

S9L5

UNIT 3

Marco Falchi

Consegna

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. **Analizzate** la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di **attacchi in corso**
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro



Cattura_U3_W1_L3.pcapng

Prime analisi

Dai dati forniti dalla scansione tramite wireshark è facilmente individuabile che i dispositivi coinvolti sono due:

IPv4: 192.168.200.100

IPv4: 192.168.200.150

No.	Time	Source	Destination	Protocol	Length	SPort	DPort	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286			Host Announcement METASPLOITABLE Workstation, Server, Print Queue Server, Xenix Ser...
2	23.764214955	192.168.200.100	192.168.200.150	TCP	74	53660	80	53660 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS...
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876	443	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS...
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80	53660	80 → 53660 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443	33876	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815269	192.168.200.100	192.168.200.150	TCP	66	53660	80	53660 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764830091	192.168.200.100	192.168.200.150	TCP	66	33876	443	33876 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	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	28.775230909	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	41304	23	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS...
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120	111	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS...
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878	443	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS...
15	36.774360305	192.168.200.100	192.168.200.150	TCP	74	58636	554	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS...
16	36.774485627	192.168.200.100	192.168.200.150	TCP	74	52358	135	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS...
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138	993	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS...
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182	21	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS...
19	36.774685955	192.168.200.150	192.168.200.100	TCP	74	23	41304	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466
20	36.774685952	192.168.200.150	192.168.200.100	TCP	74	111	56120	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466
21	36.774685996	192.168.200.150	192.168.200.100	TCP	60	443	33878	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	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	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774708404	192.168.200.100	192.168.200.150	TCP	66	41304	23	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120	111	56120 → 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	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141223	192.168.200.150	192.168.200.100	TCP	74	21	41182	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466
28	36.775174848	192.168.200.100	192.168.200.150	TCP	66	41182	21	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174	113	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS...
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656	22	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS...
31	36.775524284	192.168.200.100	192.168.200.150	TCP	74	53662	80	53662 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS...
32	36.775530306	192.168.200.150	192.168.200.100	TCP	66	113	59174	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	41304	23	41304 → 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	56120	111	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775789938	192.168.200.150	192.168.200.100	TCP	74	21	55656	21 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80	53662	80 → 53662 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656	22	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775803888	192.168.200.100	192.168.200.150	TCP	66	55656	22	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
OS Minor Version: 9								
Server Type: 0x0015a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser								
Browser Protocol Major Version: 15								
Signature: 0xaa55								
Host Comment: metasploitable server (Samba 3.0.20-Debian)								
0000	ff ff ff ff ff ff 00 00	27 fd 87 1e 00 00 45 00						E
0010	01 10 00 00 40 00 40 11	26 fd c0 a8 96 c0 a8						0 0 &
0020	c8 ff 00 8a 00 8a 00 fc	4b 01 11 8a 75 b4 c0 a8						K u
0030	c8 96 00 8a 00 e6 00 00	20 45 4e 45 46 46 45 45						ENEEFEE
0040	42 46 44 46 41 45 4d 45	50 45 4a 46 45 45 42 45						BFDFAE ME PEJFEER
0050	43 45 4d 45 46 43 41 41	41 00 20 40 48 45 50 46						CMEFCAA A FNEP

Una volta visionati i dati è stata fatta una identificazione delle macchine

192.168.200.100 come macchina attaccante

192.168.200.150 come vittima.

Nella sezione info (nella parte bassa dello screenshoot) possiamo inoltre notare come la macchina vittima si presenta come una macchina Metasploitable.

Analisi generale della cattura del traffico

Appare evidente che ciò che sta avvenendo è che l'attaccante tenta di sfruttare il three way handshake del protocollo TCP.

Vengono aperte numerose connessioni con il target, su vari servizi e subito dopo la ricezione del pacchetto ACK da parte della vittima, spesso l'attaccante invia un pacchetto RST che ha la funzione di terminare immediatamente la connessione, prima di inviare informazioni utili.

Si riassume quello che succede:

1. Fase di connessione

- L'IP 192.168.200.100 (attaccante) invia pacchetti SYN a più porte su 192.168.200.150 (vittima)

- La vittima risponde con il pacchetto SYN-ACK

- L'attaccante completa l'handshake con il pacchetto ACK

Facendo quindi una **scansione di tipo "aggressivo"**

2. Fase di reset immediato

- Dopo aver completato l'handshake l'attaccante invia un pacchetto RST, ACK che interrompe immediatamente la connessione appena avviata

Facendo quindi una **scansione di tipo "stealth"**

3. Verifica delle porte aperte

tcp.flags.syn == 1 && tcp.flags.ack == 1									
No.	Time	Source	Destination	Protocol	Length	Info			
4	23.76477323	192.168.200.150	192.168.200.100	TCP	74	89 → 53660 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
19	36.77468585	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	36.77468562	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
27	36.775143273	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
35	36.775799938	192.168.200.150	192.168.200.100	TCP	74	22 → 55056 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797894	192.168.200.150	192.168.200.100	TCP	74	89 → 53662 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33842 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46998 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 68632 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
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
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
267	36.788095940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
994	36.828722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42948 [SYN, ACK] Seq=0	Ack=1	Win=5792	Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64

Porte aperte trovate: 20-21-22-23-25-53-80-111-139-445-512-513-514

Analisi approfondite

Sono stati utilizzati dei filtri all'interno di WireShark per ottenere una visuale dei pacchetti inviati dalla macchina attaccante tramite il comando:

ip.src_host==192.168.200.100

questo ha permesso di vedere quali connessioni ha tentato di stabilire e come siano state gestite:

No.	Time	Source	Destination	Protocol	Length	SPort	DPort	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53660	80	53660 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=0
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876	443	33876 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53660	80	53660 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951105
7	23.764899991	192.168.200.100	192.168.200.150	TCP	66	53660	80	53660 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951105
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41394	23	41394 -> 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=0
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120	111	56120 -> 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=0
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878	443	33878 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=0
15	36.774366395	192.168.200.100	192.168.200.150	TCP	74	58636	554	58636 -> 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=0
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358	135	52358 -> 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=0
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138	993	46138 -> 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=0
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182	21	41182 -> 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=0
24	36.774700454	192.168.200.100	192.168.200.150	TCP	66	41394	23	41394 -> 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	56120	111	56120 -> 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182	21	41182 -> 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775377890	192.168.200.100	192.168.200.150	TCP	74	59174	113	59174 -> 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=0
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656	22	55656 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=0
31	36.775524264	192.168.200.100	192.168.200.150	TCP	74	53662	80	53662 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41394	23	41394 -> 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775624497	192.168.200.100	192.168.200.150	TCP	66	56120	111	56120 -> 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
37	36.775903106	192.168.200.100	192.168.200.150	TCP	66	55656	22	55656 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53662	80	53662 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182	21	41182 -> 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656	22	55656 -> 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53662	80	53662 -> 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	59084	199	59084 -> 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=0
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220	995	54220 -> 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=0
44	36.776339010	192.168.200.100	192.168.200.150	TCP	74	34648	587	34648 -> 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33842	445	33842 -> 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
46	36.776402590	192.168.200.100	192.168.200.150	TCP	74	49814	256	49814 -> 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990	139	46990 -> 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33296	143	33296 -> 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632	25	60632 -> 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
52	36.776566866	192.168.200.100	192.168.200.150	TCP	74	49654	110	49654 -> 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282	53	37282 -> 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898	580	54898 -> 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534	487	51534 -> 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=0
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33842	445	33842 -> 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466

Lo screen allegato mostra quanto precedentemente spiegato, vediamo la quantità di pacchetti SYN inviati dalla macchina attaccante verso le porte della macchina target.

È stato dunque modificato il filtro col comando

ip.src_host==192.168.200.100 && ip.dst_host==192.168.200.150 && tcp.flags.reset==1

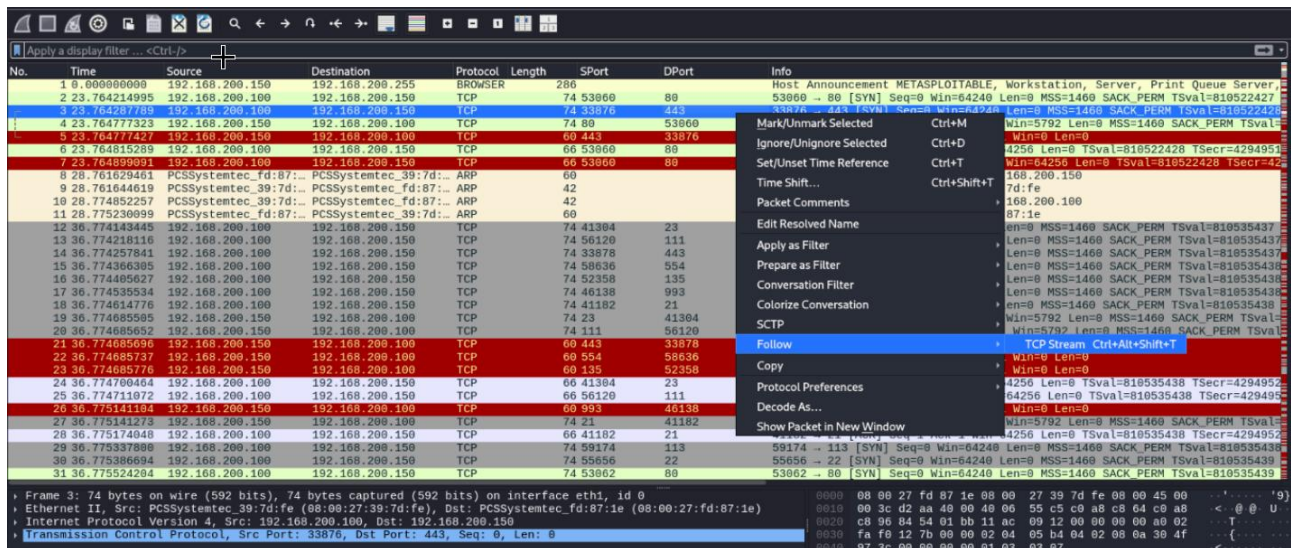
Per verificare solamente i pacchetti RST inviati dalla macchina attaccante per chiudere le connessioni avviate con il server.

No.	Time	Source	Destination	Protocol	Length	SPort	DPort	Info
7	23.764899991	192.168.200.100	192.168.200.150	TCP	66	53660	80	53660 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951105
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41394	23	41394 -> 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775624497	192.168.200.100	192.168.200.150	TCP	66	56120	111	56120 -> 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182	21	41182 -> 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656	22	55656 -> 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53662	80	53662 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
49	36.776478201	192.168.200.100	192.168.200.150	TCP	66	46990	139	46990 -> 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632	25	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	37282 -> 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
170	36.781989537	192.168.200.100	192.168.200.150	TCP	66	45648	512	45648 -> 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
273	36.789861130	192.168.200.100	192.168.200.150	TCP	66	51396	514	51396 -> 514 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535453 TSecr=4294952467
1975	36.829275924	192.168.200.100	192.168.200.150	TCP	66	42048	513	42048 -> 513 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535493 TSecr=4294952471

Lo screen mostra l'apertura seguita da immediata chiusura delle connessioni con le porte 80, 23, 111, 21, 22, 445, 139, 25, 53, 512, 514, 513

Successivamente utilizziamo la funzione per seguire lo stream TCP:

cliccando un pacchetto di interesse con il tasto destro > Follow > TCP Stream



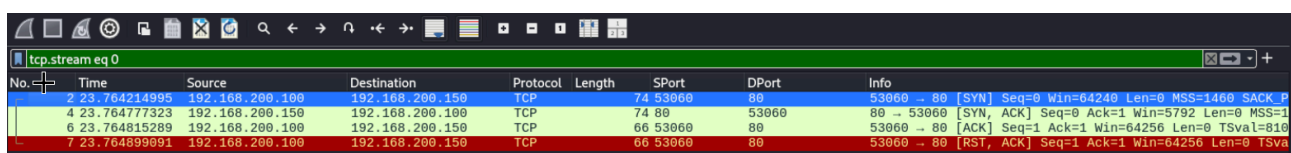
Possiamo vedere il flusso TCP per ogni connessione stabilita e successivamente resettata.

Viene quindi aperta una nuova finestra di Wireshark che normalmente contiene i dati e le informazioni scambiate tra client e server durante la comunicazione ma poiché il pacchetto RST viene inviato senza aver scambiato alcun dato tra le macchine, non è presente alcuna informazione.

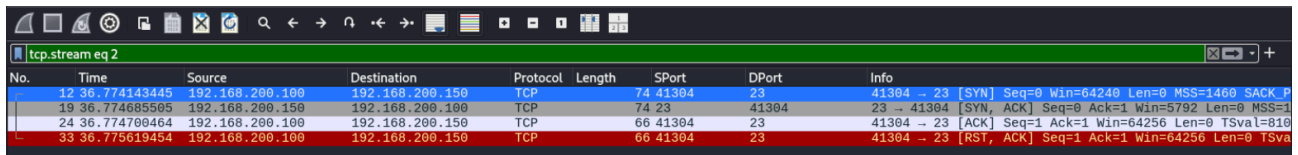
Tuttavia il filtro per seguire lo stream ci è molto utile poiché vengono filtrati singolarmente i pacchetti della connessione stabilita e resettata. Ci basta incrementare il numero dello stream per vedere tutte quante le connessioni al variare della porta

Susseguono immagini di alcuni stream aperti e chiusi dall'attaccante

Stream 0 - Porta 80 HTTP:

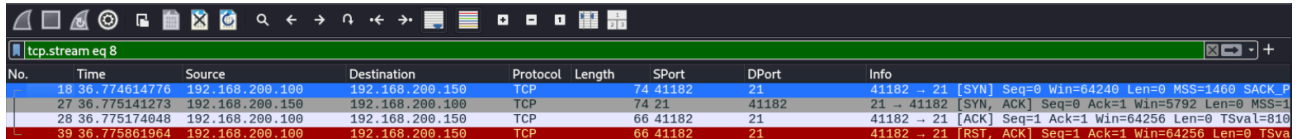


Stream 2 - Porta 23 Telnet:



No.	Time	Source	Destination	Protocol	Length	SPort	DPort	Info
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304	23	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
19	36.774685585	192.168.200.150	192.168.200.100	TCP	74	23	41304	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1
24	36.774788464	192.168.200.100	192.168.200.150	TCP	66	41304	23	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=818
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304	23	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva

Stream 8 - Porta 21 FTP:



No.	Time	Source	Destination	Protocol	Length	SPort	DPort	Info
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182	21	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21	41182	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1
28	36.775174848	192.168.200.100	192.168.200.150	TCP	66	41182	21	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=818
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182	21	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva

Identificazione degli IOC

La tabella di seguito riassume gli indicatori di compromissione del possibile attacco:

IOC	Descrizione
Fonte dell'attacco	IP attaccante: 192.168.200.100
Target	IP vittima: 192.168.200.150
Tecnica usata	Invio pacchetti TCP RST
Caratteristiche	Handshake TCP e invio di pacchetti RST immediati

Ipotesi sui potenziali vettori di attacco

Ipotesi 1: Scansione delle porte

Sulla base degli indicatori che ho trovato, ho ipotizzato che l'attaccante abbia eseguito due scansioni, una prima aggressiva e una seconda stealth (ad esempio con nmap sulle porte TCP del target). L'ipotesi della scansione trova riscontro nella quantità di pacchetti SYN inviati dall'attaccante e nei pacchetti RST inviati dal server al client dopo il primo pacchetto SYN ricevuto, il che indica che la porta scansionata è chiusa.

Ipotesi 2: Attacco DoS - RST flood (altamente improbabile)

Considerando invece le connessioni terminate immediatamente dall'attaccante, possiamo ipotizzare in un futuro attacco DoS di tipo RST flood.

Sembra infatti che spesso vengano provati dei piccoli attacchi Dos

1196	36.834576712	192.168.200.100	192.168.200.150	TCP	74.51438	-	642	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1197	36.83444481	192.168.200.100	192.168.200.150	TCP	74.42724	-	756	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1198	36.834717727	192.168.200.100	192.168.200.150	TCP	74.58998	-	865	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1199	36.834730079	192.168.200.100	192.168.200.150	TCP	74.58824	-	349	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1200	36.834841743	192.168.200.100	192.168.200.150	TCP	74.55968	-	695	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1201	36.83492572	192.168.200.100	192.168.200.150	TCP	74.49132	-	208	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1202	36.834977389	192.168.200.100	192.168.200.150	TCP	74.47984	-	88	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1203	36.835049959	192.168.200.100	192.168.200.150	TCP	74.44292	-	451	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1204	36.835104563	192.168.200.100	192.168.200.150	TCP	74.47804	-	815	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1205	36.835168257	192.168.200.100	192.168.200.150	TCP	74.38660	-	48	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1206	36.835232147	192.168.200.100	192.168.200.150	TCP	74.42224	-	162	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1207	36.835260651	192.168.200.100	192.168.200.150	TCP	74.50746	-	875	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935498	Tsecr=0	WS=128
1208	36.835362548	192.168.200.100	192.168.200.150	TCP	74.38352	-	1822	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1209	36.835426559	192.168.200.100	192.168.200.150	TCP	74.45820	-	225	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1210	36.835466907	192.168.200.100	192.168.200.150	TCP	74.56484	-	454	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1211	36.835508415	192.168.200.100	192.168.200.150	TCP	74.42742	-	37	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1212	36.835524520	192.168.200.100	192.168.200.150	TCP	74.44816	-	118	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1213	36.835689181	192.168.200.100	192.168.200.150	TCP	74.41810	-	136	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1214	36.835732119	192.168.200.100	192.168.200.150	TCP	74.58510	-	134	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1215	36.835816973	192.168.200.100	192.168.200.150	TCP	74.58112	-	441	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1216	36.835886815	192.168.200.100	192.168.200.150	TCP	74.44332	-	918	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1217	36.835945031	192.168.200.100	192.168.200.150	TCP	74.55668	-	480	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1218	36.836008884	192.168.200.100	192.168.200.150	TCP	74.57498	-	744	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1219	36.836072760	192.168.200.100	192.168.200.150	TCP	74.58888	-	161	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1220	36.836136952	192.168.200.100	192.168.200.150	TCP	74.47654	-	774	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1221	36.836209072	192.168.200.100	192.168.200.150	TCP	74.37698	-	688	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935499	Tsecr=0	WS=128
1222	36.836265031	192.168.200.100	192.168.200.150	TCP	74.48198	-	658	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1223	36.836338288	192.168.200.100	192.168.200.150	TCP	74.48386	-	614	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1224	36.836402293	192.168.200.100	192.168.200.150	TCP	74.47864	-	140	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1225	36.836466049	192.168.200.100	192.168.200.150	TCP	74.42852	-	246	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1226	36.836531870	192.168.200.100	192.168.200.150	TCP	74.45840	-	952	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1227	36.836598519	192.168.200.100	192.168.200.150	TCP	74.41254	-	766	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1228	36.836661285	192.168.200.100	192.168.200.150	TCP	74.44812	-	840	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1229	36.836724991	192.168.200.100	192.168.200.150	TCP	74.43898	-	1812	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1230	36.836793913	192.168.200.100	192.168.200.150	TCP	74.49964	-	884	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1231	36.836854551	192.168.200.100	192.168.200.150	TCP	74.41682	-	577	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1232	36.836917770	192.168.200.100	192.168.200.150	TCP	74.44894	-	418	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1233	36.836981177	192.168.200.100	192.168.200.150	TCP	74.46540	-	216	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1234	36.837044822	192.168.200.100	192.168.200.150	TCP	74.47864	-	408	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1235	36.837108120	192.168.200.100	192.168.200.150	TCP	74.51852	-	325	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935500	Tsecr=0	WS=128
1236	36.83725583	192.168.200.100	192.168.200.150	TCP	74.38224	-	531	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935501	Tsecr=0	WS=128
1237	36.837399652	192.168.200.100	192.168.200.150	TCP	74.41482	-	31	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935501	Tsecr=0	WS=128
1238	36.837468068	192.168.200.100	192.168.200.150	TCP	74.40290	-	792	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935501	Tsecr=0	WS=128
1239	36.837523814	192.168.200.100	192.168.200.150	TCP	74.37756	-	293	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935501	Tsecr=0	WS=128
1240	36.837587278	192.168.200.100	192.168.200.150	TCP	74.38362	-	715	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935501	Tsecr=0	WS=128
1241	36.837652783	192.168.200.100	192.168.200.150	TCP	74.52524	-	734	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935501	Tsecr=0	WS=128
1242	36.837733206	192.168.200.100	192.168.200.150	TCP	74.50998	-	189	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935501	Tsecr=0	WS=128
1243	36.837817133	192.168.200.100	192.168.200.150	TCP	74.54772	-	335	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK	PERM	Tsval=818935501	Tsecr=0	WS=128

Difatti dalla riga 1196 alla 1243 (47 richieste) sembra quasi un piccolo tentativo di Dos, magari per verificare se la rete sia monitorata dando quindi la parvenza di star tastando il terreno per un possibile attacco futuro, provando a trovare una falla come un firewall assente o un anti Dos.

Possibili contromisure

Di seguito ho elencato possibili contromisure per ridurre l'impatto di questo attacco e prevenire attacchi simili in futuro:

1. Contromisure immediate

- Bloccare l'indirizzo IP dell'attaccante (ad esempio tramite il firewall)
- Usare tool di rilevamento di pacchetti RST sospetti (ad esempio Snort)
- Limitare i pacchetti RST per evitare il flooding (regole di firewall)

2. Protezione a lungo termine e prevenzione

- Abilitare il logging avanzato per rilevare pacchetti RST anomali

- Impedire agli utenti non autorizzati di effettuare scanning della rete (tramite regole di firewall)
- Implemento di IDS e IPS a seconda delle necessità aziendali
- Segmentare la rete per limitare movimenti laterali (tramite VLAN o firewall fra le segmentazioni)

3. Protezione a lungo termine e prevenzione **AVANZATE**

- Implementare rate limiting (limita la quantità di traffico e il numero di richieste che un utente può fare a un server in un certo periodo e serve a prevenire attacchi DoS/DDoS, bloccando o rallentando chi cerca di sovraccaricare un sistema e garantire la stabilità e la disponibilità del servizio per tutti gli utenti)
- Implementare i SYN Cookies (una tecnica per difendere un server dagli attacchi SYN Flood, Quando un client invia una richiesta di connessione (SYN), il server non alloca memoria per la connessione. Invece, risponde con un pacchetto SYN-ACK che contiene un "cookie" crittografato nel numero di sequenza. Se il client è legittimo, risponde con un ACK che include il cookie. Solo a quel punto il server convalida il cookie e stabilisce la connessione, ignorando le richieste false. Questo impedisce che la coda di connessioni del server si riempia di richieste fasulle, mantenendo il servizio disponibile.)

Conclusione

Dall'analisi del traffico di rete è possibile ipotizzare che è in corso una ricognizione per un possibile futuro attacco DoS.

L'indirizzo IP della macchina dell'attaccante è 192.168.200.100.

Con certezza vi è una scansione delle porte sulla macchina target, per i numerosi tentativi di connessione alle porte.