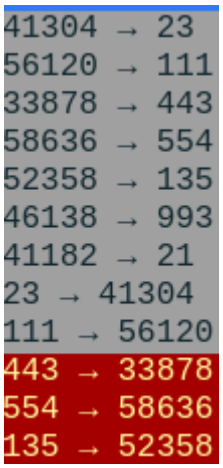
CONSEGNA U3 S9 L3

Per prima cosa, dalla scansione effettuata tramite **Wireshark**, si evince che la comunicazione avviene sempre e solo tra questi due indirizzi IP **(192.168.200.100 – 192.168.200.150).**

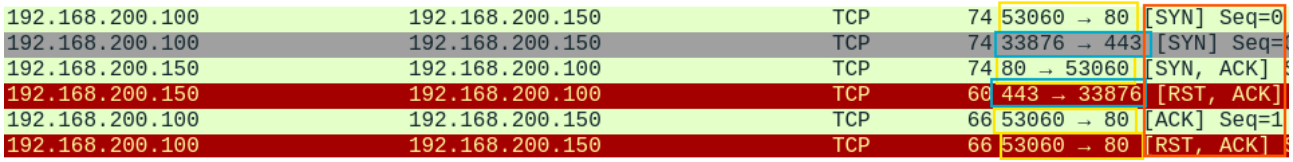
192.168.200.150	192.168.200.255
192.168.200.100	192.168.200.150
192.168.200.100	192.168.200.150
192.168.200.150	192.168.200.100
192.168.200.150	192.168.200.100
192.168.200.100	192.168.200.150
192.168.200.100	192.168.200.150

Si evince anche che una delle due macchine tenta di connettersi a differenti porte dell'altra. Alcune connessioni vanno a buon fine ed altre, invece, vengono terminate o rifiutate.

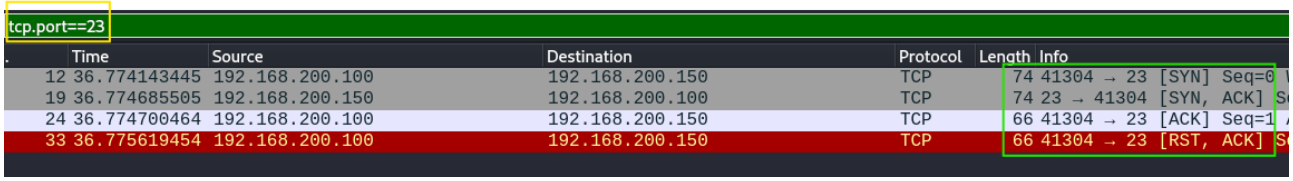


Analizziamo qualche esempio nel dettaglio. La macchina all'IP **192.168.200.100** tenta di avviare una connessione all'IP **192.168.200.150** verso la **porta 80 (HTTP)** tramite una richiesta **SYN**. La macchina ricevente risponde accettando di eseguire la connessione tramite una **SYN-ACK**. Quindi viene creata la connessione tra l'IP **192.168.200.100**, che risponde con un **ACK** finale alla macchina sull'IP **192.168.200.150**; la connessione sulla **porta 80** è avvenuta con successo. Poi subito la connessione viene chiusa dalla stessa macchina che inizialmente l'aveva richiesta, ovvero la macchina all'IP **192.168.200.100,** tramite un pacchetto **RST-ACK**.

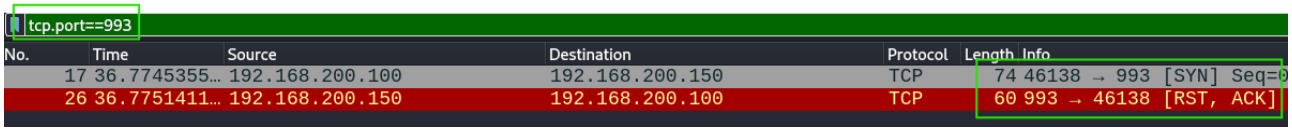
Da notare invece, che la connessione richiesta dalla macchina sul **192.168.200.100** alla macchina sul **192.168.200.150** verso la **porta 443 (HTTPS)** viene subito rifiutata tramite un pacchetto **RST-ACK**.



Analizziamo un comportamento simile su altre due richieste di connessione della macchina sul **192.168.200.100** alla macchina sul **192.168.200.150** verso la **porta 23 (TELNET)**. In questo caso, la connessione viene stabilita correttamente dopo che le due macchine hanno effettuato il **Three Way Handshake**. Quindi, sempre la macchina richiedente, tramite una richiesta **RST-ACK**, va a chiudere la stessa connessione.



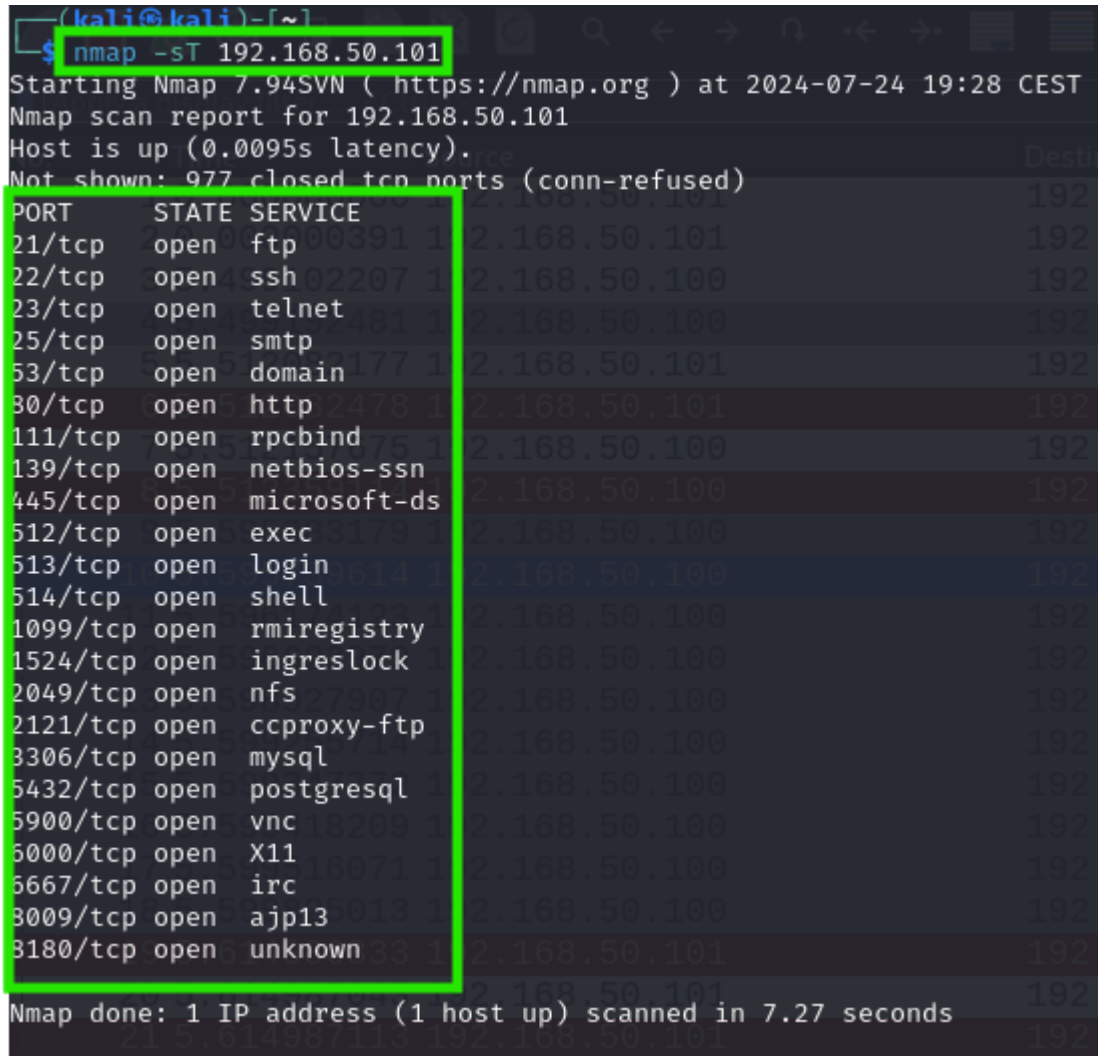
Quando la macchina **(192.168.200.100)** tenta una connessione alla **porta 993 (IMAP4)** della seconda macchina **(192.168.200.150)** la connessione viene subito rifiutata con un **RST-ACK**.

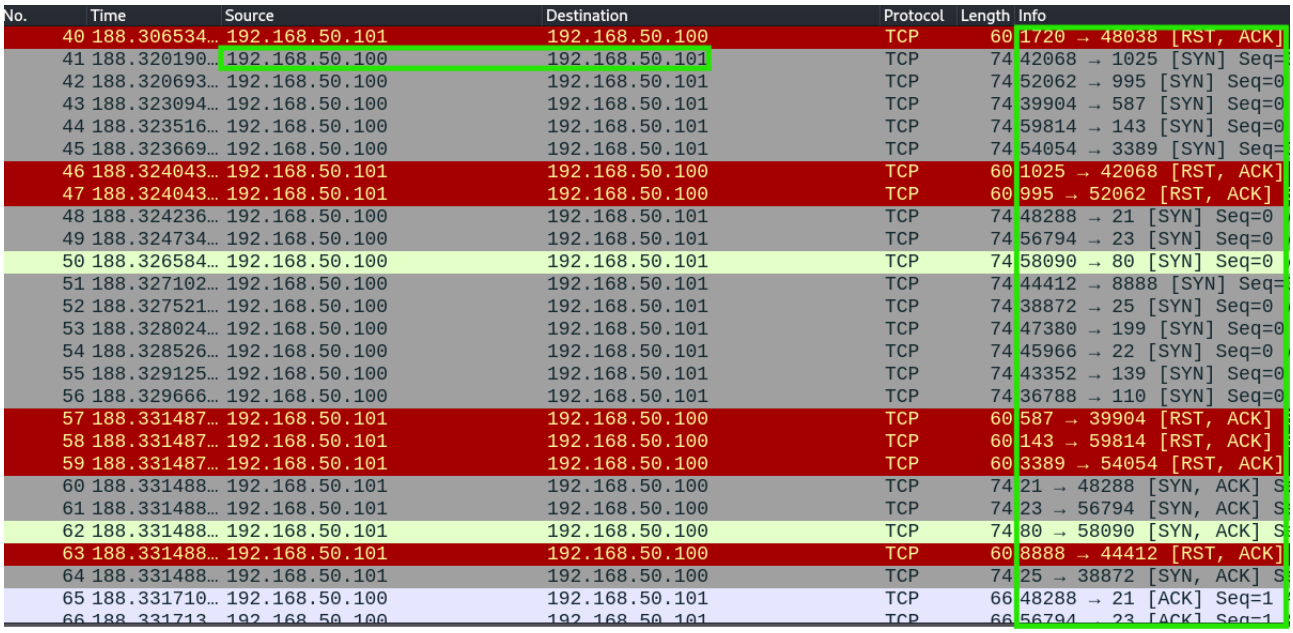


Conclusioni

Dopo aver analizzato accuratamente il traffico di rete tra le due macchine, la mia deduzione è che si tratti di una scansione delle porte attive sulla macchina target all'IP **192.168.200.150**. Probabilmente una scansione delle porte attive tramite un comando del tipo **nmap -sT** o di tipo **nmap -sV**, dato che una scansione di questo tipo va ad aprire una effettiva connessione tra le macchine tramite il completamento del **Three Way Handshake (SYN, SYN-ACK, ACK).** Laddove la porta invece è chiusa, la connessione tra le due macchine non avviene. Ciò si nota dalla richiesta **RST-ACK** che fa la macchina richiedente all'IP **192.168.200.100** verso la macchina target all'IP **192.168.200.150**.

Avviando un port scanner con il comando **nmap -sT** dalla macchina Kali **(192.168.50.100)** alla Metasploitable **(192.168.50.101)** e analizzando il traffico tramite **Wireshark**, si nota un risultato molto simile.





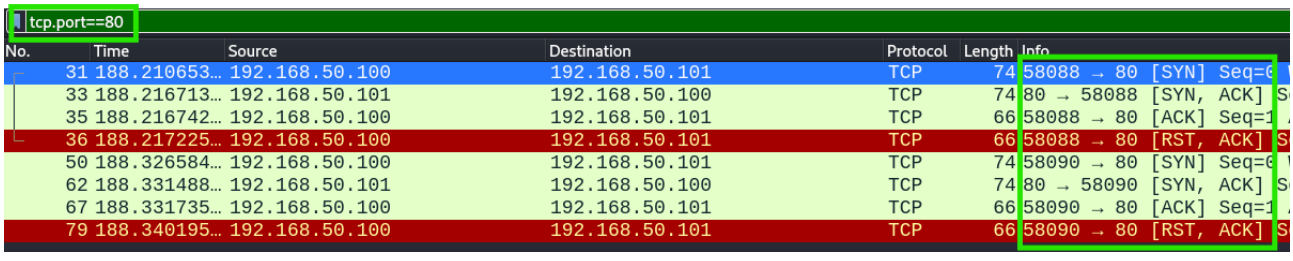
No.	Time	Source	Destination	Protocol	Length	Info
40	188.306534…	192.168.50.101	192.168.50.100	TCP	60	1720 → 48038 [RST, ACK]
41	188.320190…	192.168.50.100	192.168.50.101	TCP	74	42068 → 1025 [SYN] Seq=
42	188.320693…	192.168.50.100	192.168.50.101	TCP	74	52062 → 995 [SYN] Seq=0
43	188.323094…	192.168.50.100	192.168.50.101	TCP	74	39904 → 587 [SYN] Seq=0
44	188.323516…	192.168.50.100	192.168.50.101	TCP	74	59814 → 143 [SYN] Seq=0
45	188.323669…	192.168.50.100	192.168.50.101	TCP	74	54054 → 3389 [SYN] Seq=
46	188.324043…	192.168.50.101	192.168.50.100	TCP	60	1025 → 42068 [RST, ACK]
47	188.324043…	192.168.50.101	192.168.50.100	TCP	60	995 → 52062 [RST, ACK]
48	188.324236…	192.168.50.100	192.168.50.101	TCP	74	48288 → 21 [SYN] Seq=0
49	188.324734…	192.168.50.100	192.168.50.101	TCP	74	56794 → 23 [SYN] Seq=0
50	188.326584…	192.168.50.100	192.168.50.101	TCP	74	58090 → 80 [SYN] Seq=0
51	188.327102…	192.168.50.100	192.168.50.101	TCP	74	44412 → 8888 [SYN] Seq=
52	188.327521…	192.168.50.100	192.168.50.101	TCP	74	38872 → 25 [SYN] Seq=0
53	188.328024…	192.168.50.100	192.168.50.101	TCP	74	47380 → 199 [SYN] Seq=0
54	188.328526…	192.168.50.100	192.168.50.101	TCP	74	45966 → 22 [SYN] Seq=0
55	188.329125…	192.168.50.100	192.168.50.101	TCP	74	43352 → 139 [SYN] Seq=0
56	188.329666…	192.168.50.100	192.168.50.101	TCP	74	36788 → 110 [SYN] Seq=0
57	188.331487…	192.168.50.101	192.168.50.100	TCP	60	587 → 39904 [RST, ACK]
58	188.331487…	192.168.50.101	192.168.50.100	TCP	60	143 → 59814 [RST, ACK]
59	188.331487…	192.168.50.101	192.168.50.100	TCP	60	3389 → 54054 [RST, ACK]
60	188.331488…	192.168.50.101	192.168.50.100	TCP	74	21 → 48288 [SYN, ACK] S
61	188.331488…	192.168.50.101	192.168.50.100	TCP	74	23 → 56794 [SYN, ACK] S
62	188.331488…	192.168.50.101	192.168.50.100	TCP	74	80 → 58090 [SYN, ACK] S
63	188.331488…	192.168.50.101	192.168.50.100	TCP	60	8888 → 44412 [RST, ACK]
64	188.331488…	192.168.50.101	192.168.50.100	TCP	74	25 → 38872 [SYN, ACK] S
65	188.331710…	192.168.50.100	192.168.50.101	TCP	66	48288 → 21 [ACK] Seq=1
66	188.331713…	192.168.50.100	192.168.50.101	TCP	66	56794 → 23 [ACK] Seq=1

In questo caso la connessione dalla Kali alla Meta sulla **porta 443 (HTTPS)** è stata rifiutata.

tcp.port==443

No.	Time	Source	Destination	Protocol	Length	Info
32	188.210731…	192.168.50.100	192.168.50.101	TCP	74	38534 → 443 [SYN] Seq=
34	188.216713…	192.168.50.101	192.168.50.100	TCP	60	443 → 38534 [RST, ACK]
90	188.346731…	192.168.50.100	192.168.50.101	TCP	74	38548 → 443 [SYN] Seq=
120	188.476939…	192.168.50.101	192.168.50.100	TCP	60	443 → 38548 [RST, ACK]

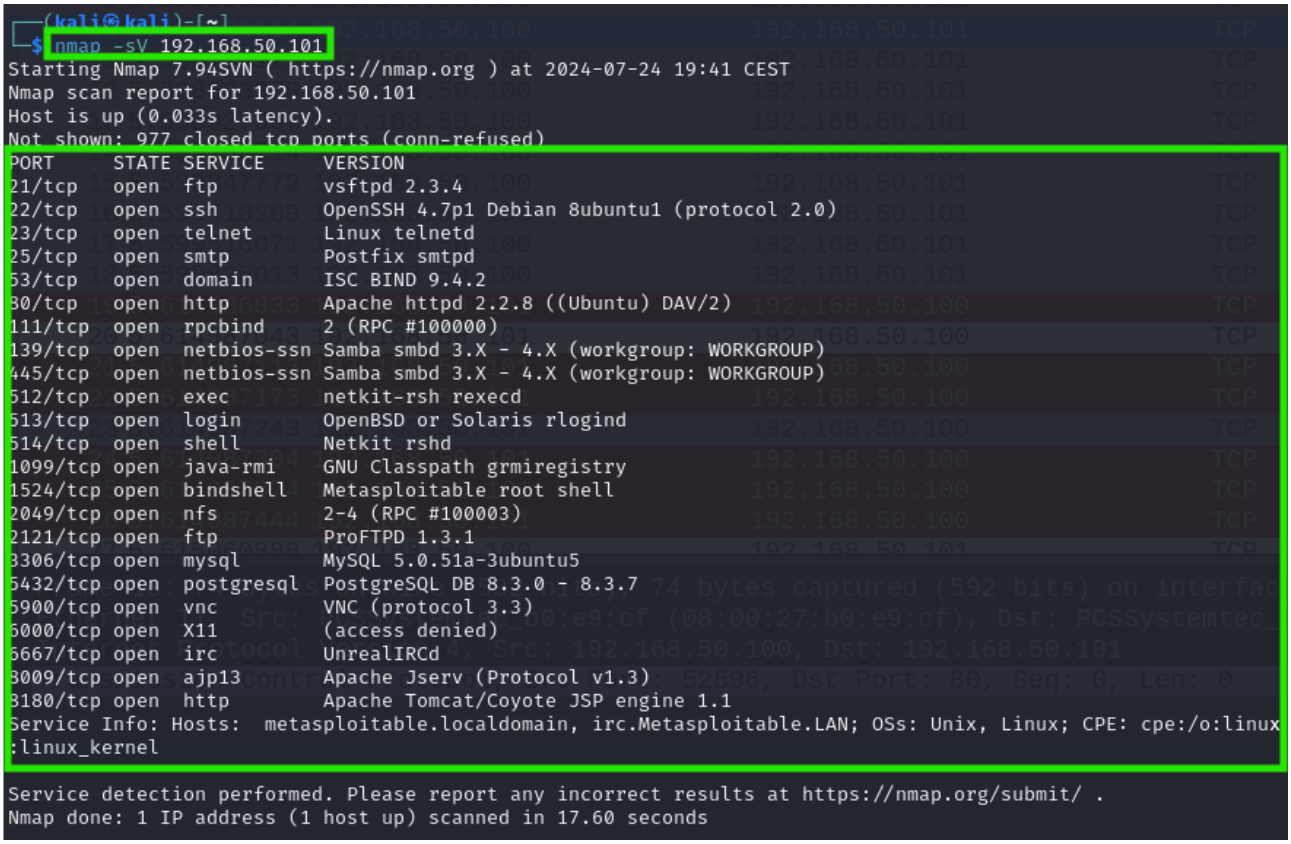
Mentre la connessione viene avviata per ben due volte con successo e poi interrotta, sulla **porta 80 (HTTP)** sempre dalla Kali verso la Metasploitable.



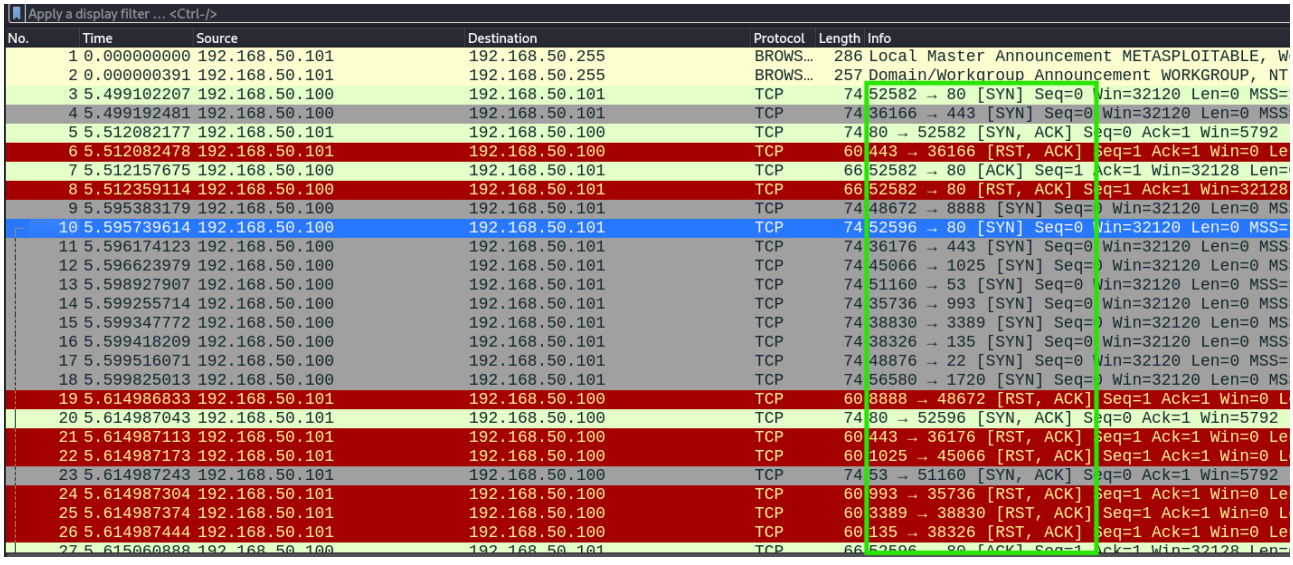
tcp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
31	188.210653…	192.168.50.100	192.168.50.101	TCP	74	58088 → 80 [SYN] Seq=0
33	188.216713…	192.168.50.101	192.168.50.100	TCP	74	80 → 58088 [SYN, ACK] S
35	188.216742…	192.168.50.100	192.168.50.101	TCP	66	58088 → 80 [ACK] Seq=1
36	188.217225…	192.168.50.100	192.168.50.101	TCP	66	58088 → 80 [RST, ACK] S
50	188.326584…	192.168.50.100	192.168.50.101	TCP	74	58090 → 80 [SYN] Seq=0
62	188.331488…	192.168.50.101	192.168.50.100	TCP	74	80 → 58090 [SYN, ACK] S
67	188.331735…	192.168.50.100	192.168.50.101	TCP	66	58090 → 80 [ACK] Seq=1
79	188.340195…	192.168.50.100	192.168.50.101	TCP	66	58090 → 80 [RST, ACK] S

Eseguendo invece una scansione sulle porte col comando **nmap -sV** la situazione è leggermente differente, dato che oltre ai tentativi di connessione tra le due macchine completando il **TWH**, c'è uno scambio di pacchetti per la comunicazione del banner dei servizi che risultano attivi sulle porte della macchina Metasploitable.



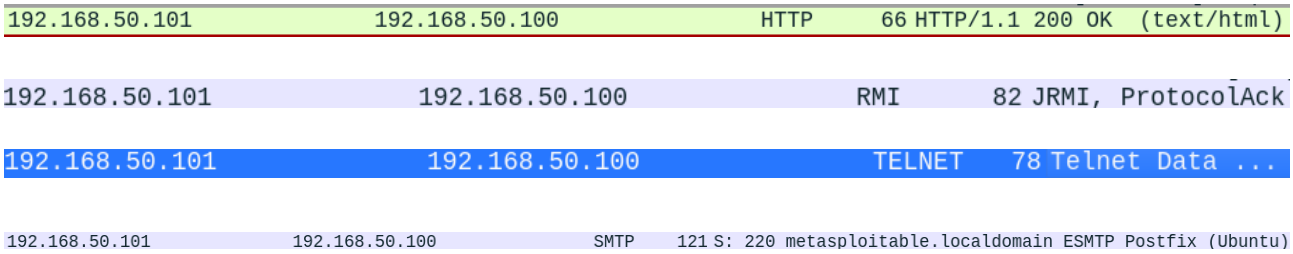
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 19:41 CEST
Nmap scan report for 192.168.50.101
Host is up (0.033s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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
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 17.60 seconds
```



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.101	192.168.50.255	BROWS…	286	Local Master Announcement METASPLOITABLE, W
2	0.000000391	192.168.50.101	192.168.50.255	BROWS…	257	Domain/Workgroup Announcement WORKGROUP, NT
3	5.499102207	192.168.50.100	192.168.50.101	TCP	74	52582 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=
4	5.499192481	192.168.50.100	192.168.50.101	TCP	74	36166 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS
5	5.512082177	192.168.50.101	192.168.50.100	TCP	74	80 → 52582 [SYN, ACK] Seq=0 Ack=1 Win=5792
6	5.512082478	192.168.50.101	192.168.50.100	TCP	60	443 → 36166 [RST, ACK] Seq=1 Ack=1 Win=0 Le
7	5.512157675	192.168.50.100	192.168.50.101	TCP	66	52582 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=
8	5.512359114	192.168.50.100	192.168.50.101	TCP	66	52582 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128
9	5.595383179	192.168.50.100	192.168.50.101	TCP	74	48672 → 8888 [SYN] Seq=0 Win=32120 Len=0 MS
10	5.595739614	192.168.50.100	192.168.50.101	TCP	74	52596 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=
11	5.596174123	192.168.50.100	192.168.50.101	TCP	74	36176 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS
12	5.596623979	192.168.50.100	192.168.50.101	TCP	74	45066 → 1025 [SYN] Seq=0 Win=32120 Len=0 MS
13	5.598927907	192.168.50.100	192.168.50.101	TCP	74	51160 → 53 [SYN] Seq=0 Win=32120 Len=0 MSS=
14	5.599255714	192.168.50.100	192.168.50.101	TCP	74	35736 → 993 [SYN] Seq=0 Win=32120 Len=0 MSS
15	5.599347772	192.168.50.100	192.168.50.101	TCP	74	38830 → 3389 [SYN] Seq=0 Win=32120 Len=0 MS
16	5.599418209	192.168.50.100	192.168.50.101	TCP	74	38326 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS
17	5.599516071	192.168.50.100	192.168.50.101	TCP	74	48876 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=
18	5.599825013	192.168.50.100	192.168.50.101	TCP	74	56580 → 1720 [SYN] Seq=0 Win=32120 Len=0 MS
19	5.614986833	192.168.50.101	192.168.50.100	TCP	60	8888 → 48672 [RST, ACK] Seq=1 Ack=1 Win=0 L
20	5.614987043	192.168.50.101	192.168.50.100	TCP	74	80 → 52596 [SYN, ACK] Seq=0 Ack=1 Win=5792
21	5.614987113	192.168.50.101	192.168.50.100	TCP	60	443 → 36176 [RST, ACK] Seq=1 Ack=1 Win=0 Le
22	5.614987173	192.168.50.101	192.168.50.100	TCP	60	1025 → 45066 [RST, ACK] Seq=1 Ack=1 Win=0 L
23	5.614987243	192.168.50.101	192.168.50.100	TCP	74	53 → 51160 [SYN, ACK] Seq=0 Ack=1 Win=5792
24	5.614987304	192.168.50.101	192.168.50.100	TCP	60	993 → 35736 [RST, ACK] Seq=1 Ack=1 Win=0 Le
25	5.614987374	192.168.50.101	192.168.50.100	TCP	60	3389 → 38830 [RST, ACK] Seq=1 Ack=1 Win=0 L
26	5.614987444	192.168.50.101	192.168.50.100	TCP	60	135 → 38326 [RST, ACK] Seq=1 Ack=1 Win=0 Le
27	5.615060888	192.168.50.100	192.168.50.101	TCP	66	52596 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=

Qui si vedono infatti le informazioni che condivide la macchina Metasploitable verso la macchina Kali per l'elenco dei vari servizi attivi sulle porte.



Remediation Actions

Il consiglio che mi sento di dare in questi casi, è di rendere le porte non strettamente necessarie, irraggiungibili dall'esterno, tramite la configurazione di policy dedicate su un firewall. Sicuramente chi avrà condotto questo port scanning, starà probabilmente eseguendo dei controlli sulle possibili vulnerabilità della macchina per poi, dopo opportuno studio, sferrare un attacco.