

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.

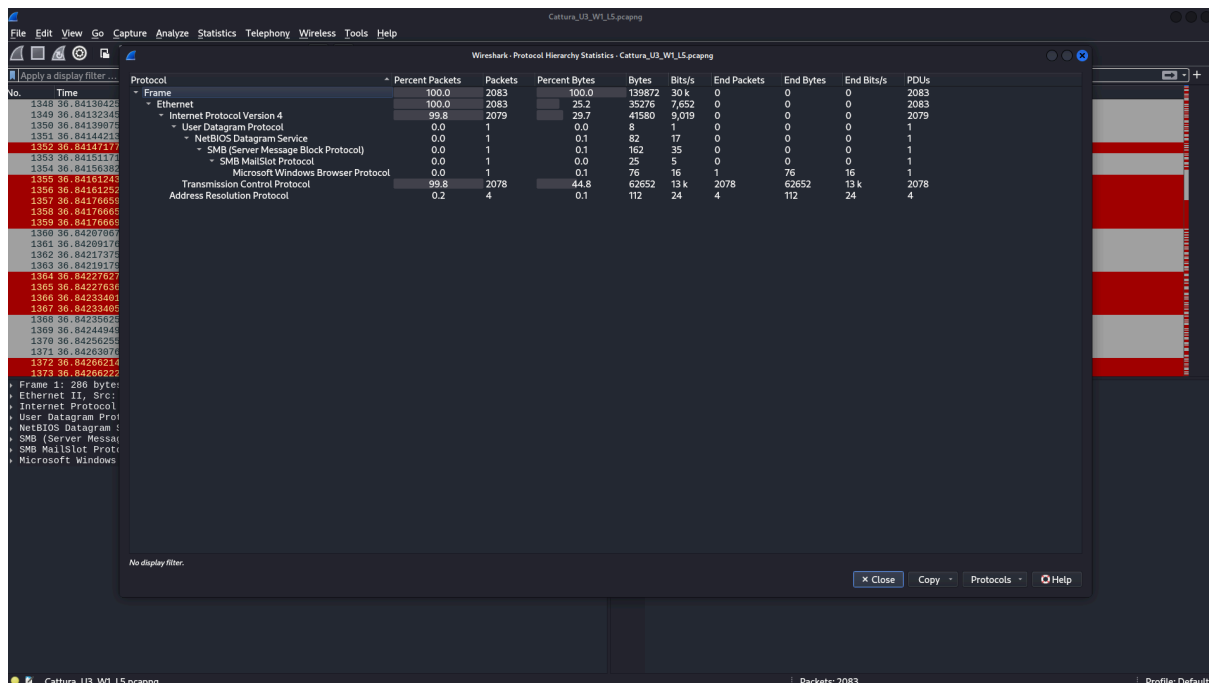
Indicatori di Compromissione (IOC)

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).



Cattura_U3_W1L5.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

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 Workstation, NT Server, Potential
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53860 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764297798	192.168.200.100	192.168.200.150	TCP	74	33878 -> 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777523	192.168.200.150	192.168.200.100	TCP	74	80 -> 53860 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=429495165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 -> 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815230	192.168.200.100	192.168.200.150	TCP	60	53860 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=429495165
7	23.764899991	192.168.200.100	192.168.200.150	TCP	60	53860 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=429495165
8	28.761629461	PCSSystemtec.fid:87:10	PCSSystemtec.39:7d:10	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec.39:7d:10	PCSSystemtec.fid:87:10	ARP	42	192.168.200.100 is at 08:00:27:fd:87:1e
10	28.774852527	PCSSystemtec.39:7d:10	PCSSystemtec.fid:87:10	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230999	PCSSystemtec.fid:87:10	PCSSystemtec.39:7d:10	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	30.774188451	192.168.200.100	192.168.200.150	TCP	74	43304 -> 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	30.774218116	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	30.774257841	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	30.774306305	192.168.200.100	192.168.200.150	TCP	74	53860 -> 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	30.774495627	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	30.774535534	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	30.774614776	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	30.774685595	192.168.200.100	192.168.200.150	TCP	74	23 -> 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	30.774685652	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=810535438 TSecr=4294952466
21	30.774685652	192.168.200.150	192.168.200.100	TCP	60	443 -> 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	30.774685737	192.168.200.150	192.168.200.100	TCP	60	554 -> 53860 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	30.774695776	192.168.200.150	192.168.200.100	TCP	60	105 -> 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	30.774700464	192.168.200.100	192.168.200.150	TCP	60	43304 -> 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=4294952466
25	30.774711872	192.168.200.100	192.168.200.150	TCP	60	56120 -> 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=4294952466
26	30.775111184	192.168.200.150	192.168.200.100	TCP	60	993 -> 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

Ethernet II, Src: PCSSystemtec.fid:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255

User Datagram Protocol, Src Port: 138, Dst Port: 138

NetBIOS Datagram Service

Message Type: Direct group datagram (17)

Flags: 0x00, This is first fragment, Node Type: M node

Datagram ID: 0x75b4

Source IP: 192.168.200.150

Source Port: 138

Datagram length: 238 bytes

Packet offset: 0 bytes

Source name: METASPLOITABLE-009 (Workstation/Redirector)

Destination name: WORKGROUP-1d3 (Local Master Browser)

SMB (Server Message Block Protocol)

SMB Header

Trans Request (0x25)

SMB Mailslot Protocol

Opcode: Write Mail Slot (1)

Priority: 1

Class: Unreliable & Broadcast (2)

Size: 93

Mailslot Name: \MAILSLOT\BROWSE

Microsoft Windows Browser Protocol

Command: Host Announcement (0x01)

Update Count: 1

Update Periodicity: 2 minutes

Cattura_U3_W1L5.pcapng

Packets: 2083

Profile: Default

Cattura_U3_W1L5.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smb

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 Workstation, NT Server, Potential Brows...

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

Ethernet II, Src: PCSSystemtec.fid:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255

User Datagram Protocol, Src Port: 138, Dst Port: 138

NetBIOS Datagram Service

SMB (Server Message Block Protocol)

Server Component: SMB

SMB Command: Trans (0x25)

Error Class: Success (0x00)

Reserved: 0000

Error Code: No Error

Flags: 0x00

0... .. = Request/Response: Message is a request to the server

0... .. = Notify: Notify client only on open

0... .. = Oplocks: Oplock not requested/granted

0... .. = Canonicalized Pathnames: Pathnames are not canonicalized

0... .. = Case Sensitivity: Path names are case sensitive

0... .. = Receive Buffer Posted: Receive buffer has not been posted

0... .. = Lock and Read: LockRead, WriteUnlock are not supported

Flags2: 0x0000

0... .. = Unicode Strings: Strings are ASCII

0... .. = Error Code Type: Error codes are DOS error codes

0... .. = Execute-only Reads: Don't permit reads if execute-only

0... .. = DFS: Don't resolve pathnames with DFS

0... .. = Extended Security Negotiation: Extended security negotiation is not supported

0... .. = Reparse Path: The request does not use a 0GMT reparse path

0... .. = Long Names Used: Path names in request are not long file names

0... .. = Security Signatures Required: Security signatures are not required

0... .. = Compressed: Compression is not requested

0... .. = Security Signatures: Security signatures are not supported

0... .. = Extended Attributes: Extended attributes are not supported

0... .. = Long Names Allowed: Long file names are not allowed in the response

Process ID High: 0

Signature: 0000000000000000

Reserved: 0000

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:

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

Capture_UI_WI_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	53860 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
13	23.774242989	192.168.200.100	192.168.200.150	TCP	74	53876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
12	23.774143445	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	30.774218110	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	30.774257441	192.168.200.100	192.168.200.150	TCP	74	53878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
15	30.774366395	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
16	30.774405627	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	30.774535534	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	30.774614776	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	30.775378900	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	30.775386504	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	30.775524294	192.168.200.100	192.168.200.150	TCP	74	53862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
42	30.776179338	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	30.776233889	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	30.776338610	192.168.200.100	192.168.200.150	TCP	74	34646 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	30.776385694	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	30.776492589	192.168.200.100	192.168.200.150	TCP	74	48614 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
49	30.776478291	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	30.776496366	192.168.200.100	192.168.200.150	TCP	74	33286 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	30.776512221	192.168.200.100	192.168.200.150	TCP	74	66632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52	30.776568096	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	30.776671271	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	30.776728715	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
59	30.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 407 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
70	30.777143814	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	30.777273892	192.168.200.100	192.168.200.150	TCP	74	35338 → 433 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128

Transmission Control Protocol, Src Port: 53862, Dst Port: 80, Seq: 0, Len: 0

Source Port: 53862
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
0100 = Header Length: 40 bytes (10)
Flags: 0x0000
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 00 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00 ...'...'9)...E
0010 00 3c 7a 00 40 00 40 06 ae 0f c0 a8 c8 64 c0 a8 ...<?@?o'd
0020 c8 96 ef 46 00 50 a3 05 1a bf 00 00 00 00 00 ...P.F.....
0030 00 12 7d 00 00 02 01 0c 04 00 00 00 00 00 ...P.....
0040 0a 0f 00 00 00 00 01 03 03 07 ...a.....

Packets: 2083 - Displayed: 1026 (49.3%) Profile: Default

Capture_UI_WI_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 → 33858 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1060	36.828697243	192.168.200.150	192.168.200.100	TCP	60	450 → 41880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1061	36.828697310	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	611 → 47382 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1063	36.828697415	192.168.200.150	192.168.200.100	TCP	60	614 → 55292 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1065	36.828798902	192.168.200.150	192.168.200.100	TCP	60	486 → 57834 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1067	36.828912912	192.168.200.150	192.168.200.100	TCP	60	124 → 48848 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1068	36.828913622	192.168.200.150	192.168.200.100	TCP	60	49 → 32920 [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 → 56066 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1075	36.829275924	192.168.200.100	192.168.200.150	TCP	66	42648 → 513 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535493 TSecr=4294952471
1076	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 → 50584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1082	36.829854777	192.168.200.150	192.168.200.100	TCP	60	852 → 68626 [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

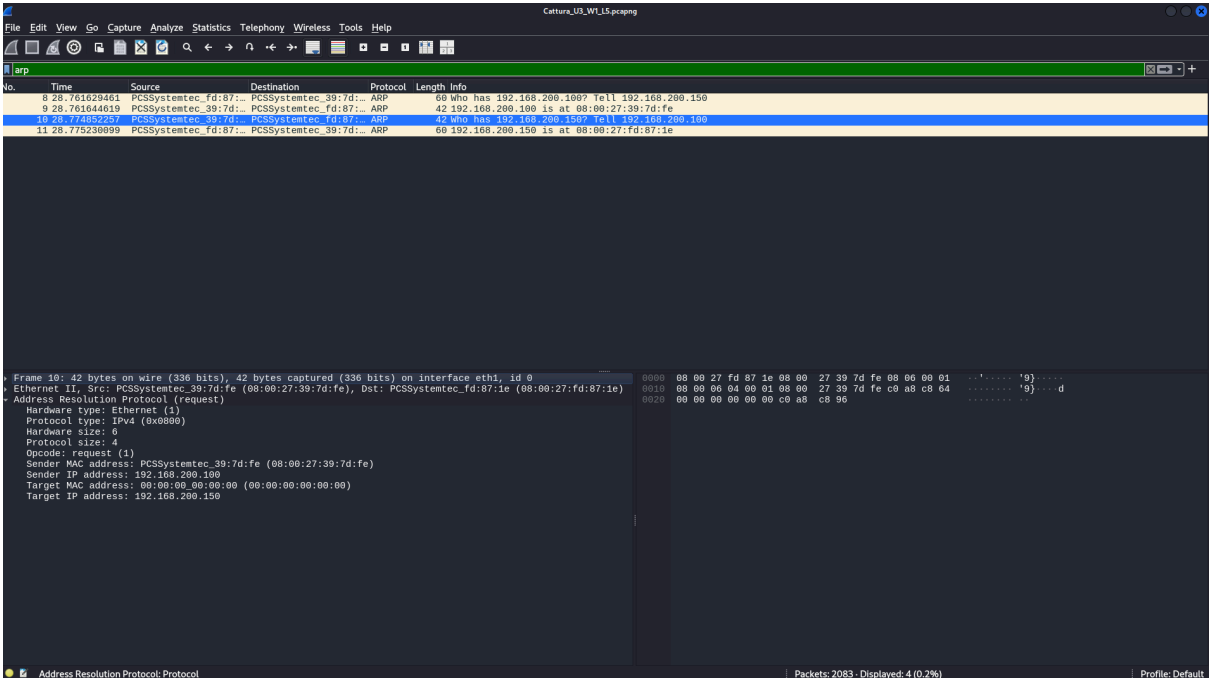
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x61c3 (57795)
... 010 = Flags: 0x2, Don't Fragment
... 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x46b4 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.200.150
Destination Address: 192.168.200.100
[Stream index: 1]
Transmission Control Protocol, Src Port: 42648, Dst Port: 513, Seq: 1, Ack: 1, Len: 0
Source Port: 42648
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): 1473016865
1000 = Header Length: 32 bytes (8)
Flags: 0x0000
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 00 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00 ...'...'9)...E
0010 00 34 e1 c3 4b 00 4b 00 40 b4 c9 a8 c8 64 c0 a8 ...4.??F...d
0020 c9 99 04 4b 02 01 35 53 8b 5f 57 c7 01 00 10 ...-?-5..W...
0030 01 f6 12 73 00 00 01 01 08 0a 30 4f ca 45 ff ff ...s.....'00E..
0040 c0 17 ...

Packets: 2083 - Displayed: 1026 (49.3%) Profile: Default

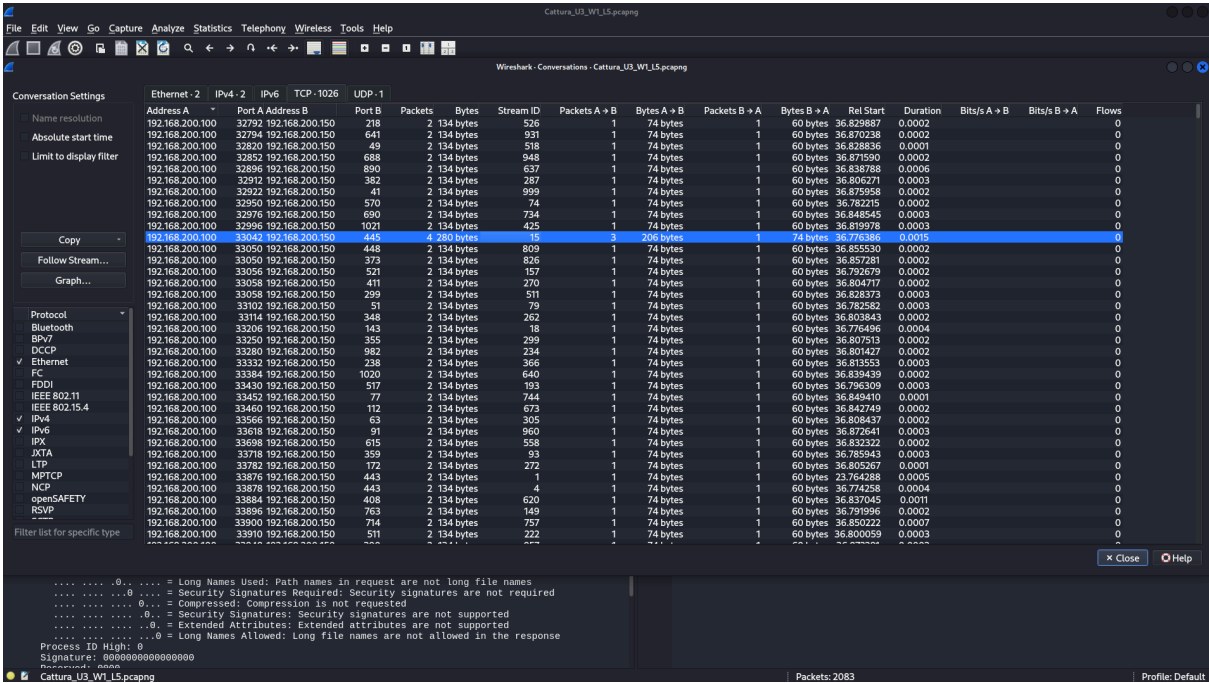
Traffico ARP sospetto

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.