66:40:1E (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.9 - 2.6.24 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.9 (97%), Linux 2.6.18 (Debian 4, VMware) (96%), Linksys RV042 router (96%)
No exact OS matches for host (test conditions non-ideal).
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 19.13 seconds
```

### 2) SYN Scan Metasploitable con `sudo nmap -sS 192.168.50.101`

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 09:30 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0089s 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: 08:00:27:66:40:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.07 seconds
```

### 3) TCP Connect con **sudo nmap -sT 192.168.50.101**

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.50.101 -oN report.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 09:16 EDT
Nmap scan report for 192.168.50.101
Host is up (0.010s 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: 08:00:27:66:40:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
```

### 4) Differenza SYN Scan e TCP Connect. Il SYN SCAN non completa il 3-WH, ergo non completa la scansione TCP, motivo per cui vi è il reset.

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 09:30 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0089s 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: 08:00:27:66:40:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.07 seconds
```

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 09:12 EDT
Nmap scan report for 192.168.50.101
Host is up (0.034s 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: 08:00:27:66:40:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.70 seconds
```

5) Version detection con **sudo nmap -sV 192.168.50.101**

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 08:54 EDT
Nmap scan report for 192.168.50.101
Host is up (0.024s 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?
25/tcp    open  smtp?
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  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  ccproxy-ftp?
3306/tcp  open  mysql?
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: 08:00:27:66:40:1E (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 196.21 seconds
```

- 6) Creazione report con comando `sudo nmap -sT 192.168.50.101 -oN report.txt`. In seguito ho usato il comando `ls` per aver conferma della creazione del file in .txt. Infine con comando `cat report.txt` ho aperto il report.

```
(kali@kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -oN report.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 09:16 EDT
Nmap scan report for 192.168.50.101
Host is up (0.010s 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: 08:00:27:66:40:1E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds

(kali@kali)-[~]
└─$ ls
192.168.50.101  brute.py  Documents  gameshell-save.sh  https.pcapng  Pictures  quiz10.c  report.txt  Videos
brute2.py       Desktop  Downloads  gameshell.sh       Music         Public    quiz.c    Templates

(kali@kali)-[~]
└─$ cat report.txt
# Nmap 7.93 scan initiated Wed May 31 09:16:16 2023 as: nmap -sT -oN report.txt 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.010s 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: 08:00:27:66:40:1E (Oracle VirtualBox virtual NIC)
```

- 7) OS FINGERPRINT Windows 7 con **sudo nmap -O 192.168.50.102**. Avendo già disattivato il firewall su Windows 7 è stato possibile la scansione.

```
(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 07:38 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0033s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:C5:30:64 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:win
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
```