1) OS meta

```
/home/kali/Desktop
| Monte | Marta | Mart
                                  open ftp
 22/tcp
                                  open ssh
 23/tcp
                                   open
 25/tcp
                                   open
                                                           smtp
                                   open
                                                          domain
 80/tcp
                                                       http
rpcbind
                                   open
 111/tcp
                                 open
  139/tcp
                                 open
                                                           netbios-ssn
                                                         microsoft-ds
 512/tcp
                                open
                                                          exec
 513/tcp open
                                                         login
 514/tcp open
                                                         shell
1099/tcp open
1524/tcp open
                                                           rmiregistry
                                                        ingreslock
nfs
 2049/tcp open
  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:F2:31:C7 (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
 OS detection performed. Please report any incorrect results at https://nmap.or
```

2) SYN scan meta

```
/home/kali/Desktop
    nmap -sV -sS 192.168.178.125
Nmap scan report for 192.168.178.125

Host is up (0.00048s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION
          open ftp
open ssh
21/tcp
                                 vsftpd 2.3.4
OpenSSH 4.7pl Debian 8ubuntu1 (protocol 2.0)
22/tcp
23/tcp
                                 Linux telnetd
                  telnet
          open
25/tcp
                  smtp
                                 Postfix smtpd
          open
                                 ISC BIND 9.4.2
          open
                  domain
                                Apache httpd 2.2.8 ((Ubuntu) DAV/2)
2 (RPC #100000)
80/tcp
          open http
                  rpcbind
111/tcp
          open
          open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp
445/tcp
          open
513/tcp open
                  login
514/tcp open
1099/tcp open
                  tcpwrapped
                                 GNU Classpath grmiregistry
Metasploitable root shell
                  java-rmi
1524/tcp open
                  bindshell
                 2049/tcp open
2121/tcp open
3306/tcp open
5432/tcp open
5900/tcp open
6000/tcp open X11
6667/tcp open
                                 UnrealIRCd
                                Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
8009/tcp open ajp13
8180/tcp open http
MAC Address: 08:00:27:F2:31:C7 (Oracle 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 65.01 seconds
```

3) TCP scan meta

```
# nmap -sV -sT 192.168.178.125

Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-10 10:32 EST

Nmap scan report for 192.168.178.125

Host is up (0.0057s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
             open ftp
                                          vsftpd 2.3.4
                                          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Linux telnetd
22/tcp
23/tcp
              open ssh
                       telnet
              open
25/tcp
                                           Postfix smtpd
                       smtp
              open
53/tcp
80/tcp
                                          ISC BIND 9.4.2
Apache httpd 2.2.8 ((Ubuntu) DAV/2)
2 (RPC #100000)
              open
                       domain
              open
                       http
                       rpcbind
111/tcp
             open
                       netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp
              open
445/tcp
512/tcp open
                        exec?
513/tcp
                       login
                                          OpenBSD or Solaris rlogind
             open
                       tcpwrapped
514/tcp open
1099/tcp open
                       java-rmi GNU Classpath grmiregistry
bindshell Metasploitable root shell
1524/tcp open
2049/tcp open
2121/tcp open
                                           2-4 (RPC #100003)
                      ftp
                                           ProFTPD 1.3.1
MySQL 5.0.51a-3ubuntu5
3306/tcp open
                       mysql
5432/tcp open
5900/tcp open
                       postgresql PostgreSQL DB 8.3.0 - 8.3.7
6000/tcp open
                                           (access denied)
6667/tcp open
88009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:F2:31:C7 (Oracle 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 62.97 seconds
```

4) Version detection meta

```
root@ kali)-[/home/kali/Desktop
nmap -sV 192.168.178.125
Starting Nmap 7.945VN (https://nmap.org ) at 2024-01-10 10:37 EST Nmap scan report for 192.168.178.125 Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
                 open ftp
open ssh
                                                       vsftpd 2.3.4
21/tcp
                                                       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp
25/tcp
                                                      Linux telnetd
Postfix smtpd
                  open telnet
                  open smtp
open domain
 53/tcp
                                                       ISC BIND 9.4.2
80/tcp
111/tcp
                  open http
                                                     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
                 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
                                                      OpenBSD or Solaris rlogind
514/tcp open tcpwrapped
1099/tcp open java-rmi
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
VNC (protocol 3.3)
(access denied)
 514/tcp open
6000/tcp open X11
6667/tcp open irc
                                                      (access denied)
UnrealIRCd
8009/tcp open ajp13
8180/tcp open http
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:F2:31:C7 (Oracle 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 63.67 seconds
```

5) Os Windows 7

```
(root@ kali)-[/home/kali/Desktop]

# nmap -0 192.168.100.7

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 10:47 EST

Nmap scan report for 192.168.100.7

Host is up (0.00067s latency).

All 1000 scanned ports on 192.168.100.7 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:DA:3A:59 (Oracle VirtualBox virtual NIC)

Too many fingerprints match this host to give specific OS details

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 24.21 seconds
```

REPORT

In seguito ai risultati ottenuti dalle scansioni per metasploitable:

- L'indirizzo IP è 192.168.178.125
- Il sistema operativo è Linux 2.6
- Le porte aperte più critiche sono la 21 e la 23.
- La versione del servizio FTP è la 2.3.4 , la versione del servizio domain è alla 9.4.2 tutte le altre si possono visualizzare nel secondo, terzo e quarto screenshot

Su windows 7 non mi è stato possibile visualizzare la versione.