ESERCIZI SU NMAP:

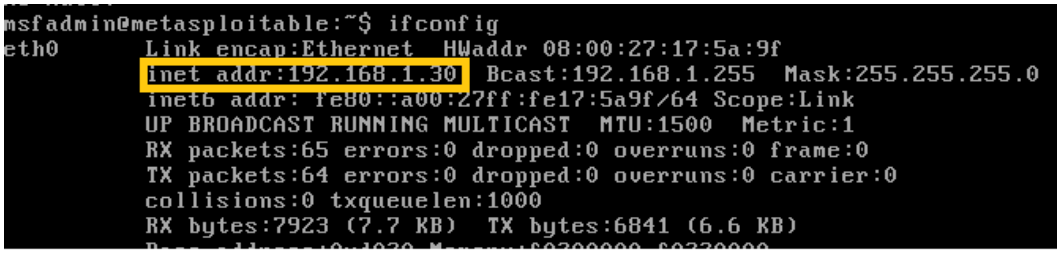
Nel compito di oggi dobbiamo ricavare delle informazioni di un target che in questo caso è Metasploitable.

La traccia chiede di fare diverse scansioni per sapere:

- Il sistema operativo che usa il nostro target
- Fare una scansione delle porte aperte
- Fare una scansione completa del tcp
- Fare una scansione dei servizi in esecuzione e quali sono le loro versioni

Come prima cosa abbiamo bisogno di conoscere l'indirizzo IP del nostro target che è Metaploitable, quindi apriamo la nostra macchina virtuale, facciamo login con le credenziali e diamo il comando "ifconfig" per trovare il nostro IP.

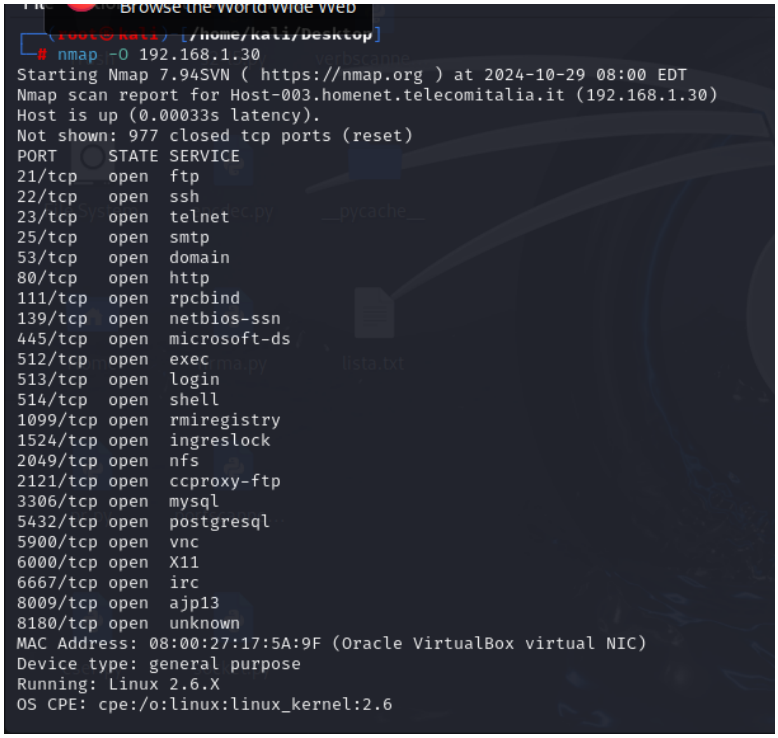
Come vediamo nell'immagine sottostante il nostro indirizzo IP è 192.168.1.30



Adesso che abbiamo l'indirizzo IP del target, apriamo un terminale su Kali, ci impostiamo come Root con il comando "sudo su" inserendo la password, e cominciamo con i comandi richiesti:

SISTEMA OPERATIVO:

Per sapere qual è il sistema operativo che utilizza il nostro target il comando è "nmap -O" seguito dall'indirizzo IP, quindi: "nmap -O 192.168.1.30" e come possiamo vedere in output dice che il nostro target utilizza un sistema operativo in base linux con annessa la versione.

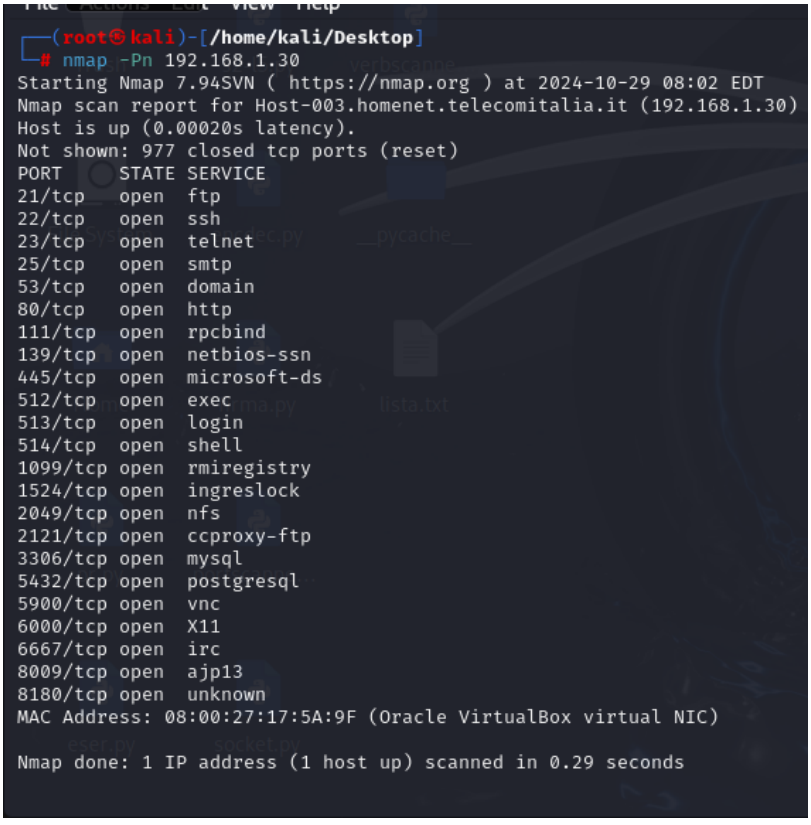


SYN SCAN:

Come seconda richiesta dobbiamo vedere sul nostro target quali porte di quali servizi sono aperte.

Il comando nmap di default chiede nel pacchetto il ping (connettività tra due host) e il SYN (scansione delle porte), quindi per ottenere in output solo la scansione delle porte togliamo dal comando il ping: “nmap -Pn 192.168.1.30” e questo è il nostro risultato scansionando in automatico le 1024 porte di servizi noti.

Come possiamo vedere ci sono 977 porte chiuse e 47 aperte con il servizio a loro riferito.



TCP CONNECT:

Come terza richiesta dobbiamo fare una scansione completa del protocollo di trasporto tcp. Per farlo il comando è “nmap -sT 192.168.1.30” dove anche qui possiamo vedere nello specifico i servizi in esecuzione delle porte aperte.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sT 192.168.1.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:02 EDT
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.30)
Host is up (0.00094s 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: 08:00:27:17:5A:9F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

VERSIONE SERVIZI:

Come ultima richiesta dobbiamo fare una scansione dei servizi in esecuzione con la versione di ognuno di loro, per farlo eseguiamo il comando “nmap -sV 192.168.1.30”

```
File  Actions  Edit  View  Help
└─# nmap -sV 192.168.1.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 08:03 EDT
Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.30)
Host is up (0.00032s 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       OpenBSD or Solaris rlogind
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: 08:00:27:17:5A:9F (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 63.37 seconds
```

Facendo una scansione dettagliata delle porte possiamo renderci conto, a seconda dei protocolli corrispondenti, quali possono essere le vulnerabilità del caso, i protocolli poco sicuri etc. Etc.