Esercizio S9-L3

Analisi di una cattura con Wireshark:

Per cominciare l'esercizio assegnato apriamo il file allegato con Wireshark sulla nostra macchina Kali e diamo un'occhiata generale per vedere di cosa si tratta.

No.	Time	Source	Destination	Protocol	Length	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 Workstati
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
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	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	28.775230099	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	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=810535437
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=810535437
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
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
28	36.775174048	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	36.775337800	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	36.775524204	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	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Analisi di una cattura con Wireshark:

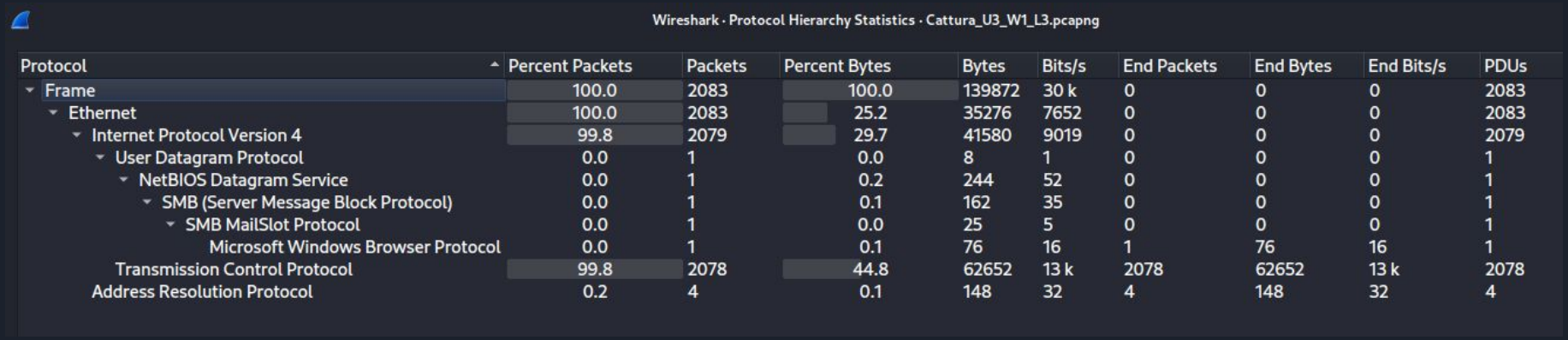
Il primo pacchetto analizzato da Wireshark ci dice che la macchina Metasploitable ha indirizzo IP 192.168.200.150 mentre la gran parte dei pacchetti successivi sembrano essere tutti protocollo TCP e molti di questi sono inviati da una macchina con indirizzo IP 192.168.200.100 verso diverse porte della macchina Metasploitable. A primo impatto sembrerebbe che una macchina stia effettuando un port scan verso Meta, andiamo ad analizzare più in dettaglio la cattura per confermare questa ipotesi.

Seguiamo il path in alto Statistics > Protocol Hierarchy per vedere più in dettaglio le informazioni sui protocolli dei pacchetti inviati.

Analisi di una cattura con Wireshark:

Da questa schermata possiamo vedere il totale dei pacchetti tracciati da Wireshark (2083) e possiamo vedere che il 99.8% di questi pacchetti sono di tipo TCP, mentre solo 4 sono di tipo ARP.

Proviamo adesso a passare ad un altra schermata seguendo il path Statistics > Conversations e premendo sul riquadro TCP ed in seguito una volta su Port B ed una volta su Packets A > B.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	2083	100.0	139872	30 k	0	0	0	2083
Ethernet	100.0	2083	25.2	35276	7652	0	0	0	2083
Internet Protocol Version 4	99.8	2079	29.7	41580	9019	0	0	0	2079
User Datagram Protocol	0.0	1	0.0	8	1	0	0	0	1
NetBIOS Datagram Service	0.0	1	0.2	244	52	0	0	0	1
SMB (Server Message Block Protocol)	0.0	1	0.1	162	35	0	0	0	1
SMB MailSlot Protocol	0.0	1	0.0	25	5	0	0	0	1
Microsoft Windows Browser Protocol	0.0	1	0.1	76	16	1	76	16	1
Transmission Control Protocol	99.8	2078	44.8	62652	13 k	2078	62652	13 k	2078
Address Resolution Protocol	0.2	4	0.1	148	32	4	148	32	4

Analisi di una cattura con Wireshark:

Qui possiamo osservare i pacchetti TCP inviati da 192.168.200.100 a Meta e messi in ordine ascendente delle porte, come possiamo osservare la macchina sta inviando pacchetti TCP a tutte le porte di Meta fino alla 1024 confermando l'ipotesi di un port scan. Possiamo osservare la colonna Packets e vedere che è segnato il numero 2 su molte porte, ciò significa che il three-way-handshake non è stato completato e la porta era chiusa.

Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 1026 | UDP · 1

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.200.100	37396	192.168.200.150	1	2	134 bytes	874	1	74 bytes	1	60 bytes	36.864770	0.0002
192.168.200.100	34748	192.168.200.150	2	2	134 bytes	292	1	74 bytes	1	60 bytes	36.806880	0.0002
192.168.200.100	58938	192.168.200.150	3	2	134 bytes	966	1	74 bytes	1	60 bytes	36.873582	0.0003
192.168.200.100	43056	192.168.200.150	4	2	134 bytes	557	1	74 bytes	1	60 bytes	36.832248	0.0003
192.168.200.100	54282	192.168.200.150	5	2	134 bytes	661	1	74 bytes	1	60 bytes	36.841442	0.0003
192.168.200.100	40874	192.168.200.150	6	2	134 bytes	212	1	74 bytes	1	60 bytes	36.798733	0.0003
192.168.200.100	52702	192.168.200.150	7	2	134 bytes	505	1	74 bytes	1	60 bytes	36.827912	0.0002
192.168.200.100	47720	192.168.200.150	8	2	134 bytes	124	1	74 bytes	1	60 bytes	36.790063	0.0001
192.168.200.100	41348	192.168.200.150	9	2	134 bytes	429	1	74 bytes	1	60 bytes	36.820242	0.0002
192.168.200.100	46014	192.168.200.150	10	2	134 bytes	216	1	74 bytes	1	60 bytes	36.799061	0.0002
192.168.200.100	37252	192.168.200.150	11	2	134 bytes	54	1	74 bytes	1	60 bytes	36.780326	0.0003
192.168.200.100	41700	192.168.200.150	12	2	134 bytes	793	1	74 bytes	1	60 bytes	36.854291	0.0002
192.168.200.100	58814	192.168.200.150	13	2	134 bytes	235	1	74 bytes	1	60 bytes	36.801464	0.0002
192.168.200.100	53648	192.168.200.150	14	2	134 bytes	382	1	74 bytes	1	60 bytes	36.815493	0.0003
192.168.200.100	42454	192.168.200.150	15	2	134 bytes	233	1	74 bytes	1	60 bytes	36.801319	0.0002

Analisi di una cattura con Wireshark:

In fondo possiamo trovare tutte le porte con numero di pacchetti 4, queste sono le porte in cui il three-way-handshake è stato completato.

Possiamo dunque concludere con certezza che la cattura di Wireshark ha tracciato un tentativo riuscito di port scan eseguito dalla macchina 192.168.200.100 verso la macchina Metasploitable e ha individuato 12 porte aperte.

192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	3	206 bytes	1	74 bytes	36.774615	0.0012
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	3	206 bytes	1	74 bytes	36.775387	0.0006
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	3	206 bytes	1	74 bytes	36.774143	0.0015
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	3	206 bytes	1	74 bytes	36.776512	0.0015
192.168.200.100	37282	192.168.200.150	53	4	280 bytes	21	3	206 bytes	1	74 bytes	36.776671	0.0014
192.168.200.100	53060	192.168.200.150	80	4	280 bytes	0	3	206 bytes	1	74 bytes	23.764215	0.0007
192.168.200.100	53062	192.168.200.150	80	4	280 bytes	11	3	206 bytes	1	74 bytes	36.775524	0.0005
192.168.200.100	56120	192.168.200.150	111	4	280 bytes	3	3	206 bytes	1	74 bytes	36.774218	0.0014
192.168.200.100	46990	192.168.200.150	139	4	280 bytes	17	3	206 bytes	1	74 bytes	36.776478	0.0014
192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	3	206 bytes	1	74 bytes	36.776386	0.0015
192.168.200.100	45648	192.168.200.150	512	4	280 bytes	68	3	206 bytes	1	74 bytes	36.781357	0.0006
192.168.200.100	42048	192.168.200.150	513	4	280 bytes	480	3	206 bytes	1	74 bytes	36.825398	0.0039
192.168.200.100	51396	192.168.200.150	514	4	280 bytes	118	3	206 bytes	1	74 bytes	36.788600	0.0011

Azioni di rimedio:

Per far in modo che la macchina Metasploitable sia meno vulnerabile a port scan futuri è consigliabile:

- Implementare un Firewall che rileva quando viene inviata una quantità elevata in poco tempo di richieste TCP e che blocchi le connessioni dalla macchina che sta inviando queste richieste.
- Spostare i servizi su porte non note: lo scan che abbiamo appena analizzato si è limitato a scansionare le prime 1024 porte, se i nostri servizi fossero stati spostati su porte meno note (ad esempio porte nel range 30.000-50.000) non sarebbero stati rilevati dallo scan.
- Eseguire port scan interni per essere sempre a conoscenza dello stato delle porte aperte e chiudere porte che non si usano più.