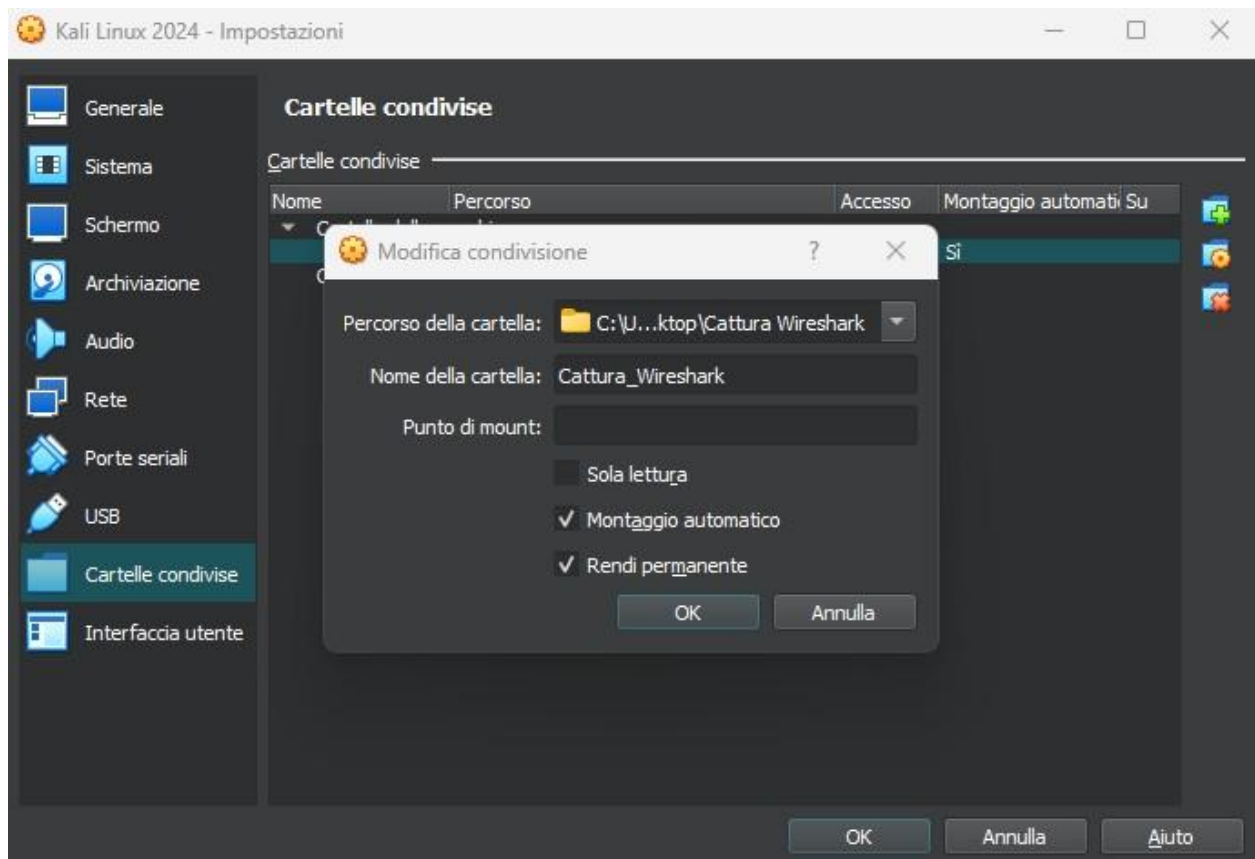


Relazione Threat Intelligence & IOC

Come richiesto dalla traccia dobbiamo:

- ✚ Identificare ed analizzare eventuali IOC, evidenze di attacchi in corso
- ✚ Ipotesi sui potenziali vettori di attacco utilizzati
- ✚ Consigliare un'azione per ridurre l'impatto e/o gli impatti dell'attacco in corso ed eventualmente attacco futuro

Nella seguente immagine creo la cartella condivisa, dal mio Host alla macchina sulla quale devo effettuare le prossime operazioni, andando sulle impostazioni della macchina Kali Linux, sulla scheda “**Cartelle condivise**”.



Nella seguente immagine e passaggio illustrato, per procedere con la visualizzazione e lo spostamento del file **Cattura_U3_W1_L3.pcapng** da “media” al mio “Desktop” Kali, devo prendere i privilegi di root, e di conseguenza utilizzo il comando **sudo -s**

- **sudo -s**: ottengo i privilegi di root
- **cd /media**: mi sposto nella cartella “media”
- **ls**: vedo la lista degli elementi all’interno della cartella “media”
- **cd**: mi sposto nella cartella sf_Cattura_Wireshark
- **ls**: vedo l’elemento all’interno della cartella sf_Cattura_Wireshark

```
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
(kali㉿kali)-[~]
# cd /media

(kali㉿kali)-[/media]
# ls
sf_Cattura_Wireshark

(kali㉿kali)-[/media]
# cd sf_Cattura_Wireshark

(kali㉿kali)-[/media/sf_Cattura_Wireshark]
# ls
Cattura_U3_W1_L3.pcapng

(kali㉿kali)-[/media/sf_Cattura_Wireshark]
#
```

Per verificare che la cartella sia effettivamente all’interno di “sf_Cattura_Wireshark”:

- **ls -la**: vedo la lista degli elementi con i vari permessi (root) nella cartella sf_Cattura_Wireshark
- con il comando **chmod ugo+rw**, modifico i permessi del file o di una directory, e con **rw** aggiungo i permessi per la lettura e la scrittura del file

```
(kali㉿kali)-[/media/sf_Cattura_Wireshark]
# ls -la
total 212
drwxrwx--- 1 root vboxsf    0 Oct 11 04:09 .
drwxr-xr-x 3 root root    4096 Oct 11 04:10 ..
-rwxrwx--- 1 root vboxsf 209024 Oct 11 03:09 Cattura_U3_W1_L3.pcapng

(kali㉿kali)-[/media/sf_Cattura_Wireshark]
# mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop

(kali㉿kali)-[/media/sf_Cattura_Wireshark]
# cd /home/kali/Desktop

(kali㉿kali)-[/home/kali/Desktop]
# chmod ugo+rw Cattura_U3_W1_L3.pcapng

(kali㉿kali)-[/home/kali/Desktop]
# chown kali Cattura_U3_W1_L3.pcapng

(kali㉿kali)-[~kali/Desktop]
#
```

Dati principali:

IP attaccante: 192.168.200.100

IP vittima: 192.168.200.150

Nella seguente immagine possiamo notare un numero elevato di pacchetti con protocollo in **TCP RST/ACK** e **SYN**:

- **SYN**: tentativo di iniziare una connessione TCP verso una porta specifica.
- **RST/ACK (Reset/Acknowledge)**: una risposta che indica che la connessione è stata rifiutata o terminata forzatamente.

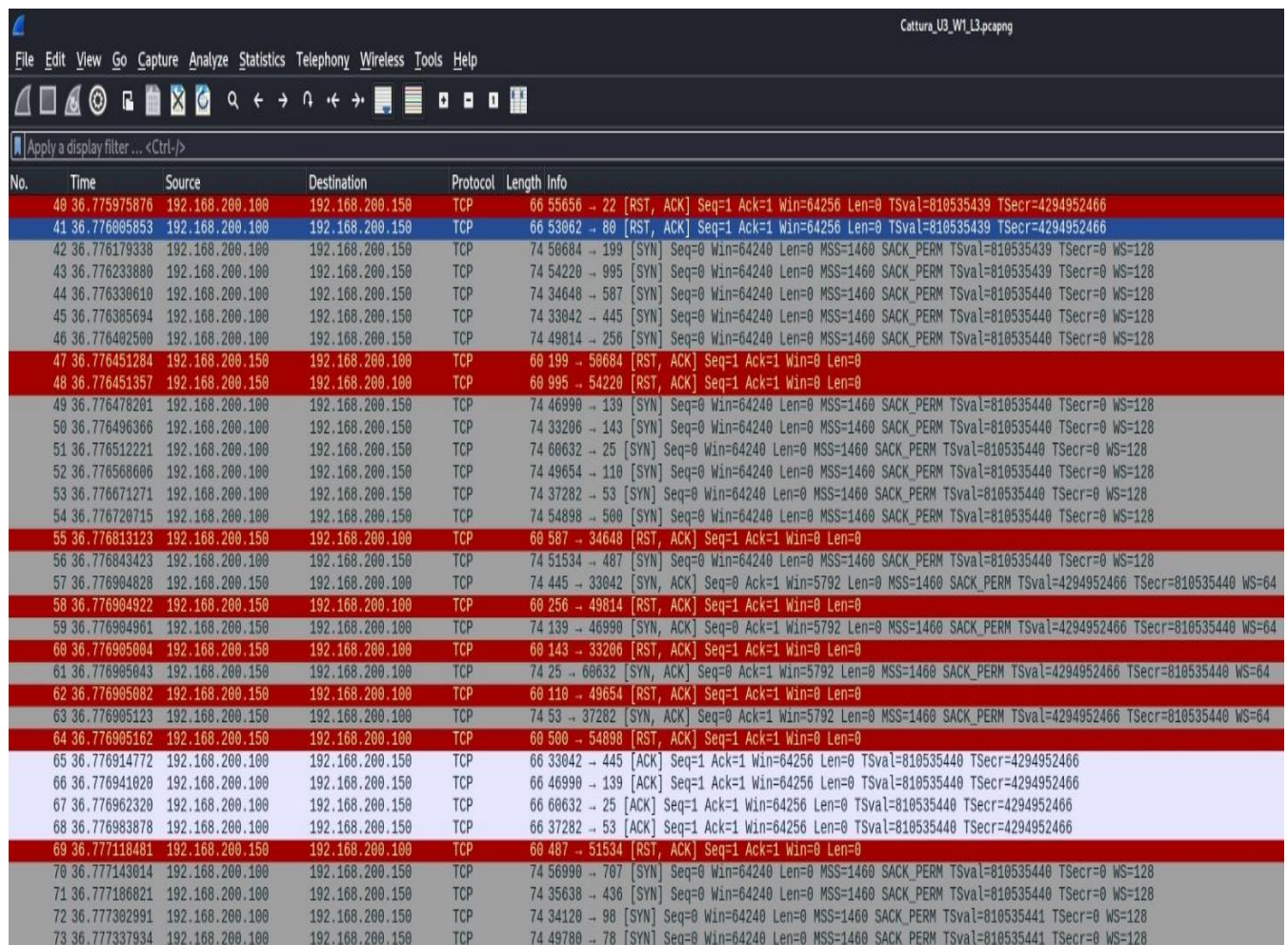
L'attaccante con questo tentativo di connessione, cerca di scoprire le porte aperte sul quale poter agire, in caso di esito negativo e quindi di **connection refused**, il sistema RST/ACK, interrompe il tentativo di connessione da parte dell'attaccante:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.100	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899891	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629451	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_fd:87:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775238099	PCSSystemtec_fd:87:...	PCSSystemtec_39:7d:...	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56128 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366395	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774495627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685595	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56128 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774788464	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711872	192.168.200.100	192.168.200.150	TCP	66	56128 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174848	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775378880	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524284	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589896	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56128 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Nella seguente immagine possiamo notare delle connessioni su specifiche porte, comunemente conosciute:

- **Porta 445 - SMB Serve Message Block:** viene utilizzata per la condivisione di file e per risorse di rete su sistemi Windows.
- **Porta 139 - NetBIOS:** utilizzata per il supporto delle funzioni di rete su Windows.

l'attaccante con questo tipo connessione alle porte comuni cerca identificare e cerca le vulnerabilità da poter sfruttare nel protocollo **Server Message Block**, come ad esempio un l'exploit conosciuto con il nome di **EternalBlue**.



The image shows a Wireshark network capture titled "Cattura_U3_W1_L3.pcapng". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a display filter set to "Apply a display filter ... <Ctrl-/>". The packet list pane shows 73 captured packets. The selected packet is number 69, a TCP RST, ACK from 192.168.200.100 to 192.168.200.150. The packet details pane shows the following information:

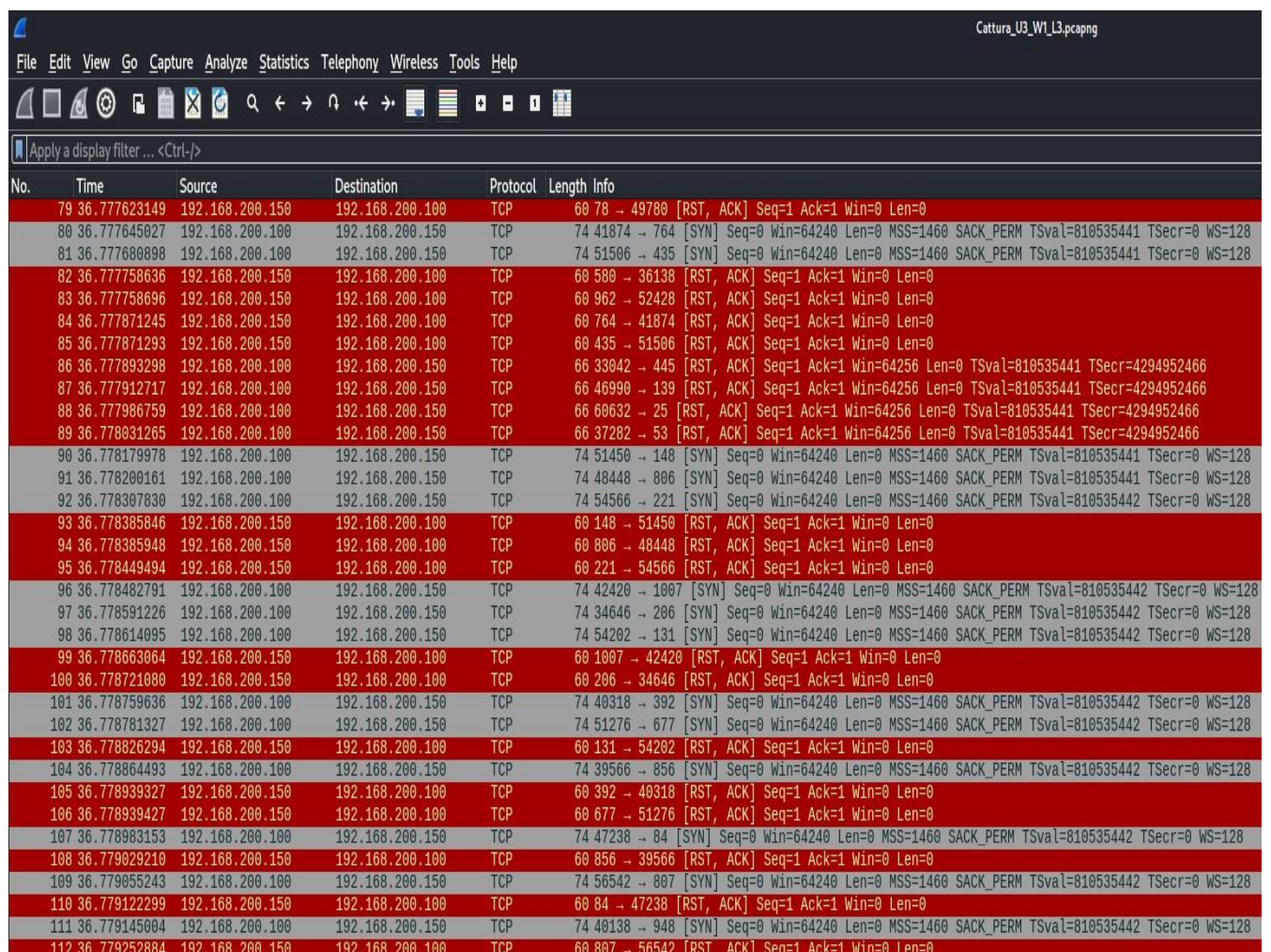
No.	Time	Source	Destination	Protocol	Length	Info
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776085853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34640 → 507 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	36.776568006	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 → 34640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
57	36.776904020	192.168.200.150	192.168.200.100	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
62	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
64	36.776905162	192.168.200.150	192.168.200.100	TCP	60	500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143014	192.168.200.150	192.168.200.150	TCP	74	56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
71	36.777166021	192.168.200.100	192.168.200.150	TCP	74	35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128

Nella seguente immagine possiamo notare un comportamento della scansione porte per ogni singolo tentativo di connessione su ogni porta

L'attaccante cerca di mappare tutti i servizi attivi della macchina vittima

L'attaccante con l'invio dei pacchetti SYN su una porta specifica, può far capire che è in corso un tentativo di connessione, su porte diverse, e quindi il cyber criminale, utilizza strumenti di scansione, come:

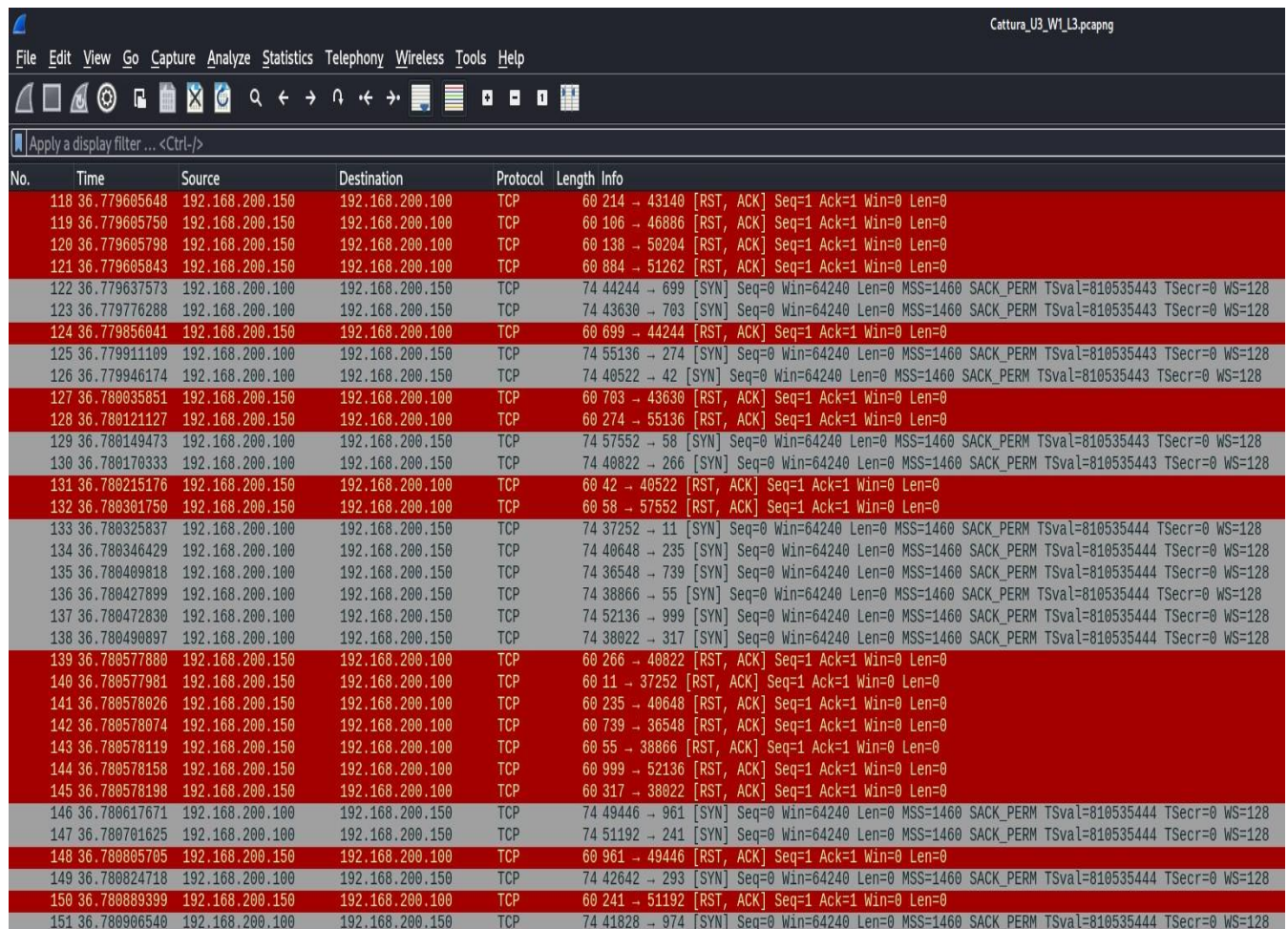
- **Nmap (Network Mapper)**: strumento open-source per scansione di reti
- **script di Metasploit**



No.	Time	Source	Destination	Protocol	Length	Info
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74	48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
92	36.778307830	192.168.200.100	192.168.200.150	TCP	74	54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60	148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385948	192.168.200.150	192.168.200.100	TCP	60	806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449494	192.168.200.150	192.168.200.100	TCP	60	221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74	54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
99	36.778663064	192.168.200.150	192.168.200.100	TCP	60	1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60	206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
103	36.778826294	192.168.200.150	192.168.200.100	TCP	60	131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
105	36.778939327	192.168.200.150	192.168.200.100	TCP	60	392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.150	192.168.200.100	TCP	60	677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778983153	192.168.200.100	192.168.200.150	TCP	74	47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
108	36.779029210	192.168.200.150	192.168.200.100	TCP	60	856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145004	192.168.200.100	192.168.200.150	TCP	74	40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Nella seguente immagine possiamo notare invii di pacchetti **RST/ACK**, il quale la macchina vittima, in questo caso: **192.168.200.150** risponde con un rifiuto di connessione (**connection refused**) in entrata.

SYN/ACK: in caso di risposte assenti, come da screenshot di Wireshark, possiamo dedurre che la macchina vittima non accetta connessioni su porte specifiche o anche perché è stato configurato un firewall, in grado di bloccare tentativi di collegamento.



Cattura_U3_W1_L3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

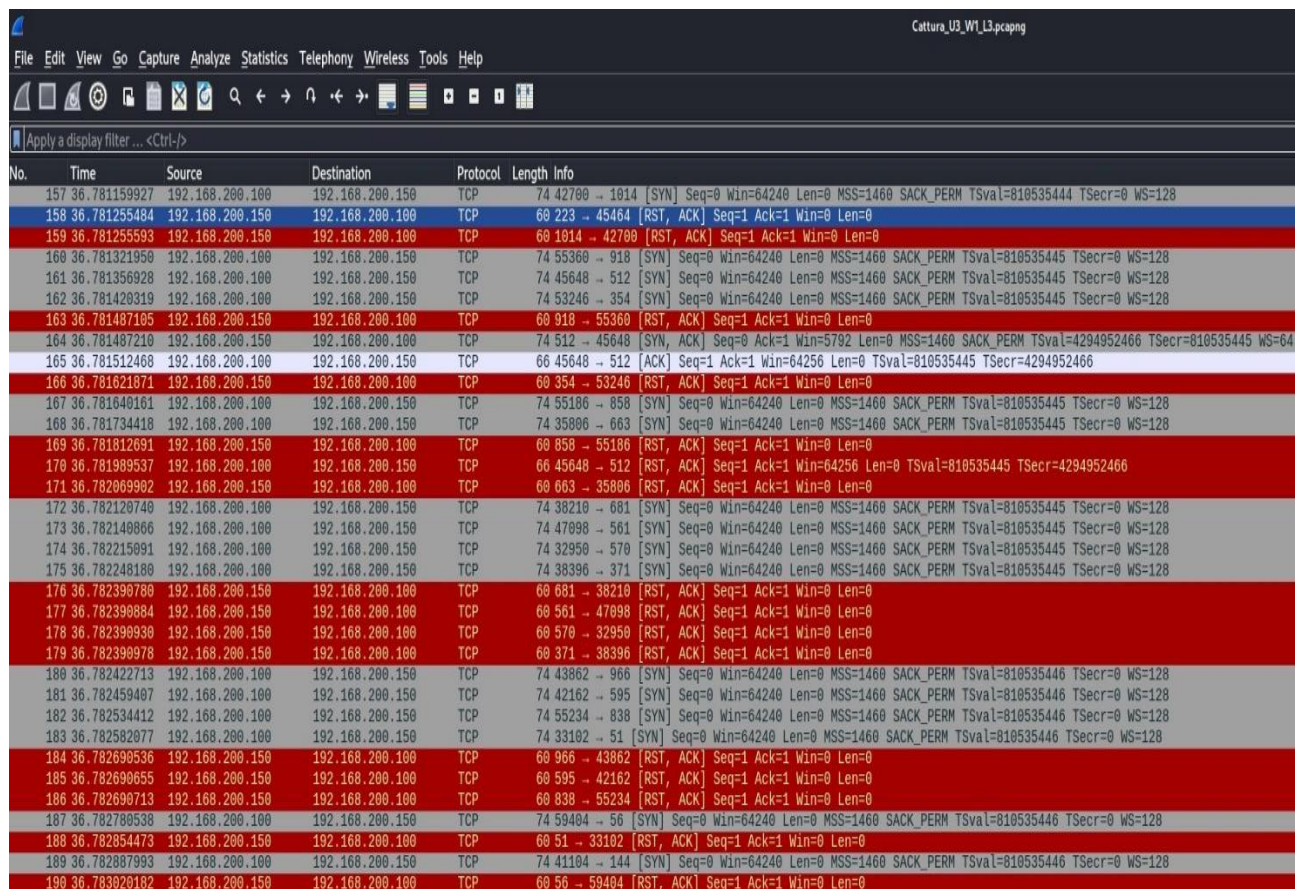
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779605750	192.168.200.150	192.168.200.100	TCP	60	106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779605798	192.168.200.150	192.168.200.100	TCP	60	138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779605843	192.168.200.150	192.168.200.100	TCP	60	884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779637573	192.168.200.100	192.168.200.150	TCP	74	44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
123	36.779776288	192.168.200.100	192.168.200.150	TCP	74	43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
124	36.779856041	192.168.200.150	192.168.200.100	TCP	60	699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779911109	192.168.200.100	192.168.200.150	TCP	74	55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
126	36.779946174	192.168.200.100	192.168.200.150	TCP	74	40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
127	36.780035851	192.168.200.150	192.168.200.100	TCP	60	703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60	274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780149473	192.168.200.100	192.168.200.150	TCP	74	57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74	40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60	42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780301750	192.168.200.150	192.168.200.100	TCP	60	58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325837	192.168.200.100	192.168.200.150	TCP	74	37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74	36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
137	36.780472830	192.168.200.100	192.168.200.150	TCP	74	52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74	38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
139	36.780577800	192.168.200.150	192.168.200.100	TCP	60	266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60	11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60	235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60	739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60	55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578158	192.168.200.150	192.168.200.100	TCP	60	999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.150	192.168.200.100	TCP	60	317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780617671	192.168.200.100	192.168.200.150	TCP	74	49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
147	36.780701625	192.168.200.100	192.168.200.150	TCP	74	51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
148	36.780805705	192.168.200.150	192.168.200.100	TCP	60	961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	36.780824718	192.168.200.100	192.168.200.150	TCP	74	42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
150	36.780889399	192.168.200.150	192.168.200.100	TCP	60	241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780906540	192.168.200.100	192.168.200.150	TCP	74	41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128

Nella seguente immagine possiamo notare numerosi tentativi di connessione da parte dell'attaccante su specifiche porte:

- **Porta 445 - SMB Serve Message Block:** c'è un repentino tentativo di connessione **SYN - RST/ACK**.
- **Porta 445:** oltre ad essere una delle più comuni è anche una delle porte prese più di mira in fase di attacco da parte di uno o più cyber criminali.

Questo tipo di tentativo è un forte indicatore di un attacco mirato verso SMB, ed è molto probabile che l'attaccante stia cercando di sfruttare una vulnerabilità nota per ottenere l'accesso al sistema di destinazione.



Cattura_U3_W1_L3.pcapng

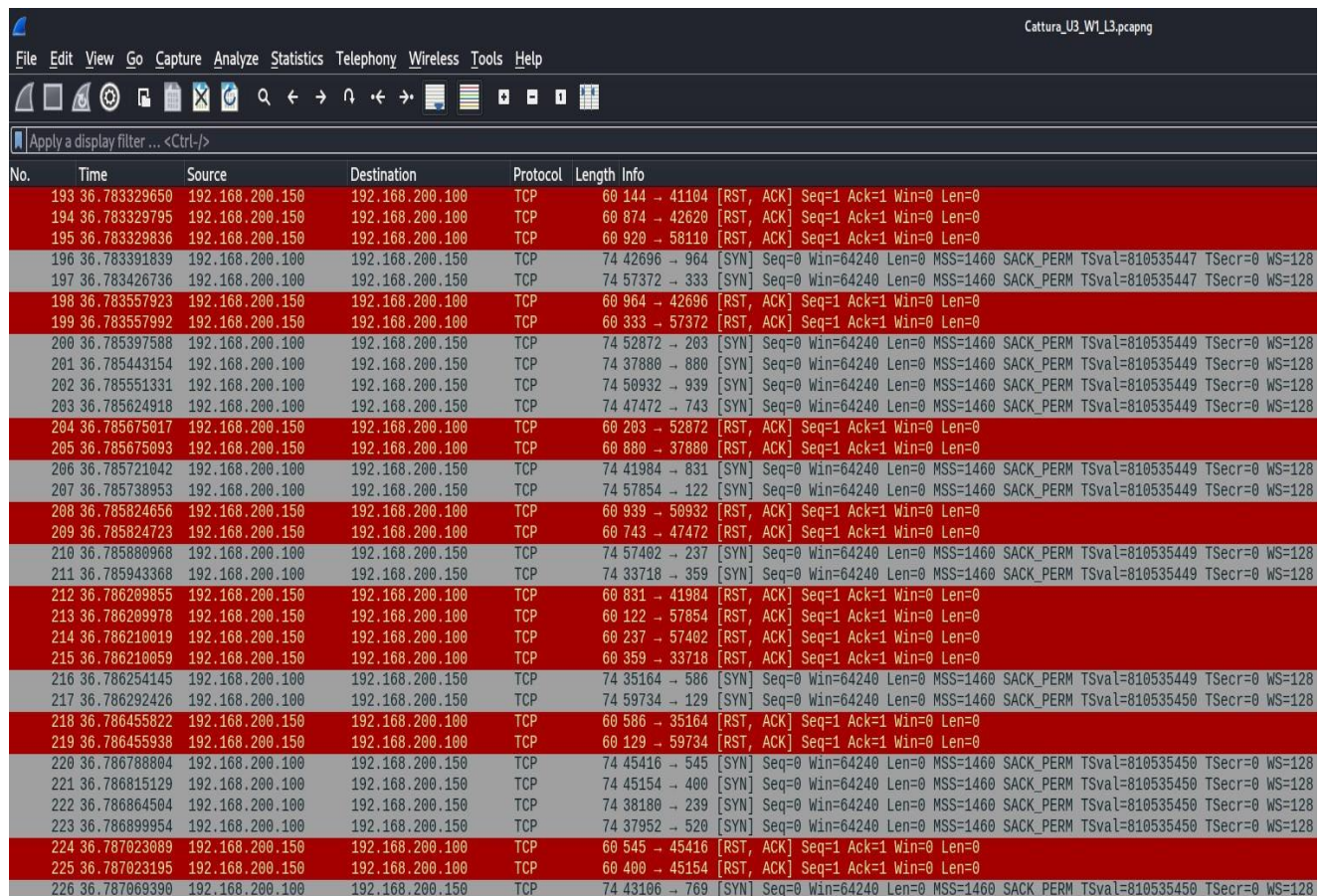
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
157	36.781159927	192.168.200.100	192.168.200.150	TCP	74	42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
158	36.781255484	192.168.200.150	192.168.200.100	TCP	60	223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	36.781255593	192.168.200.150	192.168.200.100	TCP	60	1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	36.781321950	192.168.200.100	192.168.200.150	TCP	74	55360 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
161	36.781356928	192.168.200.100	192.168.200.150	TCP	74	45648 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
162	36.781420319	192.168.200.100	192.168.200.150	TCP	74	53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
163	36.781487105	192.168.200.150	192.168.200.100	TCP	60	918 → 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
166	36.781621071	192.168.200.150	192.168.200.100	TCP	60	354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	36.781640161	192.168.200.100	192.168.200.150	TCP	74	55180 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
168	36.781734418	192.168.200.100	192.168.200.150	TCP	74	35806 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
169	36.781812691	192.168.200.150	192.168.200.100	TCP	60	858 → 55180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	36.781989537	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
171	36.782069902	192.168.200.150	192.168.200.100	TCP	60	663 → 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	36.782120740	192.168.200.100	192.168.200.150	TCP	74	38210 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
173	36.782140866	192.168.200.100	192.168.200.150	TCP	74	47098 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
174	36.782215091	192.168.200.100	192.168.200.150	TCP	74	32950 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
175	36.782248100	192.168.200.100	192.168.200.150	TCP	74	38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
176	36.782390780	192.168.200.150	192.168.200.100	TCP	60	681 → 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	36.782390884	192.168.200.150	192.168.200.100	TCP	60	561 → 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	36.782390930	192.168.200.150	192.168.200.100	TCP	60	570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	36.782390978	192.168.200.150	192.168.200.100	TCP	60	371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	36.782422713	192.168.200.100	192.168.200.150	TCP	74	43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
181	36.782459407	192.168.200.100	192.168.200.150	TCP	74	42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
182	36.782534412	192.168.200.100	192.168.200.150	TCP	74	55234 → 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
183	36.782582077	192.168.200.100	192.168.200.150	TCP	74	33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
184	36.782690536	192.168.200.150	192.168.200.100	TCP	60	966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	36.782690655	192.168.200.150	192.168.200.100	TCP	60	595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	36.782690713	192.168.200.150	192.168.200.100	TCP	60	838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	36.782780538	192.168.200.100	192.168.200.150	TCP	74	59404 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
188	36.782854473	192.168.200.150	192.168.200.100	TCP	60	51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	36.782887993	192.168.200.100	192.168.200.150	TCP	74	41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
190	36.783020182	192.168.200.150	192.168.200.100	TCP	60	56 → 59404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Nella seguente immagine ed ultima analisi fatta su **Wireshark** dei tentativi di connessione da parte dell'attaccante con **IP 192.168.200.100**, ci conferma un'attività di scansione in modo persistente tra gli IP **192.168.200.150**

In conclusione possiamo dire che c'è un costante tentativo di connessione e di attacco attraverso le porte specifiche, vulnerabili, ma che alla fine l'attacco stesso, non è andato a buon fine.



No.	Time	Source	Destination	Protocol	Length	Info
193	36.783329650	192.168.200.150	192.168.200.100	TCP	60	144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	36.783329795	192.168.200.150	192.168.200.100	TCP	60	874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	36.783329836	192.168.200.150	192.168.200.100	TCP	60	920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	36.783391839	192.168.200.100	192.168.200.150	TCP	74	42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535447 TSecr=0 WS=128
197	36.783426736	192.168.200.100	192.168.200.150	TCP	74	57372 → 333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535447 TSecr=0 WS=128
198	36.783557923	192.168.200.150	192.168.200.100	TCP	60	964 → 42696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
199	36.783557992	192.168.200.150	192.168.200.100	TCP	60	333 → 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200	36.785397588	192.168.200.100	192.168.200.150	TCP	74	52872 → 203 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
201	36.785443154	192.168.200.100	192.168.200.150	TCP	74	37880 → 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
202	36.785551331	192.168.200.100	192.168.200.150	TCP	74	50932 → 939 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
203	36.785624918	192.168.200.100	192.168.200.150	TCP	74	47472 → 743 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
204	36.785675017	192.168.200.150	192.168.200.100	TCP	60	203 → 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
205	36.785675093	192.168.200.150	192.168.200.100	TCP	60	880 → 37880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206	36.785721042	192.168.200.100	192.168.200.150	TCP	74	41984 → 831 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
207	36.785738953	192.168.200.100	192.168.200.150	TCP	74	57854 → 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
208	36.785824656	192.168.200.150	192.168.200.100	TCP	60	939 → 50932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
209	36.785824723	192.168.200.150	192.168.200.100	TCP	60	743 → 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
210	36.785880968	192.168.200.100	192.168.200.150	TCP	74	57402 → 237 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
211	36.785943368	192.168.200.100	192.168.200.150	TCP	74	33718 → 359 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
212	36.786209855	192.168.200.150	192.168.200.100	TCP	60	831 → 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
213	36.786209978	192.168.200.150	192.168.200.100	TCP	60	122 → 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
214	36.786210019	192.168.200.150	192.168.200.100	TCP	60	237 → 57402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
215	36.786210059	192.168.200.150	192.168.200.100	TCP	60	359 → 33718 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
216	36.786254145	192.168.200.100	192.168.200.150	TCP	74	35164 → 586 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535449 TSecr=0 WS=128
217	36.786292426	192.168.200.100	192.168.200.150	TCP	74	59734 → 129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
218	36.786455822	192.168.200.150	192.168.200.100	TCP	60	586 → 35164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
219	36.786455938	192.168.200.150	192.168.200.100	TCP	60	129 → 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
220	36.786788804	192.168.200.100	192.168.200.150	TCP	74	45416 → 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
221	36.786815129	192.168.200.100	192.168.200.150	TCP	74	45154 → 400 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
222	36.786864504	192.168.200.100	192.168.200.150	TCP	74	38180 → 239 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
223	36.786899954	192.168.200.100	192.168.200.150	TCP	74	37952 → 520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
224	36.787023089	192.168.200.150	192.168.200.100	TCP	60	545 → 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
225	36.787023195	192.168.200.150	192.168.200.100	TCP	60	400 → 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
226	36.787069390	192.168.200.100	192.168.200.150	TCP	74	43106 → 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128

Le raccomandazioni finali, per poter mitigare eventuali attacchi sono:

- Implementare IDS/IPS (Intrusion Detection System/ Intrusion Prevention System)
- Segmentare la rete
- Aggiornare le patch di Sicurezza