Task 17/01/25: Threat Intelligence & IOC

Traccia

Obiettivo dell'Esercizio:

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.

Passaggi da Seguire:

Analizzate la cattura attentamente e 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

Task 17/01/25: Threat Intelligence & IOC

Report

Introduzione:

Questo report analizza una cattura di traffico di rete contenente attività sospette, con particolare attenzione agli indicatori di compromissione (IOC). L'obiettivo è:

1. Identificare ed analizzare eventuali IOC.
2. Formulare ipotesi sui potenziali vettori di attacco utilizzati.
3. Proporre azioni per mitigare gli impatti dell'attacco e prevenire eventi futuri.

La cattura è stata analizzata con Wireshark e i dettagli principali sono documentati qui di seguito.

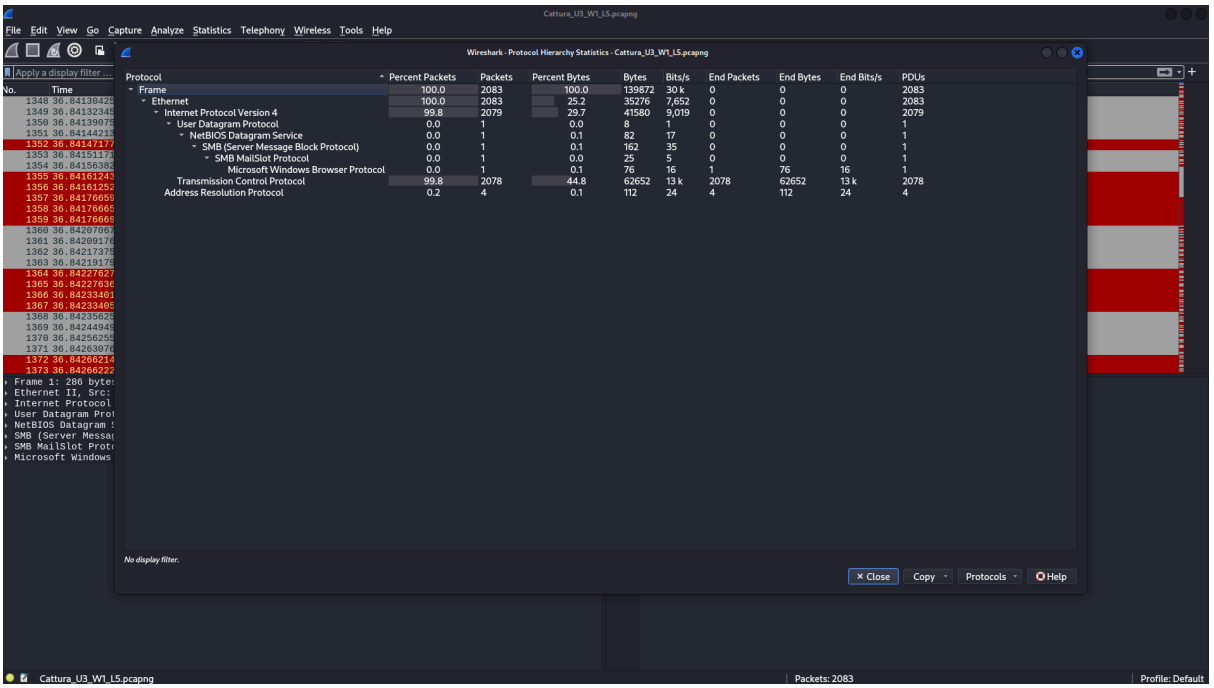
Indicatori di Compromissione (IOC)

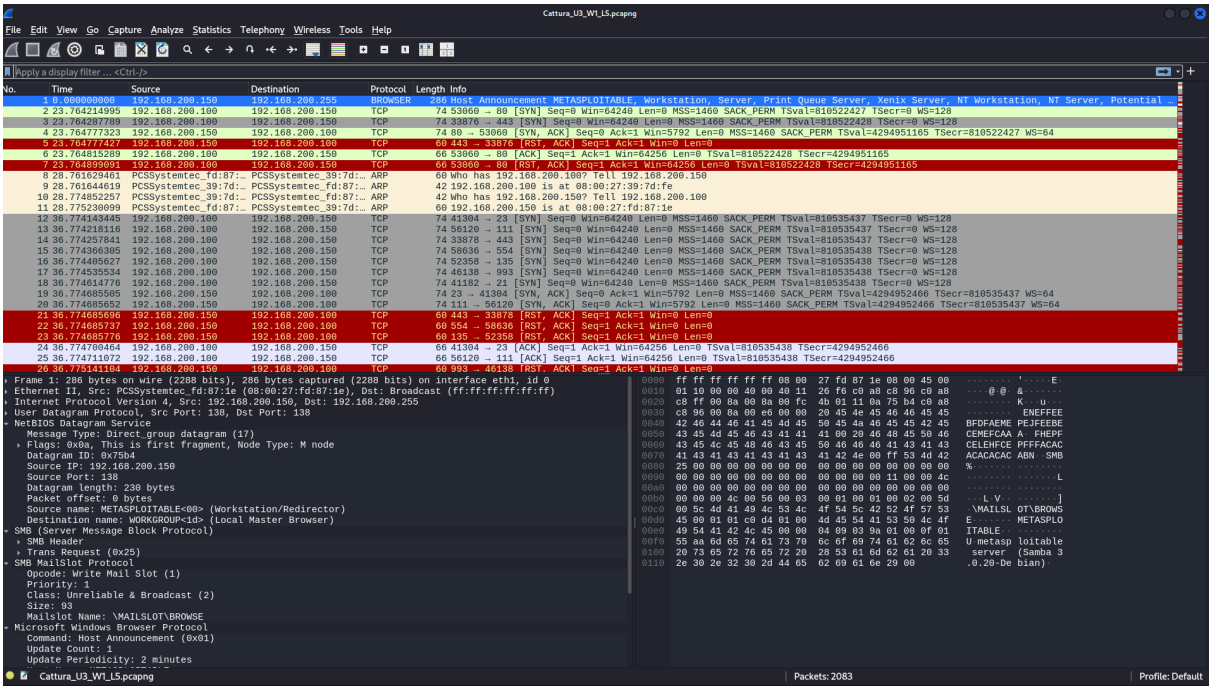
Traffico SMB sospetto

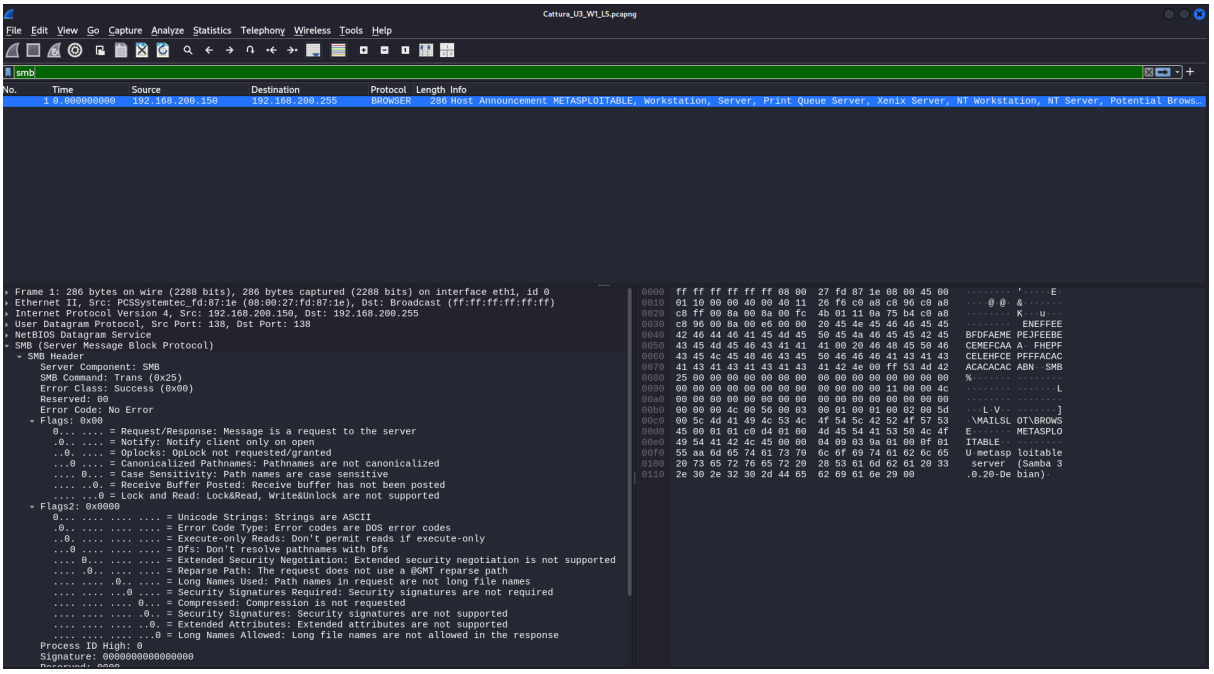
Dettagli: Sono stati identificati pacchetti SMB inviati in broadcast ("Host Announcement") provenienti dall'host 192.168.200.150.

Evidenze: Annuncio del servizio SMB con riferimento all'host METASPLOITABLE.

Porta utilizzata: 445 (tipica del protocollo SMB).







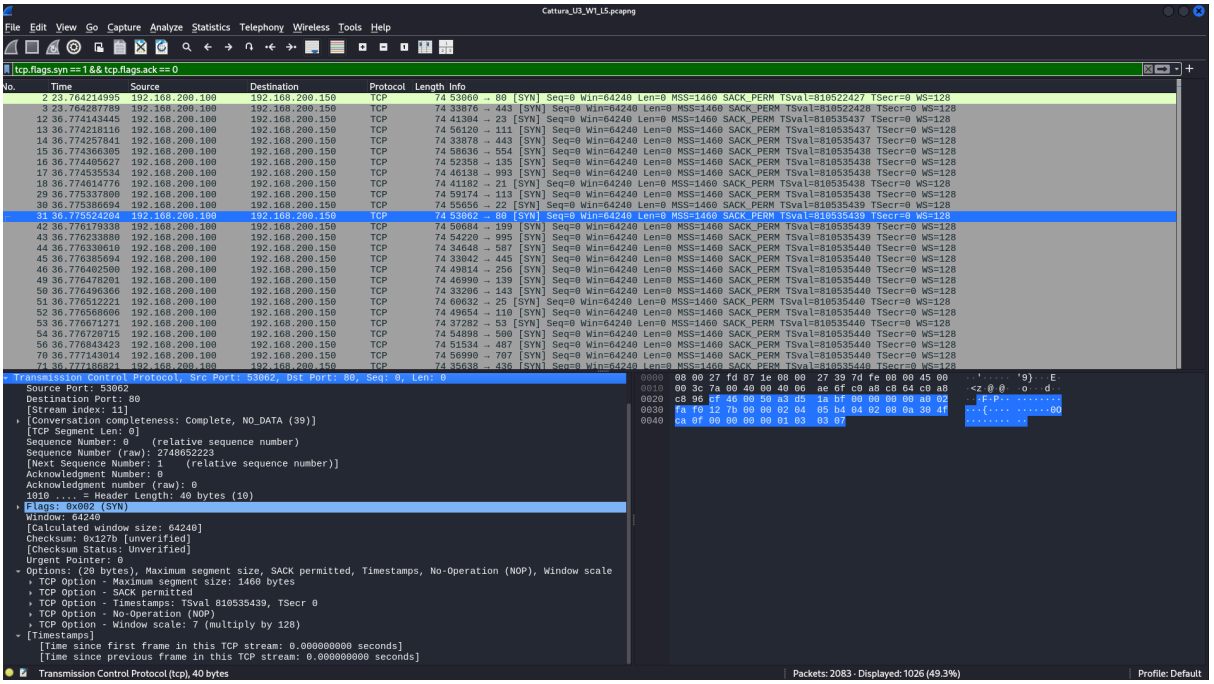
Tentativi di connessione TCP

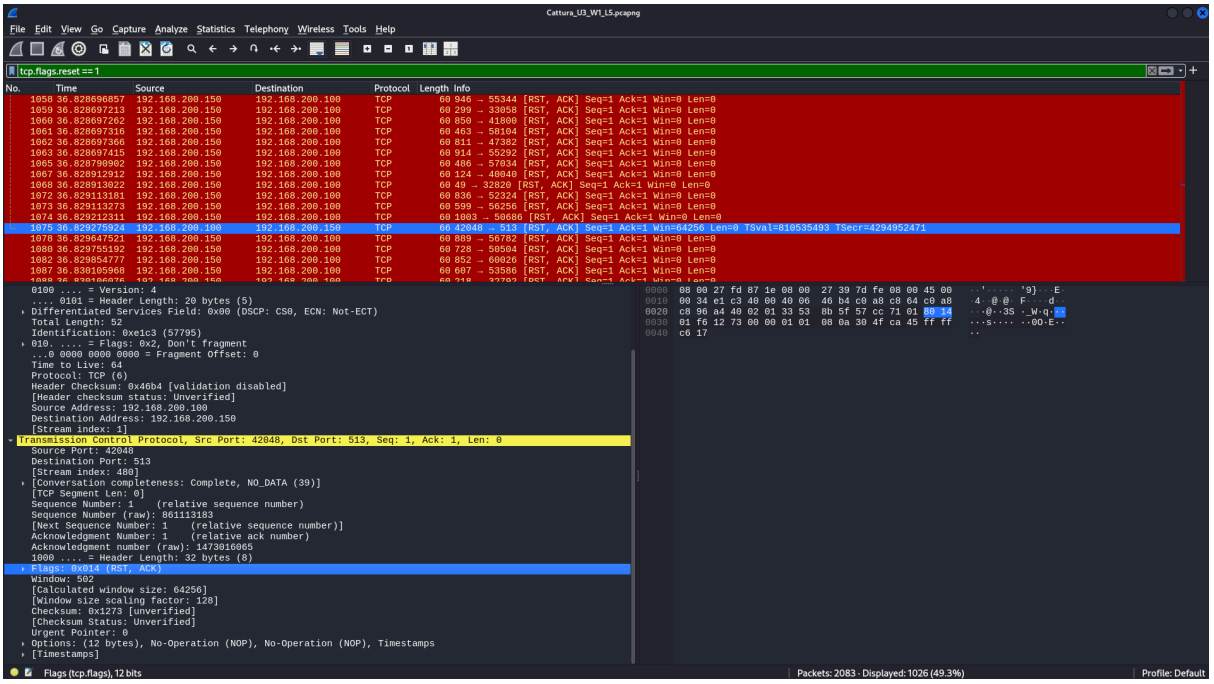
Dettagli: Sono stati rilevati numerosi pacchetti TCP SYN senza ACK successivi, indicando una possibile scansione delle porte.

Destinazione: porte 80 (HTTP) e 443 (HTTPS).

Evidenze:

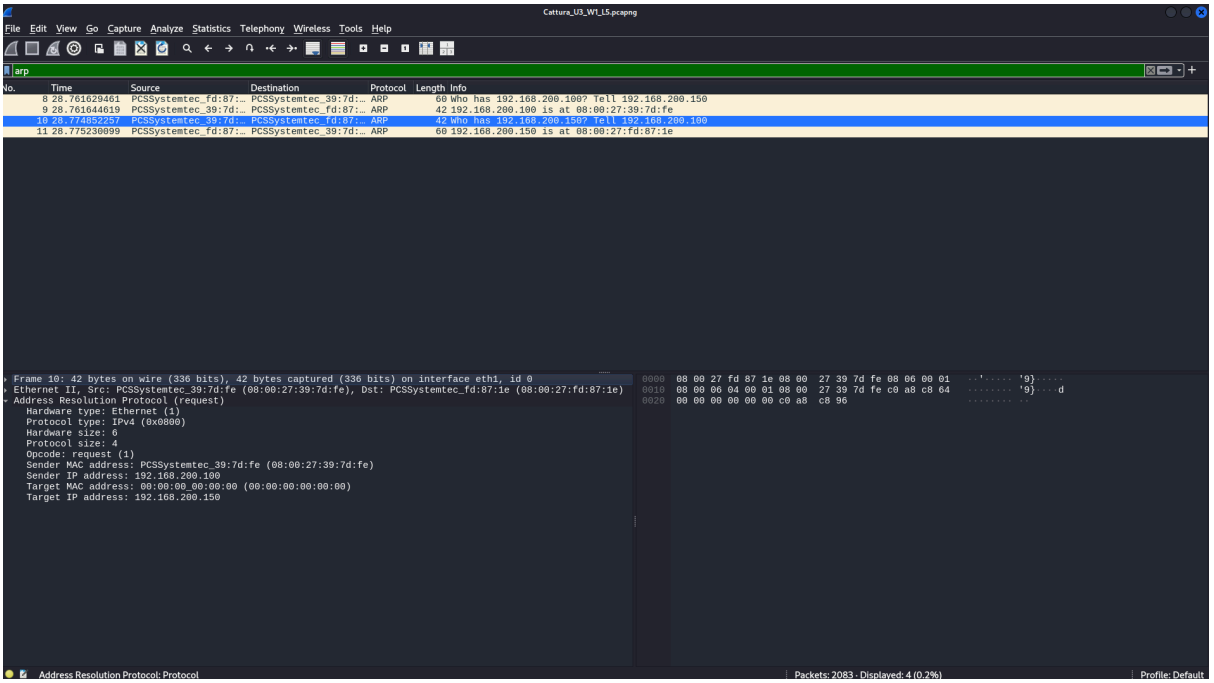
- attern di traffico tipico di una fase di ricognizione.
- Molti pacchetti hanno il flag RST, suggerendo connessioni interrotte o rifiutate.


Cattura_U3_W1_L5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 && tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
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
9 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
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 36.774360305 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
29 36.775337809 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
42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
49 36.776478201 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54 36.776720715 192.168.200.100 192.168.200.150 TCP 74 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
56 36.776843423 192.168.200.100 192.168.200.150 TCP 74 51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
70 36.777143014 192.168.200.100 192.168.200.150 TCP 74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
71 36.777418821 192.168.200.100 192.168.200.150 TCP 74 35038 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
Transmission Control Protocol, Src Port: 53062, Dst Port: 80, Seq: 0, Len: 0
Source Port: 53062
Destination Port: 80
[Stream index: 11]
[Conversation completeness: Complete, NO_DATA (39)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2748652223
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0x127b [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
TCP Option - Maximum segment size: 1460 bytes
TCP Option - SACK permitted
TCP Option - Timestamps: TSval 810535439, TSecr 0
TCP Option - No-Operation (NOP)
TCP Option - Window scale: 7 (multiply by 128)
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 3c 7a 00 40 00 40 06 ae 6f c0 a8 c8 64 c0 a8
0020 c8 96 cf 46 00 50 a3 d5 1a bf 00 00 00 00 a0 02
0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f
0040 ca 0f 00 00 00 00 01 03 03 07
Transmission Control Protocol (tcp), 40 bytes
Packets: 2083 · Displayed: 1026 (49.3%)
Profile: Default


Cattura_U3_W1_L5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.reset == 1
No. Time Source Destination Protocol Length Info
1058 36.828696857 192.168.200.150 192.168.200.100 TCP 60 946 → 55344 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1059 36.828697213 192.168.200.150 192.168.200.100 TCP 60 299 → 33058 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1060 36.828697262 192.168.200.150 192.168.200.100 TCP 60 850 → 41000 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1061 36.828697316 192.168.200.150 192.168.200.100 TCP 60 463 → 58104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1062 36.828697366 192.168.200.150 192.168.200.100 TCP 60 811 → 47382 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1063 36.828697415 192.168.200.150 192.168.200.100 TCP 60 914 → 55292 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1065 36.828790992 192.168.200.150 192.168.200.100 TCP 60 406 → 57034 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1067 36.828912912 192.168.200.150 192.168.200.100 TCP 60 124 → 40040 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1068 36.828913022 192.168.200.150 192.168.200.100 TCP 60 49 → 32820 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1072 36.829113181 192.168.200.150 192.168.200.100 TCP 60 836 → 52324 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1073 36.829113273 192.168.200.150 192.168.200.100 TCP 60 599 → 56256 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1074 36.829212311 192.168.200.150 192.168.200.100 TCP 60 1003 → 50686 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1075 36.829275924 192.168.200.100 192.168.200.150 TCP 66 42048 → 513 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535493 TSecr=4294952471
1078 36.829647521 192.168.200.150 192.168.200.100 TCP 60 889 → 56782 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1080 36.829755192 192.168.200.150 192.168.200.100 TCP 60 728 → 50504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1082 36.829854777 192.168.200.150 192.168.200.100 TCP 60 852 → 60026 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1087 36.830105968 192.168.200.150 192.168.200.100 TCP 60 607 → 53586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xe1c3 (57795)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x46b4 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.200.100
Destination Address: 192.168.200.150
[Stream index: 1]
Transmission Control Protocol, Src Port: 42048, Dst Port: 513, Seq: 1, Ack: 1, Len: 0
Source Port: 42048
Destination Port: 513
[Stream index: 480]
[Conversation completeness: Complete, NO_DATA (39)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 861113183
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1473016065
1000 .... = Header Length: 32 bytes (8)
Flags: 0x014 (RST, ACK)
Window: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0x1273 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 34 e1 c3 40 00 40 06 46 b4 c0 a8 c8 64 c0 a8
0020 c8 96 a4 40 02 01 33 53 8b 5f 57 cc 71 01 80 14
0030 01 f6 12 73 00 00 01 01 08 0a 30 4f ca 45 ff ff
0040 c6 17
Flags (tcp.flags), 12 bits
Packets: 2083 · Displayed: 1026 (49.3%)
Profile: Default

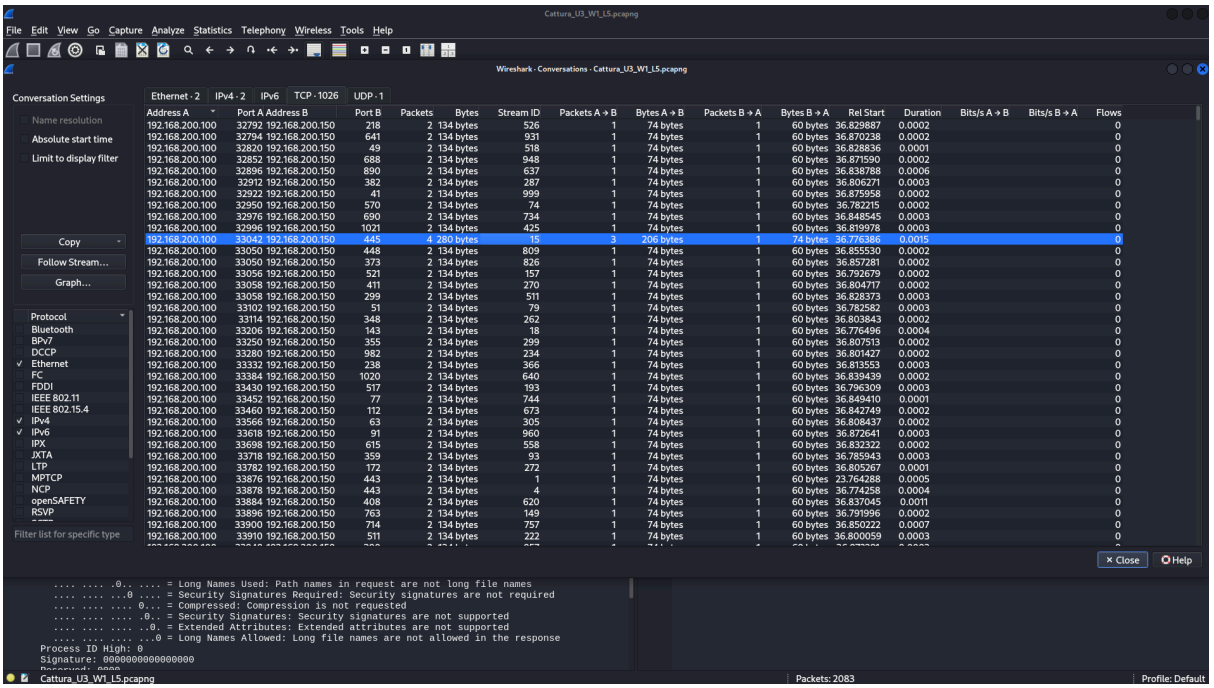
Traffico ARP sospetto

Diversi pacchetti ARP mostrano indirizzi MAC incompleti o non validi (00:00:00:00:00:00). Pattern tipico di un tentativo di ARP spoofing.



Statistiche delle conversazioni TCP/IPv4

Analizzando le conversazioni, emerge traffico significativo tra 192.168.200.100 e 192.168.200.150 sulla porta SMB (445).



Comportamento dell'attaccante

Ricognizione della rete

L'attaccante sembra aver eseguito un'operazione di ricognizione attiva attraverso traffico SMB e NetBIOS.

Pacchetti SMB inviati a un indirizzo broadcast (192.168.200.255), indicando un tentativo di scoprire dispositivi attivi nella rete che utilizzano SMB.

Questo è tipico di una scansione SMB per identificare host vulnerabili o configurazioni errate.

Scansione delle porte:

Tentativi di connessione TCP SYN su porte 80 (HTTP) e 443 (HTTPS) verso specifici indirizzi IP.

La mancanza di follow-up (ACK) indica che queste connessioni erano parte di una scansione delle porte per identificare quali servizi fossero attivi.

Potenziale sfruttamento di vulnerabilità

Focus su SMB:

L'uso di SMB/NetBIOS e la presenza dell'host METASPLOITABLE suggeriscono che l'attaccante potrebbe tentare di sfruttare vulnerabilità note come EternalBlue o altre falle comuni di Samba.

ARP Spoofing o Poisoning:

Il traffico ARP anomalo, inclusi pacchetti con indirizzi MAC non validi, potrebbe indicare un tentativo di compromettere la tabella ARP della rete e condurre un attacco man-in-the-middle.

Prove che indicano un'attività fallita o incompleta

Scansione delle porte:

I tentativi SYN sulle porte 80 e 443 non hanno avuto un follow-up (ACK), suggerendo che le connessioni non sono state stabilite. Questo indica che l'attaccante stava solo cercando di identificare quali servizi fossero disponibili, senza effettivamente accedervi.

Reset delle connessioni (RST):

Molti pacchetti TCP contengono il flag RST, che implica che le connessioni sono state terminate o rifiutate. Questo può indicare che non c'erano servizi attivi sulle porte scansionate e probabilmente un sistema di protezione (es., firewall o IDS) ha bloccato le richieste.

Traffico SMB/NetBIOS:

Anche se c'è traffico broadcast SMB, non ci sono evidenze di payload sospetti o exploit come EternalBlue. Il traffico sembra limitarsi alla scoperta di rete.

ARP Spoofing:

I pacchetti ARP sospetti non mostrano modifiche evidenti alle tabelle ARP, quindi l'attacco potrebbe essere stato tentato ma non completato.

Cosa potrebbe significare

Fase di preparazione: L'attaccante stava raccogliendo informazioni (quali dispositivi sono attivi, quali porte sono aperte) per pianificare un attacco futuro.

Attacco bloccato: Se sono in atto misure di sicurezza come firewall, segmentazione della rete o protezioni contro ARP spoofing, potrebbero aver impedito l'attacco.

Ipotesi sui vettori di attacco

Basandomi sugli IOC rilevati, posso formulare le seguenti ipotesi:

1. **Scansione SMB:**
    a. L'attaccante ha inviato pacchetti SMB per identificare dispositivi vulnerabili o con configurazioni errate.
    b. La presenza di METASPLOITABLE indica un host vulnerabile che potrebbe essere sfruttato.
2. **Scansione delle porte:**
    a. Tentativi di connessione SYN su porte 80 e 443 suggeriscono un tentativo di identificare servizi attivi nella rete.
3. **Possibile sfruttamento di vulnerabilità SMB:**
    a. La porta 445 (SMB) è stata utilizzata per comunicare con un dispositivo specifico, potenzialmente per sfruttare vulnerabilità note (es. EternalBlue).
4. **ARP Spoofing:**
    a. Pacchetti ARP anomali suggeriscono un tentativo di man-in-the-middle o di manipolazione della tabella ARP.

Azioni consigliate

Protezioni di rete

Segmentazione della rete: Isola i dispositivi critici utilizzando VLAN e limita la propagazione del traffico SMB/NetBIOS.

Regole di firewall: Blocca il traffico SMB/NetBIOS non richiesto (porte 445 e 139) e Monitora e filtra il traffico ARP.

Protezione degli endpoint

Aggiornamenti e patching: Aggiorna tutti i dispositivi per chiudere vulnerabilità note (soprattutto SMB) e rimuovi o isola macchine vulnerabili come METASPLOITABLE.

Hardening: Disabilita SMBv1 su tutti i dispositivi.

Monitoraggio e rilevamento

IDS/IPS: Configura regole per rilevare traffico SMB insolito e scansioni di rete e monitora pacchetti ARP con indirizzi sospetti.

Logging e revisione: Raccogli log dettagliati di firewall e dispositivi per individuare attività sospette.

Conclusioni

L'attacco osservato sembra essere stato limitato a una fase di ricognizione. Non ci sono evidenze di compromissione o sfruttamento di vulnerabilità, ma l'attaccante potrebbe aver raccolto informazioni utili per un attacco futuro.

Le azioni proposte mirano a mitigare i rischi identificati e a prevenire attacchi futuri con configurazioni di sicurezza più robuste.