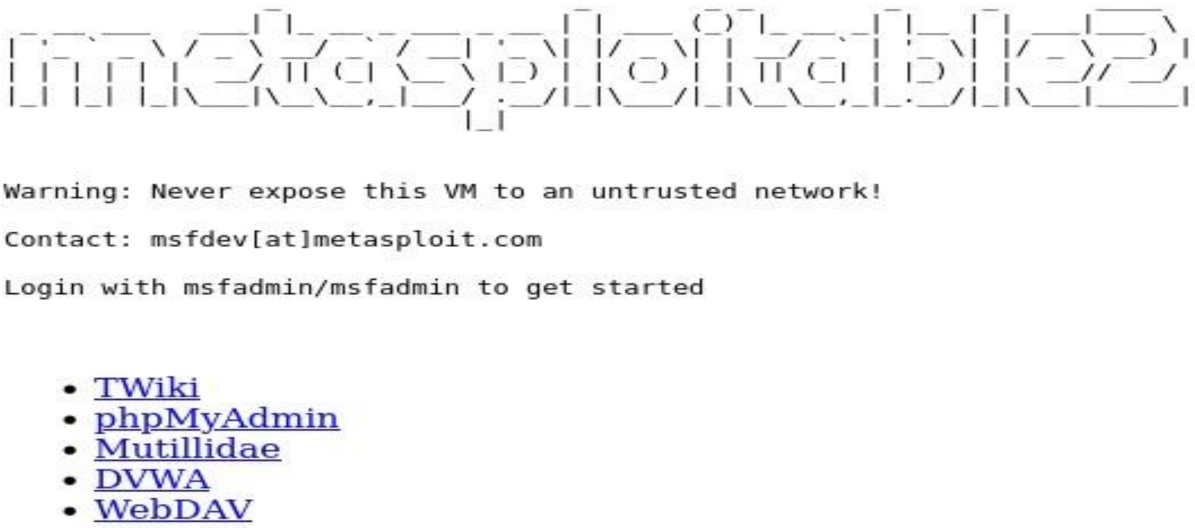
Relazione Tecniche di Scansione con Nmap (Metasploitable e Windows10)

1. Di seguito abbiamo l'immagine del nostro target, su cui andremo a fare varie operazioni di scanning con **Nmap**



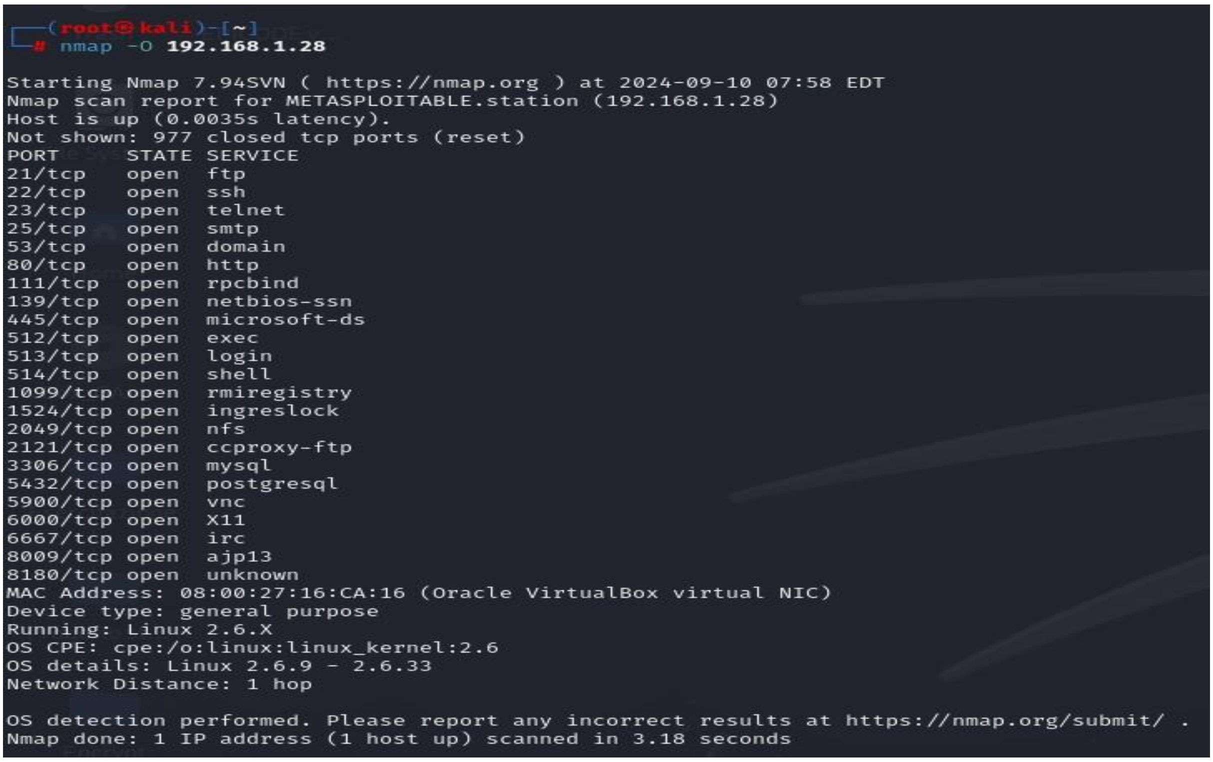
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

2. Nell'immagine seguente andiamo ad utilizzare **nmap** per rilevare l'**OS**:
   - **nmap -O 192.168.1.28**

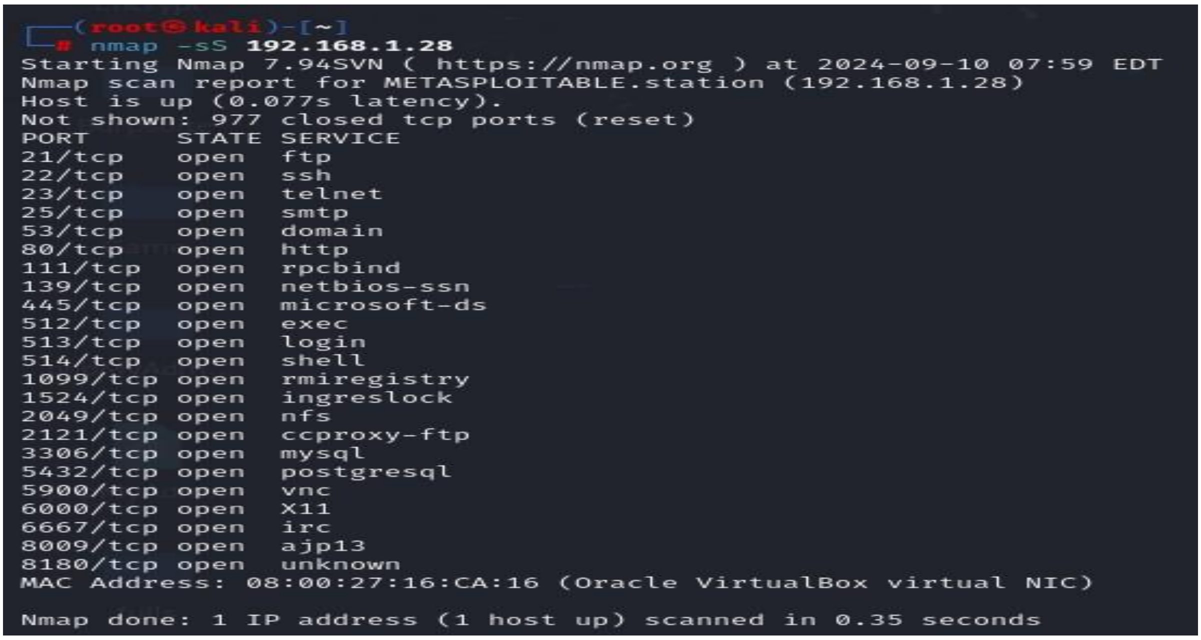


```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.1.28

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 07:58 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.28)
Host is up (0.0035s 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: 08:00:27:16:CA:16 (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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

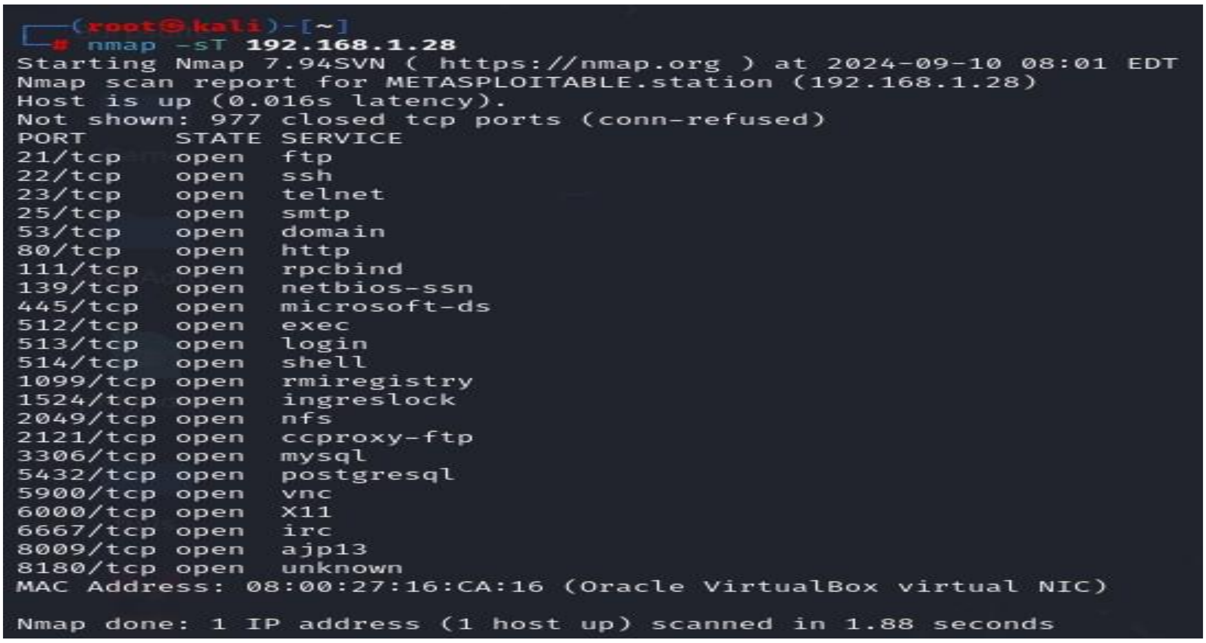
3. Nell’immagine seguente andiamo ad utilizzare **nmap** per la **SYN Scan**:
    - **nmap -sS 192.168.1.28**



```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.1.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 07:59 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.28)
Host is up (0.077s 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: 08:00:27:16:CA:16 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

4. Nell’immagine seguente andiamo ad utilizzare **nmap** per la **TCP Connect Scan**:
    - **nmap -sT 192.168.1.28**



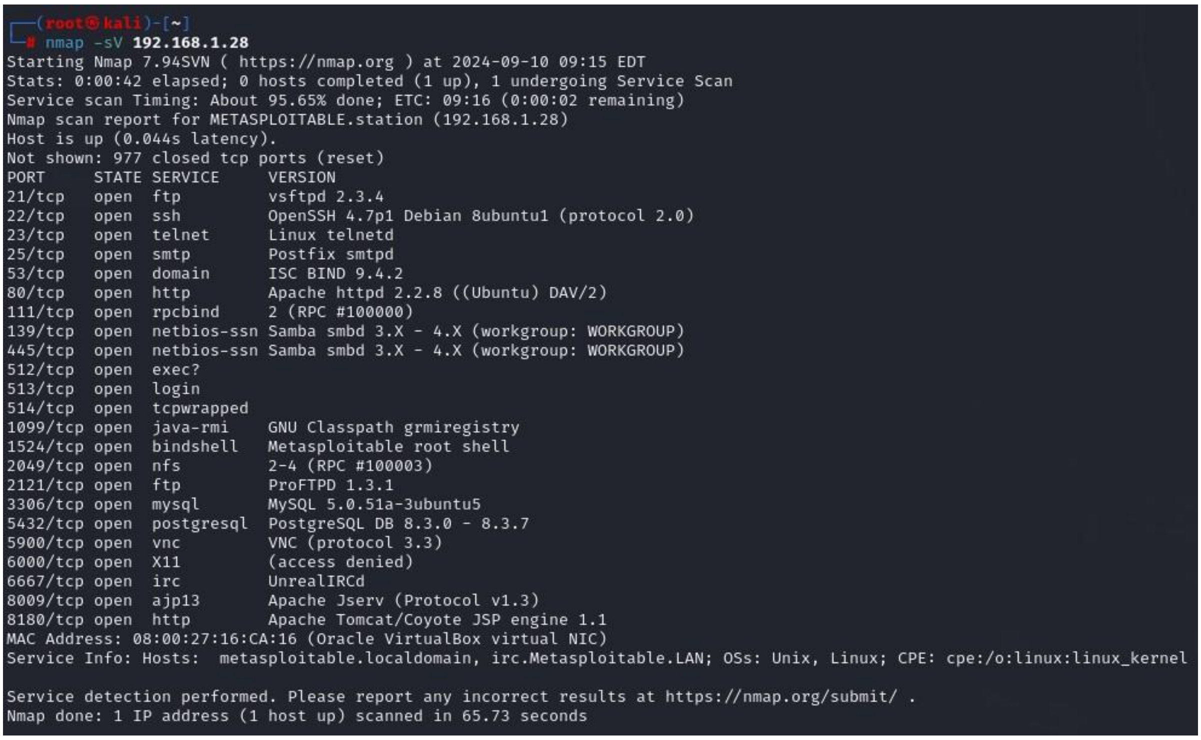
```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.1.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 08:01 EDT
Nmap scan report for METASPLOITABLE.station (192.168.1.28)
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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: 08:00:27:16:CA:16 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
```

- **Differenze tra SYN Scan e TCP Connect Scan**
    - la SYN Scan su riga di comando identificata con -sS, invia i pacchetti SYN, ma senza stabilire una connessione completa

    - la TCP Scan su riga di comando -sT, ha lo scopo di stabilire una connessione completa con una sequenza TCP, così da poter essere rilevata durante la visualizzazione dei log

5. Nell’immagine seguente andiamo ad utilizzare **nmap** per il **Version Detection dei servizi:**
   - **nmap -sV 192.168.1.28**

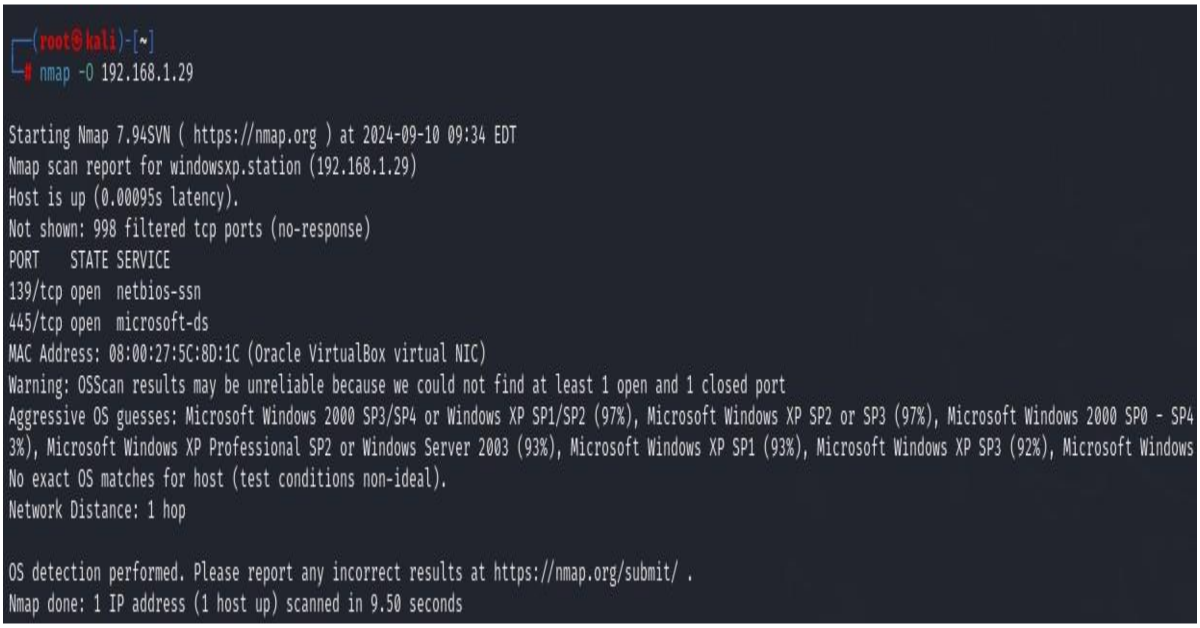


```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.1.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 09:15 EDT
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 09:16 (0:00:02 remaining)
Nmap scan report for METASPLOITABLE.station (192.168.1.28)
Host is up (0.044s 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?
513/tcp  open  login
514/tcp  open  tcpwrapped
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       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:16:CA:16 (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 65.73 seconds
```

Target Windows XP

- Nell’immagine seguente andiamo ad utilizzare **nmap** per rilevare l’**OS**
  - **nmap -O 192.168.1.29**



```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.1.29

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 09:34 EDT
Nmap scan report for windowsxp.station (192.168.1.29)
Host is up (0.00095s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4
3%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows XP SP3 (92%), Microsoft Windows
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 9.50 seconds
```