

Consegna S9L3:

Traccia:

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

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 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



Cattura_U3_W1_L3.pcapng

Andiamo ad aggiungere il file su Kali Linux, lo apriamo tramite WireShark ed abbiamo la seguente Cattura del traffico dati

Cattura_U3_W1_L3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

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 Se...
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=81052...
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=8105...
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 T...
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=42...
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 TSe...
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=81053...
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=8105...
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=8105...
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=8105...
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=8105...
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=8105...
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=81053...
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 T...
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 ...
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=42...
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=4...
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 T...
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=42...
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=8105...
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=81053...
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=81053...
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

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on i 0000 ff ff ff ff ff ff 08 00 27 fd 87 1e 08 00 45 00 ... E

Ethernet II, Src: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast 0010 01 10 00 00 40 00 40 11 26 f6 c0 a8 c8 96 c0 a8 ... @.@. &...

Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255 0020 c8 ff 00 8a 00 8a 00 fc 4b 01 11 0a 75 b4 c0 a8 ... K...u...

Da questo screenshot possiamo notare che la comunicazione avviene tramite due indirizzi IP, che sono i seguenti: 192.168.200.100 e 192.168.200.150

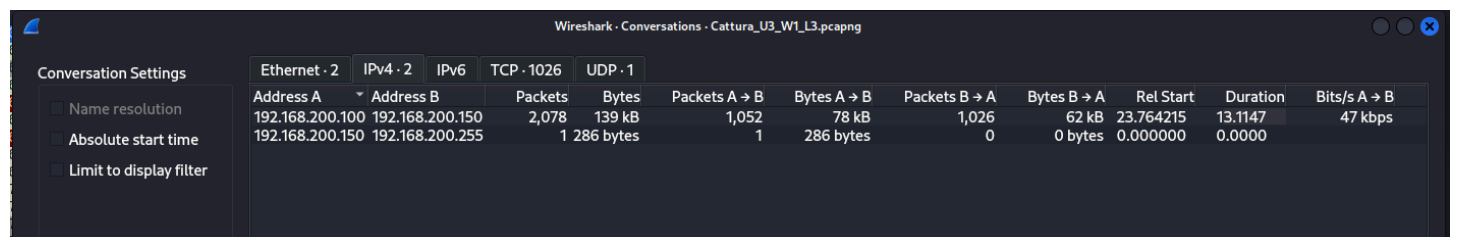
Possiamo anche notare che gli indirizzi IP cercano di connettersi ad alcune porte, alcune avvengono con successo mentre altre no. Grazie a questo possiamo notare che non si tratta di una semplice connessione, ma un vero e proprio tentativo da parte dell'attaccante di trovare qualche vulnerabilità, attaccando più porte.

192.168.200.150	TCP	74 41182 → 21 [SYN] Seq=0
192.168.200.100	TCP	74 23 → 41304 [SYN, ACK]
192.168.200.100	TCP	74 111 → 56120 [SYN, ACK]
192.168.200.100	TCP	60 443 → 33878 [RST, ACK]
192.168.200.100	TCP	60 554 → 58636 [RST, ACK]
192.168.200.100	TCP	60 135 → 52358 [RST, ACK]

Inoltre possiamo notare numerosi attacchi SYN e RST/ACK, infatti molto probabilmente si tratta di un port scanning da parte di un attaccante.

Numerosi sono anche gli attacchi RST/ACK, possono farci capire la presenza di un TCP reset, per interrompere le connessioni TCP tra gli host.

Analizzando meglio su Wireshark possiamo notare andando su “Statistiche, Conversation, IPV4” che la connessione è effettuata tra due indirizzi IP, e possiamo notare lo scambio di pacchetti inviati.



The image shows the Wireshark 'Conversations' window for the file 'Cattura_U3_W1_L3.pcapng'. The 'IPv4' tab is selected, showing a conversation between Address A (192.168.200.100) and Address B (192.168.200.150). The table below summarizes the data for this conversation.

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
192.168.200.100	192.168.200.150	2,078	139 kB	1,052	78 kB	1,026	62 kB	23.764215	13.1147	47 kbps
192.168.200.150	192.168.200.255	1	286 bytes	1	286 bytes	0	0 bytes	0.000000	0.0000	

Una possibile mitigazione puo essere sicuramente configurare le regole del firewall attraverso un indirizzo IP, in modo di respingere le richieste, questo puo essere eseguito attraverso Kali Linux eseguendo il comando “sudo iptables -A INPUT -s 192.168.200.150 -j DROP”.

Grazie alla Threat Intelligence abbiamo la possibilità di mitigare questo tipo di attacchi o quanto meno di anticipare le mosse dell’attaccante in modo che non possa adoperare con successo.