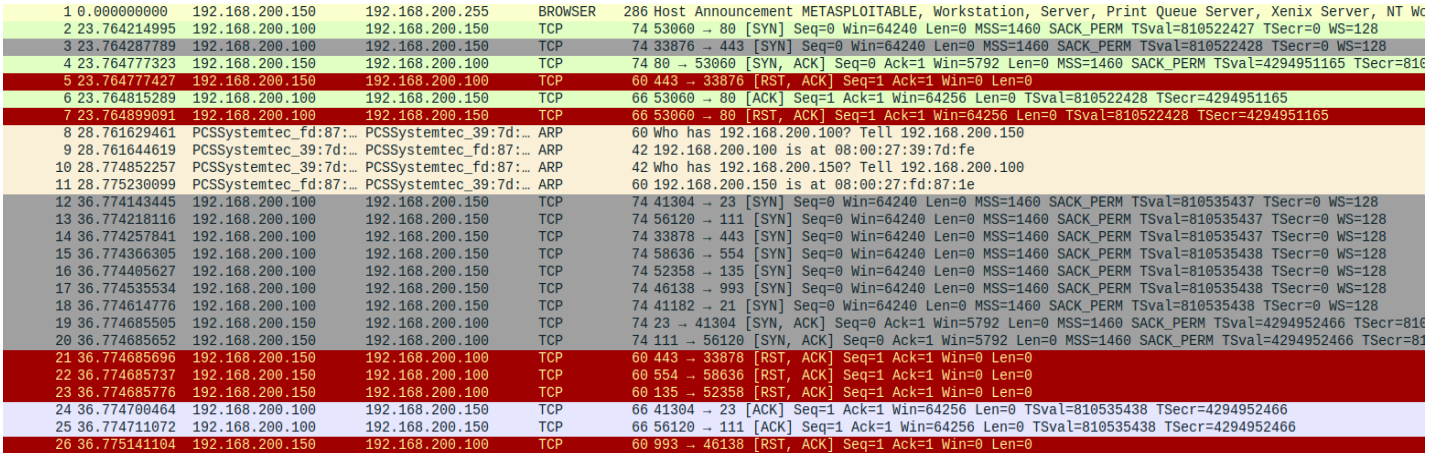
Analizzazione pacchetti con Wireshark

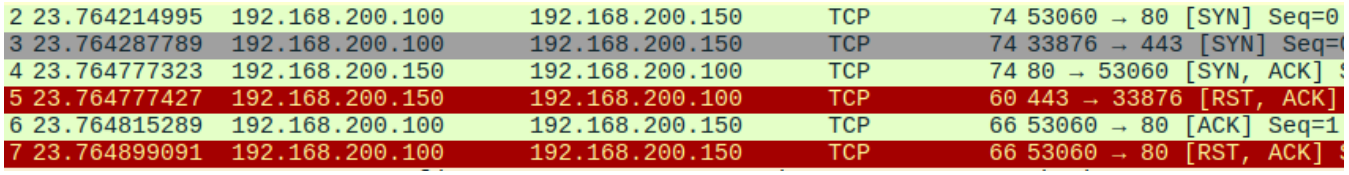
L’esercizio di oggi consiste nell’analizzare una cattura di rete eseguita con Wireshark.

1. Analisi



1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Wo
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=810
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	23.764899091	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	28.761629461	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	28.775230099	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 [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 56120 → 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	36.774366305	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	36.774405627	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	36.774685505	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810
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 TSval=4294952466 TSecr=81
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	36.774700464	192.168.200.100	192.168.200.150	TCP	66 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 [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

Dall’immagine che ho caricato si nota uno scambio di connessioni TCP tra due host, 192.168.200.100 e 192.168.200.150. La prima cosa che mi viene in mente è che si possa trattare di una scansione delle porte di rete, l’attaccante è l’indirizzo IP 192.168.200.100 e la vittima è 192.168.200.150. Molto probabilmente lo strumento d’attacco utilizzato è **Nmap,** tool molto potente per la scansione delle porte di un determinato indirizzo IP.
Adesso per capire in che modo è stato utilizzato Nmap dobbiamo visualizzare più da vicino una sequenza di scambio di pacchetti.



2	23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK]
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60 443 → 33876 [RST, ACK]
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK]

Qui possiamo notare che 192.168.200.100, partendo dalla porta 53060, invia la richiesta di connessione **SYN** a 192.168.200.150 sulla porta 80 (http). Appena 192.168.200.150 riceve il pacchetto, risponde con un [SYN, ACK], dando così una risposta positiva e confermando la sua apertura. A questo punto l’host .100 invia un ACK a .150, stabilendo una connessione. Connessione che viene terminata istantaneamente da .100 che invia un pacchetto [RST, ACK]. Questo comportamento mi ha fatto subito pensare che si trattasse di un tool automatico, in quanto questa comunicazione è avvenuta in millesimi di secondo.

La condivisione di pacchetti eseguita in questo modo, quindi prima con un SYN, poi un [SYN,ACK] e infine un ACK è nota come Three-Handway-Shake, che viene completata con la porta 80.
Invece per la porta 443 vediamo che la connessione viene interrotta subito in quanto in risposta al pacchetto SYN è stato inviato subito un pacchetto [RST, ACK].

Nel caso in cui avremmo notato che, dopo il pacchetto [SYN, ACK], ce ne fosse stato uno [RST, ACK], non avremmo avuto la completezza del Three-Way-Handshake, in quel caso la scansione sarebbe stata di tipo Syn-Scan che viene eseguita con la flag **-sS**.

2. Conclusione

Analizzando questa successione di pacchetti possiamo stabilire che 192.168.200.100 ha eseguito una scansione delle porte su 192.168.200.150 utilizzando Nmap. Più precisamente è stata utilizzata come flag nel comando Nmap **-sT ,** questa flag crea connessioni TCP complete terminando il Three-Way-Handshake.

Per ridurre gli impatti dell'attacco e evitare attacchi futuri i consigli sono:

- Isolare l'host sospetto dalla rete
- Impostare regole firewall
  Bloccare il traffico non necessario e impostare delle regole per consentire solamente il traffico legittimo.
- Implementare IDS/IPS
  Analizzano il traffico di rete e rilevano le scansioni di porte.
  Possono essere configurati per bloccare questi "attacchi" in tempo reale.