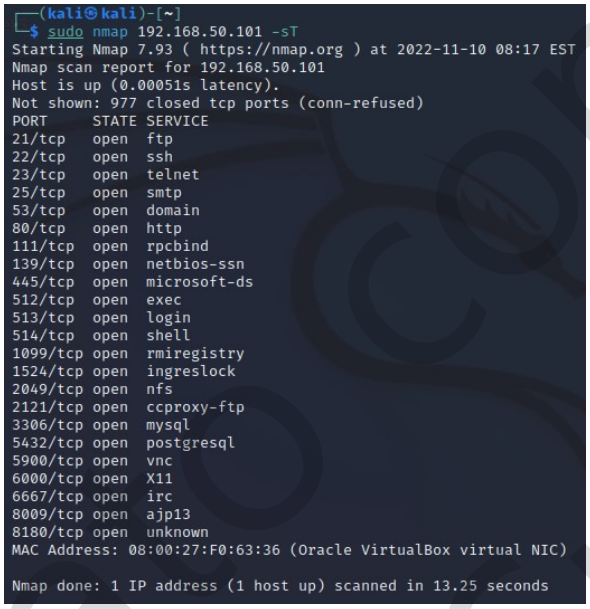
Claudio De cicco
10/12/2022

Report Nmap

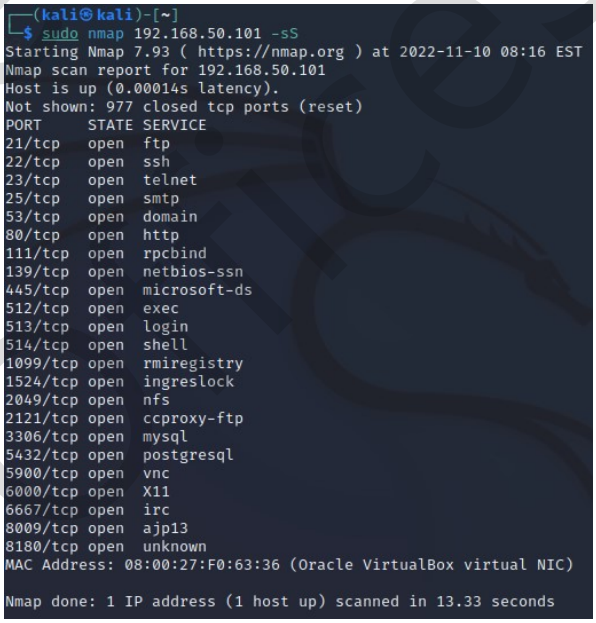
1-Scansione -sT

Come prima richiesta vado ad effettuare una scansione nmap sull'ip di metasploitable con -sT . Come risultato avrò una lista delle porte TCP aperte



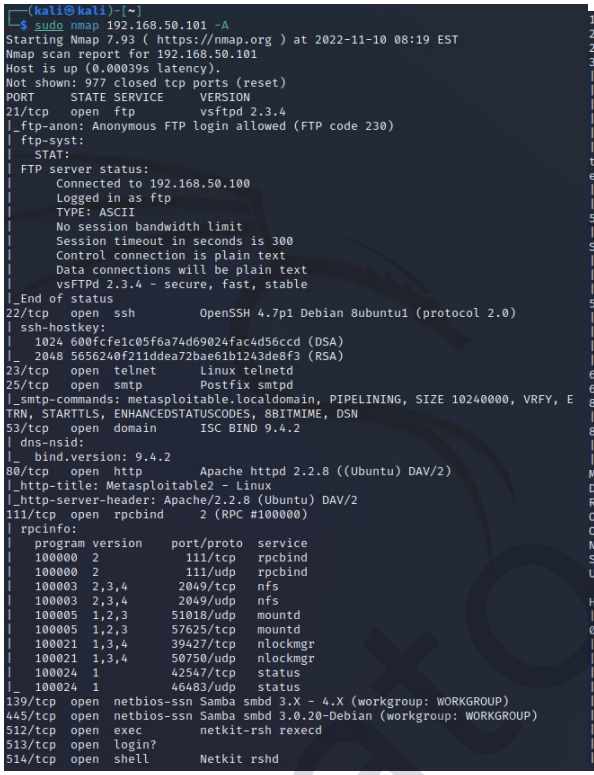
2-Scansione -sS

Come seconda richiesta faccio la scansione nmap sempre sull'ip di meta con -sS.



3-Scansione -A

Come terza richiesta faccio la stessa scansione ma con -A che abilita il rilevamento del sistema operativo, il rilevamento della versione, la scansione degli script e il traceroute



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.101 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-10 08:19 EST
Nmap scan report for 192.168.50.101
Host is up (0.00039s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, E
TRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      51018/udp   mountd
|   100005  1,2,3      57625/tcp   mountd
|   100021  1,3,4      39427/tcp   nlockmgr
|   100021  1,3,4      50750/udp   nlockmgr
|   100024  1          42547/tcp   status
|_  100024  1          46483/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: LongColumnFlag, Support41Auth, SupportsTransactions, Swi
tchToSSLAfterHandshake, ConnectWithDatabase, Speaks41ProtocolNew, SupportsCompr
ession
|   Status: Autocommit
|_  Salt: T6NhAJ0R+!aG-fb96B,P
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCO
SA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2022-11-10T13:21:40+00:00; -1s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:F0:63:36 (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

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 0
00000000000 (Xerox)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
```

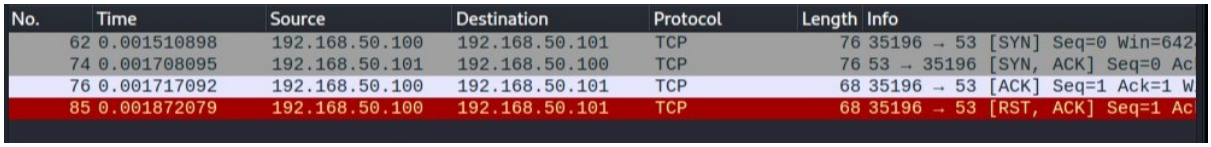
```
TRACEROUTE
HOP RTT      ADDRESS
1   0.39 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.85 seconds
```

4-Evidenziare differenza tra TCP(-sT) e SYN(-sS)

Ho effettuando la scansione con Wireshark e andando a filtrare una porta specifica vado a vedere le differenze.

No.	Time	Source	Destination	Protocol	Length	Info
27	13.100747177	192.168.50.100	192.168.50…	TCP	60	33716 → 53 [SYN] Seq=0 Wi
35	13.100883526	192.168.50.101	192.168.50…	TCP	62	53 → 33716 [SYN, ACK] Seq
37	13.100905986	192.168.50.100	192.168.50…	TCP	56	33716 → 53 [RST] Seq=1 Wi

In questa prima foto la scansione SYN e vediamo come una volta ricevuto il pacchetto SYN/ACK capisce che la porta è aperta chiude la comunicazione con un RST(reset).



No.	Time	Source	Destination	Protocol	Length	Info
62	0.001510898	192.168.50.100	192.168.50.101	TCP	76	35196 → 53 [SYN] Seq=0 Win=642
74	0.001708095	192.168.50.101	192.168.50.100	TCP	76	53 → 35196 [SYN, ACK] Seq=0 Ac
76	0.001717092	192.168.50.100	192.168.50.101	TCP	68	35196 → 53 [ACK] Seq=1 Ack=1 W
85	0.001872079	192.168.50.100	192.168.50.101	TCP	68	35196 → 53 [RST, ACK] Seq=1 Ac

In questa seconda foto invece con la scansione TCP(-sT), vediamo come a differenza della scansione SYN ,nmap completa il 3-way-handshake creando cosi il canale.

5-Tabella con i risultati delle scan

Fonte dello scan	Destinazione	Tipo di scan	Risultati
Linux 192.168.50.100	Meta 192.168.50.101	-sT	12 servizi attivi per le porte well know
Linux 192.168.50.100	Meta 192.168.50.101	-sS	12 servizi attivi per le porte well know
Linux 192.168.50.100	Meta 192.168.50.101	-A	12 servizi attivi per le porte well know