

## M3 D4

## GIORNO 5 – ESERCIZIO

## FASE DI RACCOLTA INFORMAZIONI

**nmap -sn -PE (nostro IP)** ci permettere di scansionare una rete e scoprirne gli host attivi.



```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
# nmap -sn -PC 192.168.50.1/24  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-05-06 15:37 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.00078s latency).  
MAC Address: 08:00:12:7D:1E:61A5 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.50.100  
Host is up.  
Nmap done: 256 IP addresses (2 hosts up) scanned in 8.22 seconds  
root@kali: ~  
#
```

**nmap (nostro IP) --top-ports 10 --open** viene utilizzato per eseguire una scansione di un singolo target e identificare le 10 porte più frequentemente utilizzate e aperte su tale target.

```
root@kali: ~  
File Actions Edit View Help  
root@kali:~# nmap 192.168.50.101 --top-ports 10 --open  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 15:41 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0011s latency).  
Not shown: 3 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:01:E6:A5 (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds  
root@kali:~#
```

**nmap (nostro IP) -p -sV --reason** è un comando utilizzato per eseguire una scansione di tutte le porte aperte su di uno specifico target e identificarne i servizi in esecuzione su ciascuna porta.

```
root@kali: ~  
File Actions Edit View Help  
root@kali:~# nmap 192.168.50.101 -p -sV --reason  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 15:48 CEST  
Nmap scan report for 192.168.50.101  
Host is up, received arp-response (0.00048s latency).  
Not shown: 65545 closed tcp ports (reset)  
PORT      STATE SERVICE      REASON      VERSION  
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4  
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian Bubuntu (protocol 2.0)  
23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd  
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd  
53/tcp    open  domain       syn-ack ttl 64 ISC BIND 9.4.2  
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      syn-ack ttl 64 2 (RPC #100000)  
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         syn-ack ttl 64 netkit-rsh rshcd  
513/tcp   open  login?       syn-ack ttl 64  
514/tcp   open  shell        syn-ack ttl 64 Netkit rshd  
1099/tcp  open  java-rmi     syn-ack ttl 64 GNU Classpath gmrregistry  
1524/tcp  open  bindshell    syn-ack ttl 64 Metasploitable root shell  
2049/tcp  open  nfs          syn-ack ttl 64 2-4 (RPC #100003)  
2121/tcp  open  ftp          syn-ack ttl 64 ProFTPD 1.3.1  
3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5  
2632/tcp  open  distccd      syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  
5432/tcp  open  postgresql   syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          syn-ack ttl 64 VNC (protocol 3.3)  
6000/tcp  open  x11          syn-ack ttl 64 (access denied)  
6067/tcp  open  irc          syn-ack ttl 64 UnrealIRCd  
6697/tcp  open  irc          syn-ack ttl 64 UnrealIRCd  
8080/tcp  open  ajp13        syn-ack ttl 64 Apache 2.2.8 (Protocol v1.3)  
8180/tcp  open  http         syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1  
8787/tcp  open  drb          syn-ack ttl 64 Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)  
36019/tcp open  mountd       syn-ack ttl 64 1-3 (RPC #100005)  
44305/tcp open  nlockmgr     syn-ack ttl 64 1-4 (RPC #100021)  
53506/tcp open  java-rmi     syn-ack ttl 64 GNU Classpath gmrregistry  
60032/tcp open  status       syn-ack ttl 64 1 (RPC #100024)  
MAC Address: 08:00:27:01:E6:A5 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.IAN; 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 134.90 seconds  
root@kali:~#
```

**nmap -sS -sV -T4 (nostro IP)** questa scansione utilizza una combinazione di tecniche di scansione per determinare quali porte sono aperte sul target e identificare i servizi specifici che vengono eseguiti su tali porte. La scansione viene eseguita utilizzando una tecnica di scansione SYN, che riduce il rischio di essere rilevati, e viene eseguita con un livello di intensità moderato per ridurre il tempo di scansione.

```
root@kali:~# nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 15:56 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00040s 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/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 rshcd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath gmicregistry
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-ubuntu5
5432/tcp  open  postgresql   PostgreSQL 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
8080/tcp  open  ajp13        Apache/2.2.8 (Ubuntu) (Protocol v1.1)
8180/tcp  open  http         Apache/2.2.8 (Ubuntu) (Protocol v1.1)
MAC Address: 08:00:27:1D:1E:15 (Oracle VM 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 53.24 seconds

root@kali:~#
```