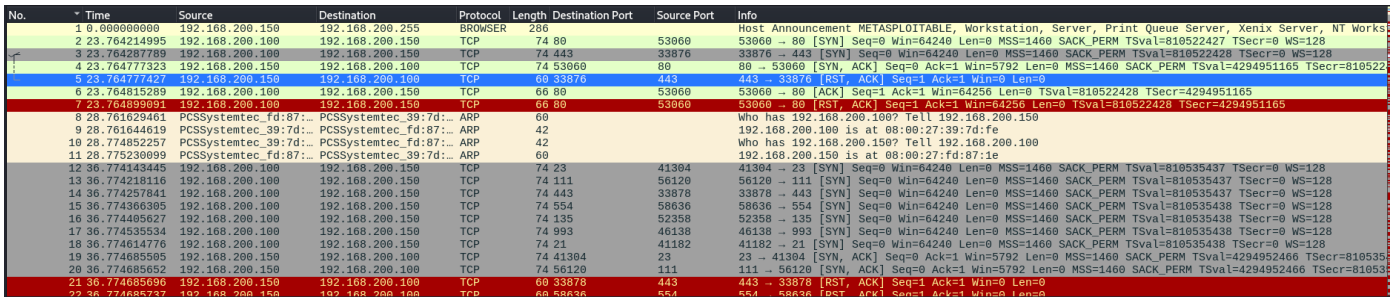
S9/L5

L'esercizio di oggi consiste nell'analizzare una cattura di rete tramite wireshark è 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.

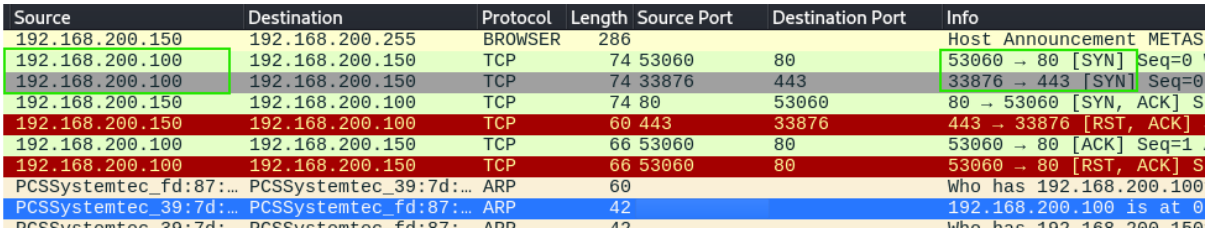
Come prima cosa apriamo il traffico fornitoci tramite WireShark:



No.	Time	Source	Destination	Protocol	Length	Destination Port	Source Port	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286			Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Works
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	80	53060	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	443	33876	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	53060	80	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	33876	443	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	80	53060	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	80	53060	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	23	41304	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	111	56120	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	443	33878	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	554	58636	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	135	52358	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	993	46138	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	21	41182	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	41304	23	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	56120	111	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=81053
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	33878	443	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	58636	554	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

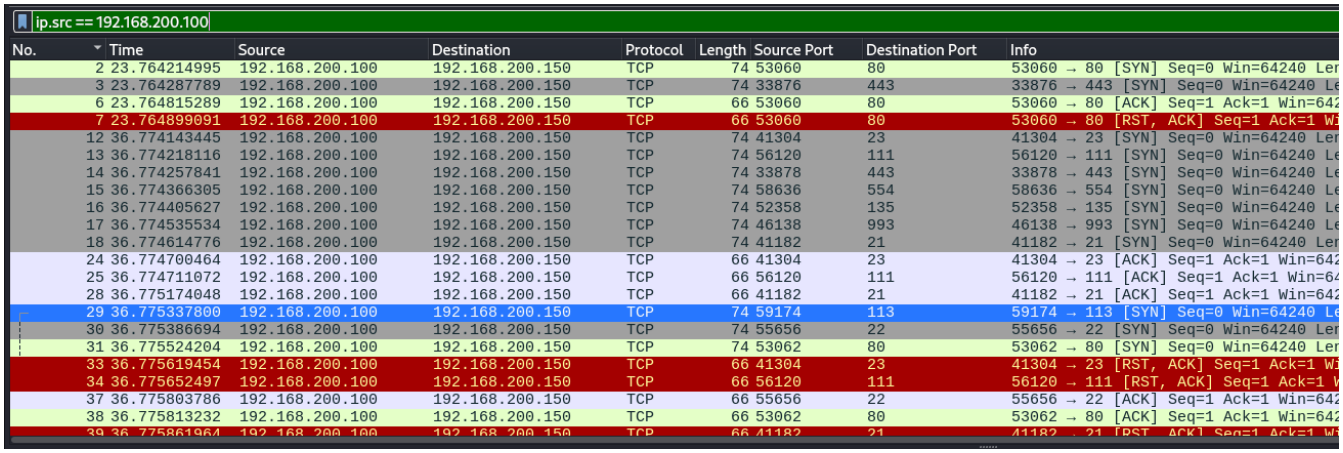
1) Scendendo notiamo subito come ci siano tantissimi pacchetti SYN, RST e ACK che è la cosa che ci insospettisce di più è quindi iniziamo a cercare applicando dei filtri per semplificare la ricerca.

Notiamo anche che le prime richieste SYN partono dall'indirizzo 192.168.200.100 deduciamo infatti che questo è l'ip dell'attaccante.



Source	Destination	Protocol	Length	Source Port	Destination Port	Info
192.168.200.150	192.168.200.255	BROWSER	286			Host Announcement METAS
192.168.200.100	192.168.200.150	TCP	74	53060	80	53060 → 80 [SYN] Seq=0
192.168.200.100	192.168.200.150	TCP	74	33876	443	33876 → 443 [SYN] Seq=0
192.168.200.150	192.168.200.100	TCP	74	80	53060	80 → 53060 [SYN, ACK] S
192.168.200.150	192.168.200.100	TCP	60	443	33876	443 → 33876 [RST, ACK]
192.168.200.100	192.168.200.150	TCP	66	53060	80	53060 → 80 [ACK] Seq=1
192.168.200.100	192.168.200.150	TCP	66	53060	80	53060 → 80 [RST, ACK] S
PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60			Who has 192.168.200.100
PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42			192.168.200.100 is at 0

Una volta capito ciò applichiamo un filtro che ci permette di vedere tutte le richieste partite dall'IP dell'attaccante, **ip.src== 192.168.200.100.**

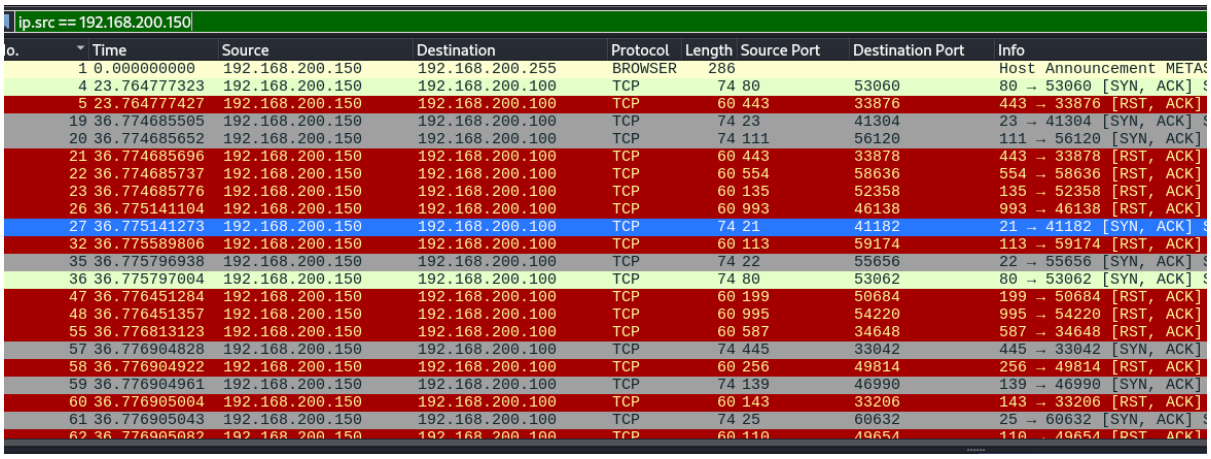


ip.src == 192.168.200.100

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060	80	53060 → 80 [SYN] Seq=0 Win=64240 Len
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876	443	33876 → 443 [SYN] Seq=0 Win=64240 Le
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060	80	53060 → 80 [ACK] Seq=1 Ack=1 Win=642
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060	80	53060 → 80 [RST, ACK] Seq=1 Ack=1 Wi
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304	23	41304 → 23 [SYN] Seq=0 Win=64240 Len
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120	111	56120 → 111 [SYN] Seq=0 Win=64240 Le
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878	443	33878 → 443 [SYN] Seq=0 Win=64240 Le
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636	554	58636 → 554 [SYN] Seq=0 Win=64240 Le
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358	135	52358 → 135 [SYN] Seq=0 Win=64240 Le
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138	993	46138 → 993 [SYN] Seq=0 Win=64240 Le
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182	21	41182 → 21 [SYN] Seq=0 Win=64240 Len
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304	23	41304 → 23 [ACK] Seq=1 Ack=1 Win=642
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120	111	56120 → 111 [ACK] Seq=1 Ack=1 Win=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182	21	41182 → 21 [ACK] Seq=1 Ack=1 Win=642
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174	113	59174 → 113 [SYN] Seq=0 Win=64240 Le
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656	22	55656 → 22 [SYN] Seq=0 Win=64240 Len
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062	80	53062 → 80 [SYN] Seq=0 Win=64240 Len
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304	23	41304 → 23 [RST, ACK] Seq=1 Ack=1 Wi
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120	111	56120 → 111 [RST, ACK] Seq=1 Ack=1 W
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656	22	55656 → 22 [ACK] Seq=1 Ack=1 Win=642
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062	80	53062 → 80 [ACK] Seq=1 Ack=1 Win=642
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182	21	41182 → 21 [RST, ACK] Seq=1 Ack=1 Wi

Notiamo anche che tutte le richieste partono da porte diverse verso porte della vittima.

Se poi mettiamo come filtro l'IP della vittima vediamo questo:



ip.src == 192.168.200.150

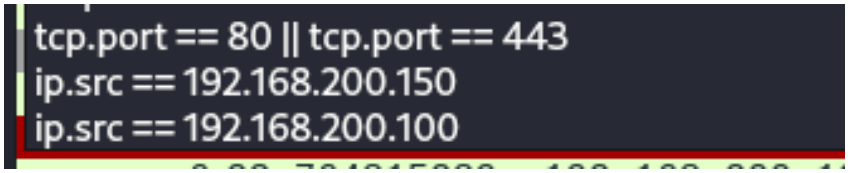
No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286			Host Announcement METAS
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80	53060	80 → 53060 [SYN, ACK] S
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443	33876	443 → 33876 [RST, ACK]
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23	41304	23 → 41304 [SYN, ACK] S
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111	56120	111 → 56120 [SYN, ACK]
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443	33878	443 → 33878 [RST, ACK]
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554	58636	554 → 58636 [RST, ACK]
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135	52358	135 → 52358 [RST, ACK]
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993	46138	993 → 46138 [RST, ACK]
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21	41182	21 → 41182 [SYN, ACK] S
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113	59174	113 → 59174 [RST, ACK]
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22	55656	22 → 55656 [SYN, ACK] S
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80	53062	80 → 53062 [SYN, ACK] S
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199	50684	199 → 50684 [RST, ACK]
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995	54220	995 → 54220 [RST, ACK]
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587	34648	587 → 34648 [RST, ACK]
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445	33042	445 → 33042 [SYN, ACK]
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256	49814	256 → 49814 [RST, ACK]
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139	46990	139 → 46990 [SYN, ACK]
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143	33206	143 → 33206 [RST, ACK]
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25	60632	25 → 60632 [SYN, ACK] S
62	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110	49654	110 → 49654 [RST, ACK]

Vediamo che ad alcune richieste viene data una risposta SYN, ACK mentre ad altre porte viene solo la richiesta RST, ACK.

questo ci fa pensare che questa possa essere una scansione NMAP, è che quando viene trovata una porta aperta il sistema della vittima invia una richiesta SYN, ACK e poi RST, ACK mentre nel caso di porta chiusa viene inviata solo il RST, ACK.

Abbiamo quindi stabilito che non ci sono evidenze di un attacco in corso ma comunque ci mette in allerta dato che in seguito ad una scansione NMAP può avvenire un attacco.

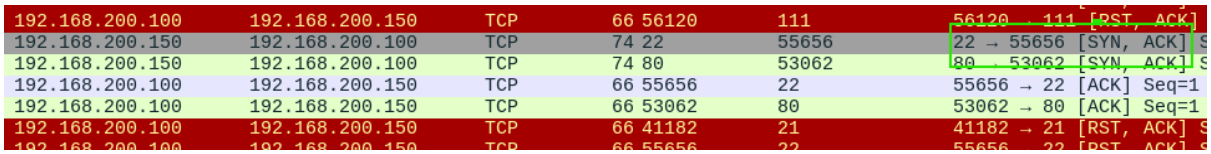
Altri filtri utilizzati:



Ip.src= serve per filtrare tutte le richieste lasciando solo quelle con l'ip sorgente richiesto.

Tcp.port==80 || tcp.port==443, serve per filtrare solo le richieste con protocollo tcp sulle porte 80 e 443.

2) Vettori d'attacco possibili:



Ci sono molti vettori d'attacco utilizzabili in seguito ad una scansione nmap come:

Attacchi sulle porte comuni:

Attacchi sulle porte comuni come 22 (ssh), 80(http) o 445(SMB).

Attacchi in base ai servizi, sappiamo che nmap può trovare anche la versione di servizi quindi ad esempio sulla porta 21(ftp) si può entrare in anonimo.

Attacchi ai sistemi operativi, nmap può trovare anche il sistema operativo che si trova sulla macchina della vittima è quindi l'attaccante può eseguire exploit tramite metasploit per avere una sessione meterpreter.

3) Non avendo trovato una evidenza d'attacco non possiamo parlare di mitigazione vera è propria ma comunque una scansione nmap può fornire molte informazioni che possono essere utili all'attaccante per costruire vettori d'attacco è quindi bisogna stare pronti difendendosi il più possibile:

1. Ridurre al minimo i servizi esposti, ovvero verificare che tutte le porte non utilizzate vengano chiuse quando possibile altrimenti protette ad esempio tramite un firewall.
2. Utilizzare sistemi di rilevamento (IDS/IPS)

3. Monitoraggio continuo della rete tramite software in modo da rilevare comportamenti anomali o IP sconosciuti (IP reputation check) è in modo da poter intervenire prima che l'attaccante possa acquisire dati privati.
4. Quando possibile aggiornare sempre i sistemi operativi e i servizi all'ultima versione.

Conclusione

Nonostante l'allert da parte del cliente possiamo tranquillizzarlo dicendo che non si tratta di un attacco ma semplicemente di una scansione che però comunque può portare alla creazione è poi all'utilizzo di un vettore d'attacco è quindi dobbiamo comunque fornirli delle best practices in modo da poter contrastare eventuali attacchi.