

REPORT:

- 1) Effettuato un host discovery con il comando **fping 192.168.50.0/24** e trova 3 host attivi (ovvero le 3 macchine virtuali di KALI, META, WINDOW 7). A seguire con il comando **nmap -sn 192.168.50.*** trova solo 2 host attivi (KALI E META).
- 2) Per scansionare le porte di Windows 7 qualsiasi comando di nmap mi dice che **host seems down**, mentre per Kali mi dice che lo stato delle porte è **ignored**.
- 3) Per poter scansionare anche le porte di windows ed eseguire un O.S fingerprint l'unico modo trovato è stato di inserire il comando **-Pn**, e tramite l'esecuzione seguente siamo riusciti a recuperare più informazioni possibili tramite un unico comando, eccetto per kali che continua a fornire come output che lo stato delle porte è "ignored":

```

kali@kali: ~
File Actions Edit View Help

kali@kali:~$ sudo nmap -Pn -sV -sT -O 192.168.50.100-102
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 17:10 EST
Nmap scan report for 192.168.50.100
Host is up (0.000094s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Stats: 0:02:02 elapsed; 1 hosts completed (3 up), 2 undergoing Service Scan
Service scan Timing: About 95.83% done; ETC: 17:12 (0:00:04 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.000715s latency).
Not shown: 977 closed tcp ports (conn-refused)
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        netkit-rsh rexecd
514/tcp   open  shell        Netkit rshd
1899/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2849/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  XI1          (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: 08:00:27:60:92:03 (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
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.50.102
Host is up (0.0010s latency).

```

```
kali@kali ~  
File Actions Edit View Help  
53/tcp open domain ISC BIND 9.4.2  
80/tcp open http Apache httpd 2.2.6 ((Ubuntu) DAV/2)  
111/tcp open rpcbind 2 (RPC #100000)  
139/tcp open netbios-ssn Samba smbd 3.0 - 4.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn Samba smbd 3.0 - 4.X (workgroup: WORKGROUP)  
512/tcp open exec netkit-rsh rexecd  
513/tcp open login?  
514/tcp open shell Netkit rshd  
3899/tcp open java-rmi GNU Classpath gmrregistry  
1554/tcp open bindshell Metasploitable root shell  
2049/tcp open nfs 2+ (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 Apache Jserv (Protocol v1.3)  
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:6B:92:43 (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  
Network Distance: 1 hop  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Nmap scan report for 192.168.50.102  
Host is up (0.0010s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT STATE SERVICE VERSION  
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/IUpnP)  
MAC Address: 08:00:27:6B:A6:3D (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose|specialized|phone  
Running: Microsoft Windows 2008 R2 [!Phone/Vista]  
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7;cpe:/o:microsoft:windows_8_cp  
e:/o:microsoft:windows_7 cpe:/o:microsoft:windows_cpe:/o:microsoft:windows_vista;- cpe:/o:microsoft:windows_vista:spl  
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Mi  
crosoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SPI, Windows Server 2008 SPI, or Windows 7, Microsoft Windows Vista SP2, Windows 7.5  
PI, or Windows Server 2008  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/about/.  
Nmap done: 3 IP addresses (3 hosts up) scanned in 150.53 seconds
```

```
kali@kali:~$
```

Con il comando: **sudo nmap -Pn -sV -sT -O** riusciamo a trarre molte informazioni necessarie:

- Ip_address: 192.168.50.102 (windows 7) – 192.168.50.101 (metasploitable) – 192.168.50.100 (kali linux)
- Rileviamo le porte attive e i relativi servizi. Notiamo che su meta vi sono diverse porte attive, mentre su Windows ne ha trovata solo una (5357-open-http service)
- O.S: su meta abbiamo info abbastanza precise, con Linux 2.6 e service info indicate come metasploitable, mentre in windows essendoci una sola porta trovata i dettagli sul O.S non sono molto attendibili. Grazie al comando -sV abbiamo catturato il banner del servizio della porta trovata e deduciamo che il S.O è windows
- Su kali stesso invece abbiamo pochissime informazioni.