

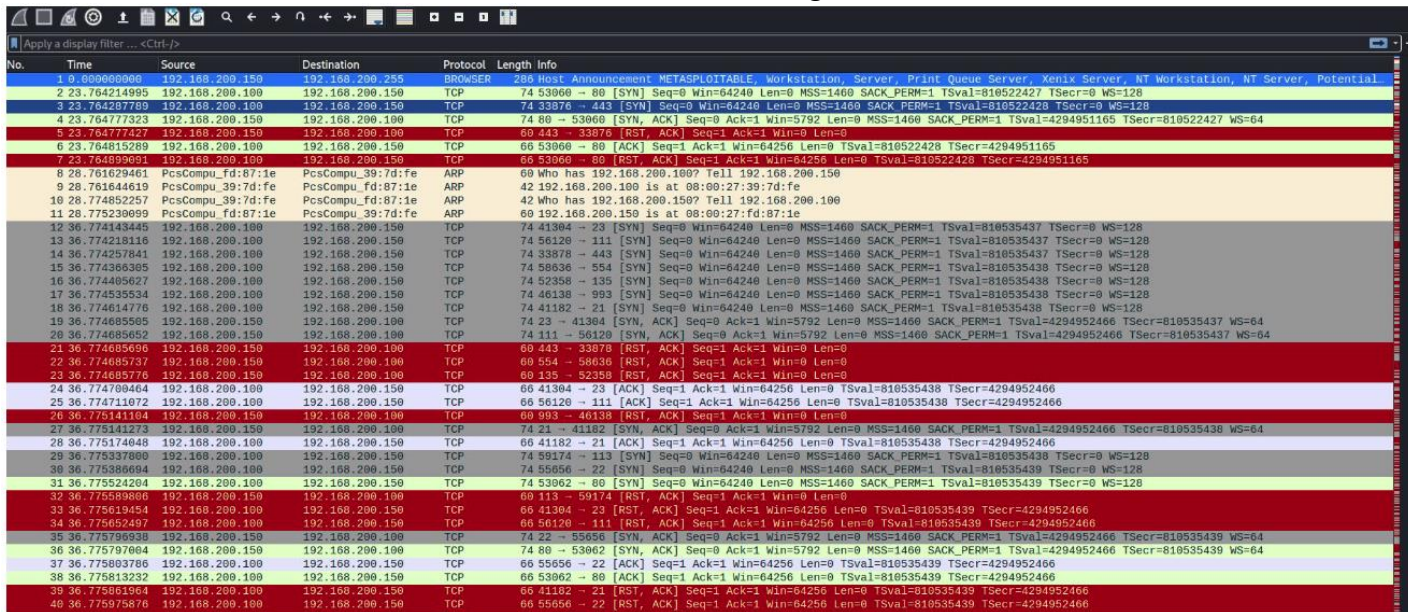
THREAD INTELLIGENCE & IOC

FRANCESCO PERSICHETTI

TASK:

- Identificare eventuali IOC
- Ipotizzare quali sono i vettori di attacco utilizzati
- Trovare un possibile rimedio

Scaricato il file di cattura di wireshark, vado ad analizzare la seguente scansione



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROADCAST	288	Webb Announcement METASPLOITABLE Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53960 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 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=1 TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 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	53960 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53960 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230899	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	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=1 TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
14	36.774257641	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
15	36.774368305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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=1 TSval=810535438 TSecr=0 WS=128
19	36.774685565	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=1 TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	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=1 TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [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	36.774709464	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	36.774711072	192.168.200.100	192.168.200.150	TCP	66	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 [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=1 TSval=4294952466 TSecr=810535438 WS=64
28	36.775174648	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	36.775337600	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535439 TSecr=0 WS=128
31	36.775524284	192.168.200.100	192.168.200.150	TCP	74	53962 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
32	36.775580306	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	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775799938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
36	36.775797064	192.168.200.150	192.168.200.100	TCP	74	80 → 53962 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	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	53962 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861954	192.168.200.100	192.168.200.150	TCP	66	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 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Uno dei maggiori elementi di compromissione che possiamo notare è il massivo invio di pacchetti TCP su diverse porte, evidenziando una scansione nei confronti della macchina target.

Potrei ipotizzare ad una scansione con il tool “nmap” e lo switch -sT poiché si vede completare la connessione con il three-way handshake.

Una soluzione più rapida per ovviare a questi tipi di attacchi potrebbe essere quella di mettere un firewall a protezione della macchina attaccata, in modo da non far sapere all’attaccante le porte aperte o meno con una semplice scansione