Threat Intelligence & IOC

Progetto Unit 3 - Week 1

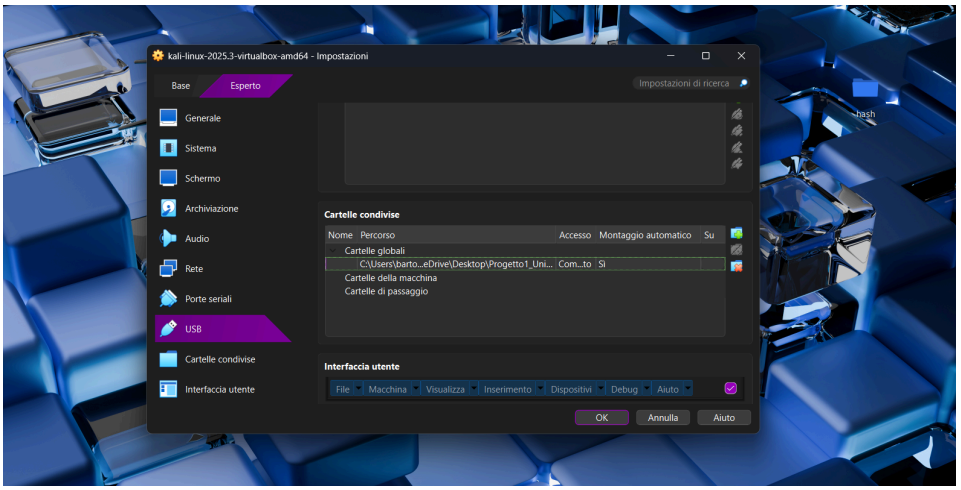
1. Obbiettivi

Analizzare una cattura di rete effettuata con Wireshark e rispondere ai seguenti requisiti:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigli su azioni per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

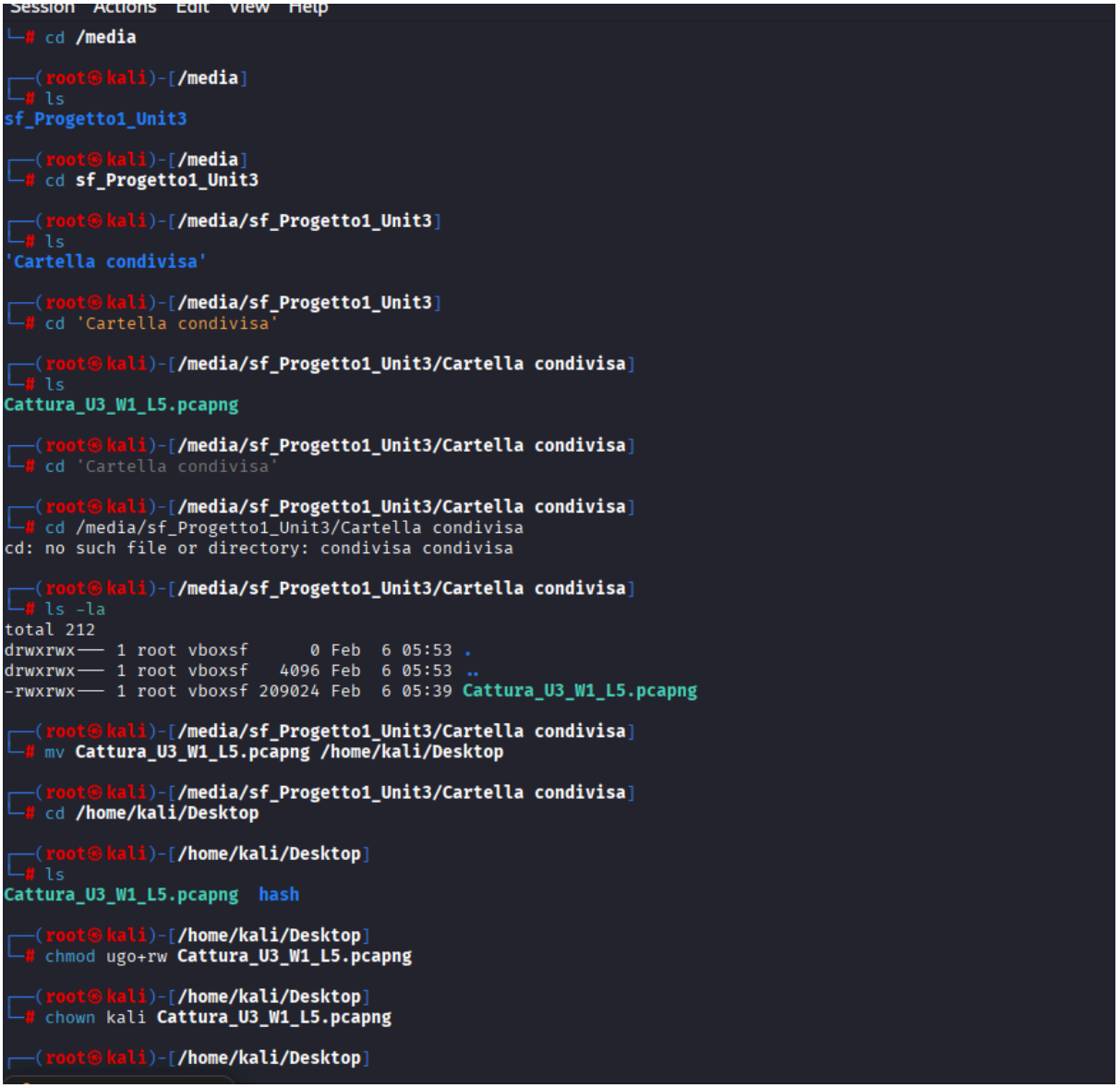
1.1 Trasferimento file su Kali

Creiamo una cartella condivisa tra il nostro sistema host e la Kali. Creiamo una cartella sul nostro host e specifichiamo nome e percorso, successivamente spostiamoci sulla Kali e configuriamo come di seguito



Per accedere al file di cattura su Kali Linux, navigare nella directory `/media` e spostare il file sul Desktop tramite il comando `mv`. Successivamente, assegnare i permessi necessari

all'utente per garantire l'accesso al documento. Infine, avviare l'analisi tecnica aprendo il file con un doppio click.



2. Executive Summary

Durante l'attività di monitoraggio dei log di rete, è stata rilevata un'anomalia significativa nel traffico tra due host della sottorete `192.168.200.0/24`. Un host non identificato ha avviato una scansione massiva delle porte (Port Scanning) verso un target critico denominato "METASPLOITABLE". L'attività è indicativa di una fase di **Reconnaissance** (ricognizione) volta a identificare servizi vulnerabili per un successivo exploit.

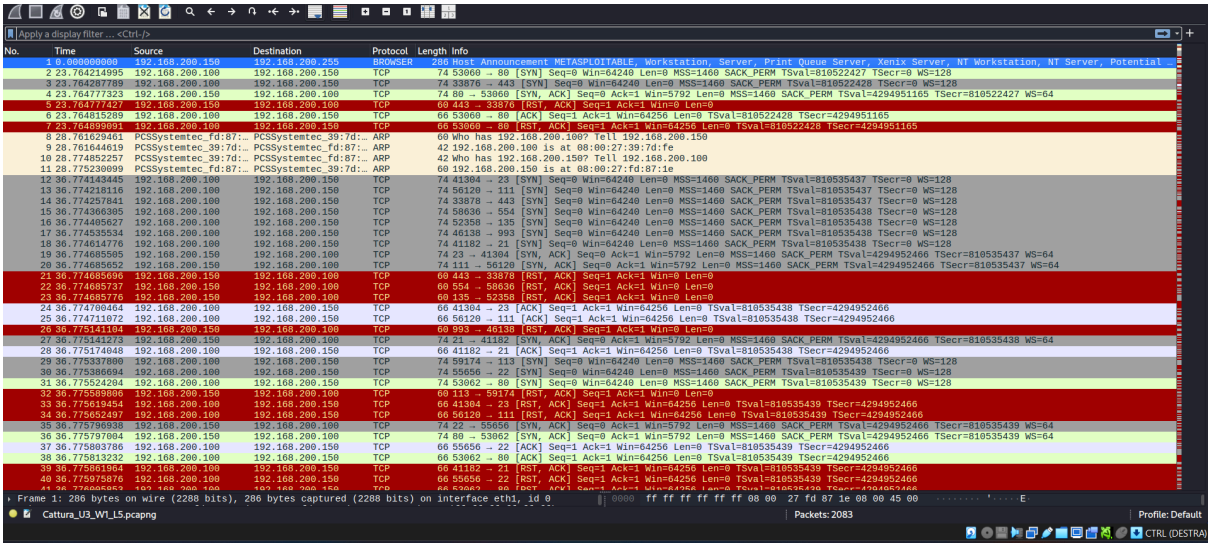
3. Analisi Tecnica e IOC (Indicators of Compromise)

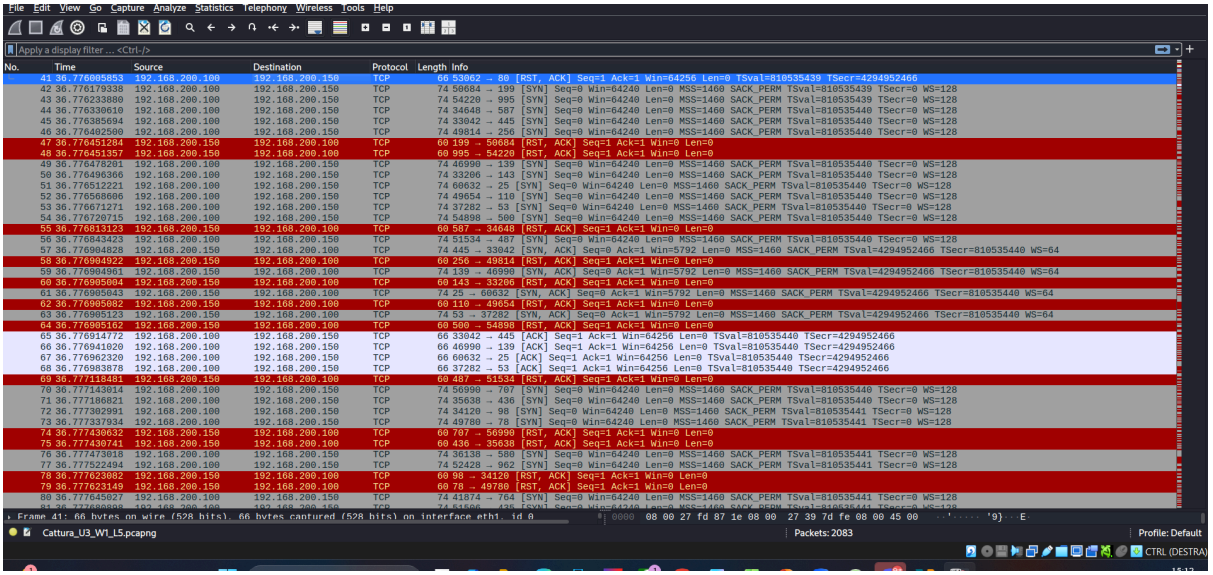
3.1 Dettagli degli Asset Coinvolti

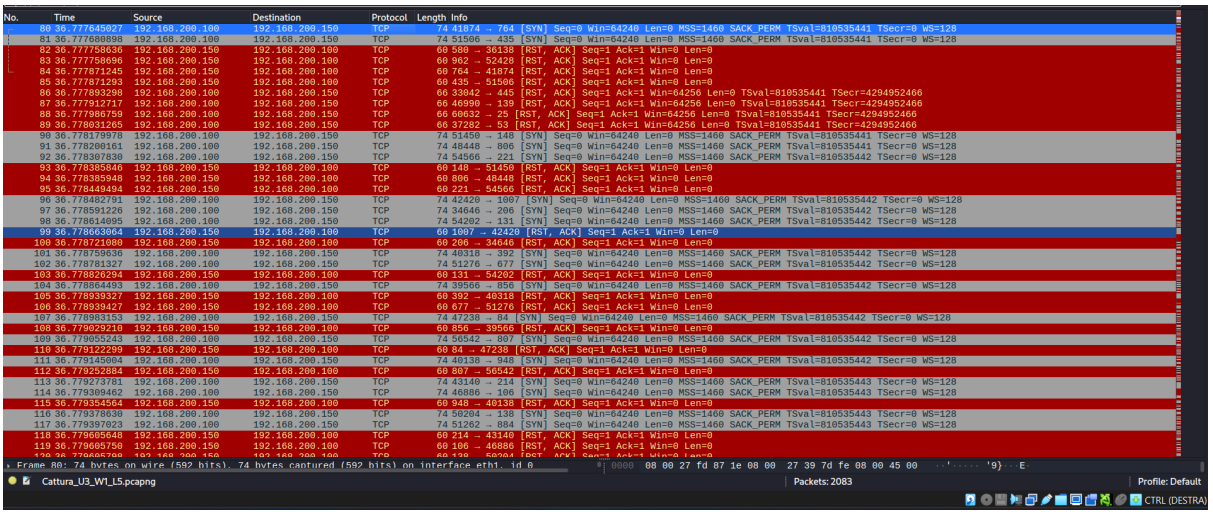
Ruolo	Indirizzo IP	Hostname Rilevato	Nota
Sorgente (Attaccante)	192.168.200.100	-	Probabile Kali Linux
Destinazione (Vittima)	192.168.200.150	METASPLOITABLE	Macchina vulnerabile

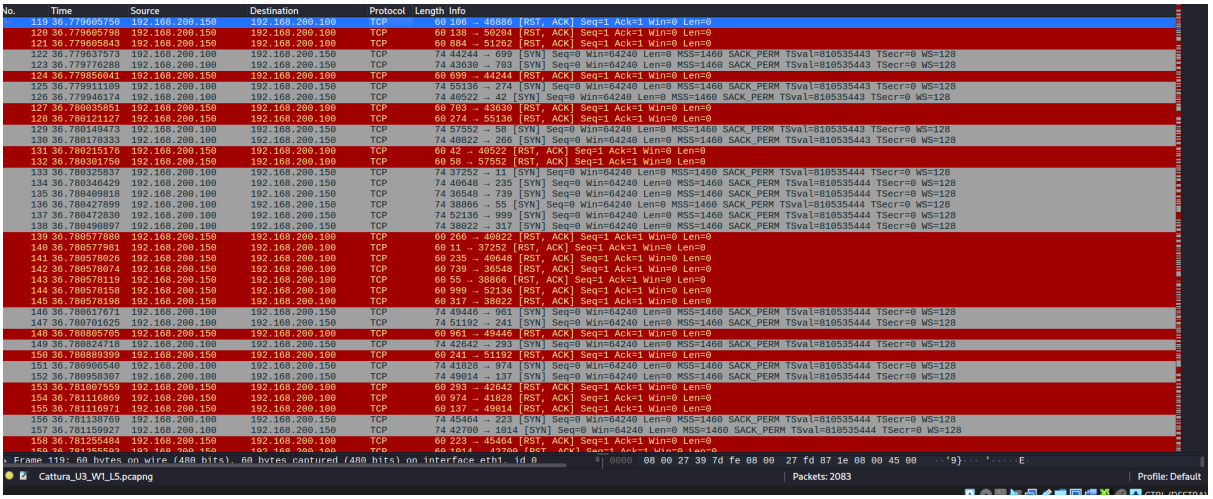
3.2 Fase di Discovery e Risoluzione Indirizzi

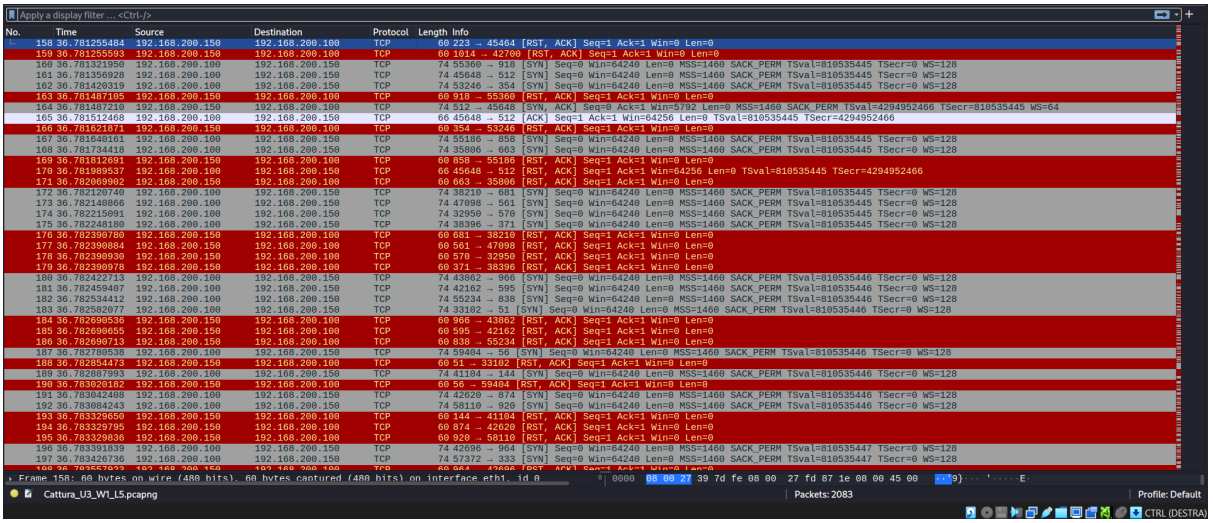
Dalle evidenze acquisite (Img 1), osserviamo un volume anomalo di traffico **TCP** diretto dall'host **192.168.200.100** verso l'host **192.168.200.150**.




File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
41 36.776005853 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
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 36.776233800 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
47 36.776451204 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 36.776451357 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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
55 36.776813123 192.168.200.150 192.168.200.100 TCP 60 587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56 36.776843423 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
57 36.776904828 192.168.200.150 192.168.200.100 TCP 74 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
58 36.776904922 192.168.200.150 192.168.200.100 TCP 60 256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 36.776904961 192.168.200.150 192.168.200.100 TCP 74 139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
60 36.776905004 192.168.200.150 192.168.200.100 TCP 60 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 36.776905043 192.168.200.150 192.168.200.100 TCP 74 25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
62 36.776905082 192.168.200.150 192.168.200.100 TCP 60 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 36.776905123 192.168.200.150 192.168.200.100 TCP 74 53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
64 36.776905162 192.168.200.150 192.168.200.100 TCP 60 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 36.776914772 192.168.200.100 192.168.200.150 TCP 66 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66 36.776941020 192.168.200.100 192.168.200.150 TCP 66 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67 36.776962320 192.168.200.100 192.168.200.150 TCP 66 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68 36.776983878 192.168.200.100 192.168.200.150 TCP 66 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69 36.777118401 192.168.200.150 192.168.200.100 TCP 60 407 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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 36.777186821 192.168.200.100 192.168.200.150 TCP 74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
72 36.777302991 192.168.200.100 192.168.200.150 TCP 74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
73 36.777337934 192.168.200.100 192.168.200.150 TCP 74 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
74 36.777430632 192.168.200.150 192.168.200.100 TCP 60 707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75 36.777430741 192.168.200.150 192.168.200.100 TCP 60 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76 36.777473018 192.168.200.100 192.168.200.150 TCP 74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
77 36.777522494 192.168.200.100 192.168.200.150 TCP 74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
78 36.777623082 192.168.200.150 192.168.200.100 TCP 60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36.777623149 192.168.200.150 192.168.200.100 TCP 60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80 36.777645027 192.168.200.100 192.168.200.150 TCP 74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
Frame 41: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth1, id 0
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
Cattura_U3_W1_L5.pcapng
Packets: 2083
Profile: Default
CTRL (DESTRA)


No. Time Source Destination Protocol Length Info
80 36.777645027 192.168.200.100 192.168.200.150 TCP 74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81 36.777688858 192.168.200.100 192.168.200.150 TCP 74 51206 → 455 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
82 36.777758636 192.168.200.150 192.168.200.100 TCP 60 580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83 36.777758696 192.168.200.150 192.168.200.100 TCP 60 962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 36.777871245 192.168.200.150 192.168.200.100 TCP 60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85 36.777871293 192.168.200.150 192.168.200.100 TCP 60 455 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86 36.777892398 192.168.200.100 192.168.200.150 TCP 66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87 36.777912717 192.168.200.100 192.168.200.150 TCP 66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88 36.777986759 192.168.200.100 192.168.200.150 TCP 66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89 36.778031265 192.168.200.100 192.168.200.150 TCP 66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90 36.778179976 192.168.200.100 192.168.200.150 TCP 74 51456 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
91 36.778200161 192.168.200.100 192.168.200.150 TCP 74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
92 36.778307830 192.168.200.100 192.168.200.150 TCP 74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
93 36.778385846 192.168.200.150 192.168.200.100 TCP 60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94 36.778385948 192.168.200.150 192.168.200.100 TCP 60 806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95 36.778449494 192.168.200.150 192.168.200.100 TCP 60 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96 36.778482791 192.168.200.100 192.168.200.150 TCP 74 42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
97 36.778591226 192.168.200.100 192.168.200.150 TCP 74 34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
98 36.778614095 192.168.200.100 192.168.200.150 TCP 74 54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
99 36.778663064 192.168.200.150 192.168.200.100 TCP 60 1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100 36.778721080 192.168.200.150 192.168.200.100 TCP 60 206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101 36.778759636 192.168.200.100 192.168.200.150 TCP 74 40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
102 36.778781327 192.168.200.100 192.168.200.150 TCP 74 51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
103 36.778820294 192.168.200.150 192.168.200.100 TCP 60 131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104 36.778864493 192.168.200.100 192.168.200.150 TCP 74 39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
105 36.778939327 192.168.200.150 192.168.200.100 TCP 60 392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106 36.778939427 192.168.200.150 192.168.200.100 TCP 60 677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107 36.778983153 192.168.200.100 192.168.200.150 TCP 74 47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
108 36.779029210 192.168.200.150 192.168.200.100 TCP 60 856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109 36.779055243 192.168.200.100 192.168.200.150 TCP 74 56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
110 36.779122289 192.168.200.150 192.168.200.100 TCP 60 84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111 36.779143904 192.168.200.100 192.168.200.150 TCP 74 40838 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
112 36.779252884 192.168.200.150 192.168.200.100 TCP 60 807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113 36.779273781 192.168.200.100 192.168.200.150 TCP 74 43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
114 36.779309462 192.168.200.100 192.168.200.150 TCP 74 46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
115 36.779354564 192.168.200.150 192.168.200.100 TCP 60 940 → 40838 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116 36.779378630 192.168.200.100 192.168.200.150 TCP 74 56204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
117 36.779397023 192.168.200.100 192.168.200.150 TCP 74 51262 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
118 36.779605648 192.168.200.150 192.168.200.100 TCP 60 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119 36.779605750 192.168.200.150 192.168.200.100 TCP 60 106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 80: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth1, id 0
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
Cattura_U3_W1_L5.pcapng
Packets: 2083
Profile: Default
CTRL (DESTRA)





- **Identificazione Host (Frame n. 1):** Grazie al protocollo `BROWSER`, viene catturato un annuncio di rete che identifica univocamente il target come **"METASPLOITABLE"**. Questo fornisce all'attaccante la conferma immediata di aver trovato un target vulnerabile.
- **Risoluzione ARP (Frame n. 8 - 11):** Prima di iniziare lo scambio TCP, osserviamo lo scambio di pacchetti **ARP (Address Resolution Protocol)**.
    - Il **Frame n. 10** mostra l'attaccante (`192.168.200.100`) che chiede: *"Who has 192.168.200.150?"*.
    - Questo passaggio conferma che l'attaccante sta operando nello stesso segmento di rete (Layer 2) e sta preparando la tabella di instradamento per l'attacco.

3.3 Analisi della Scansione TCP (Rif. Immagini 1 -> 6)

Una volta risolto l'indirizzo MAC, l'attaccante avvia la scansione sistematica.

- **Tentativi su Porte Note (Frame n. 2 - 40):** Già nella prima cattura osserviamo tentativi verso le porte più critiche:
    - **Porta 80 (HTTP)** e **443 (HTTPS)**: Frame n. 2 e 5.
    - **Porta 22 (SSH)** e **23 (Telnet)**: Frame n. 36 e 21.

    - **Porta 445 (SMB)**: Frame n. 32.
- **Pattern di Risposta (IOC):** L'analisi evidenzia una prevalenza di flag `[RST, ACK]` inviati dal target (es. **Frame n. 7, 33, 40**). Questo indica che il target sta attivamente rifiutando le connessioni su porte chiuse, ma rivela involontariamente la propria "reattività" all'attaccante.
- **Sequenzialità Temporale:** Osservando la colonna **Time**, si nota come tra il Frame n. 12 e il Frame n. 20 intercorrano solo **0.0003 secondi**. Una tale frequenza esclude categoricamente l'interazione umana, confermando l'uso di script automatizzati (Nmap).

---

4. Ipotesi sui Vettori di Attacco e Metodologia

Sulla base del comportamento rilevato, l'attacco si sta muovendo secondo la metodologia della **Cyber Kill Chain** nella sua fase iniziale.

4.1 Lo Strumento: Nmap (Network Mapper)

Il pattern di scansione (velocità, selezione delle porte e flag TCP utilizzati) è fortemente riconducibile all'uso di **Nmap**. L'attaccante lo sta usando per creare una mappa della superficie di attacco.

4.2 Obiettivi del Vettore di Attacco

L'attaccante non sta colpendo a caso. Cerca specificamente:

1. **Exploit del software (Vulnerability Mapping):** Una volta identificata una porta aperta (es. porta 80), l'attaccante cercherà di capire *quale* versione di server web è attiva per cercare una vulnerabilità nota (CVE) da sfruttare.
2. **Accesso tramite Credenziali Deboli:** Trovando porte come la 22 (SSH) o la 23 (Telnet), il passo successivo sarà un attacco "Brute Force" o "Dictionary Attack" per indovinare la password.

Spiegazione meno tecnica: L'attaccante non ha ancora "scassinato" nulla. Sta prendendo le misure delle serrature. Una volta scoperta una serratura vecchia o difettosa, tornerà con la chiave giusta (l'exploit) per entrare.

5. Matrice e Valutazione del Rischio

In ambito professionale, il rischio si calcola come: Rischio = Probabilità x Impatto

Fattore	Valutazione	Motivazione
Probabilità	**Alta**	L'attacco è in corso e automatizzato. Non è un evento casuale ma un'azione mirata.
Impatto	**Critico**	L'host target "Metasploitable" è progettato per contenere vulnerabilità gravi. Una violazione porterebbe alla perdita totale dei dati.
Rilevabilità	**Alta**	L'attacco è molto rumoroso e facilmente visibile con strumenti di monitoraggio.

5.2 Analisi del Rischio per il Business

Se questo attacco avesse successo, le conseguenze sarebbero:

- **Perdita di Riservatezza:** Accesso a dati sensibili dei clienti o della proprietà intellettuale.
- **Interruzione del Servizio:** L'attaccante potrebbe bloccare i sistemi (DDoS o Ransomware).
- **Danno Reputazionale:** Una violazione documentata mina la fiducia degli stakeholder e dei clienti.

Spiegazione meno tecnica: Anche se l'attacco è "solo" una scansione, il rischio è classificato come **Rosso (Critico)** perché il bersaglio scelto è una macchina molto vulnerabile. È come lasciare un caveau aperto: se qualcuno sta controllando se c'è la guardia, l'allarme deve scattare ora, prima che la guardia venga effettivamente aggirata.

---

6. Piano di Mitigazione e Raccomandazioni Strategiche

In questa fase, dividiamo gli interventi in base alla loro tempestività e al loro obiettivo: **Contenimento** (fermare l'incendio), **Bonifica** (pulire le ceneri) e **Prevenzione** (costruire una struttura ignifuga).

6.1 Azioni Immediate (Contenimento)

- **Interruzione del Traffico Malevolo:** Implementare una regola di blocco immediato (Blacklisting) sull'apparecchio di confine (Firewall o Router) per l'IP `192.168.200.100`.
    - *Comando suggerito (iptables):* `iptables -A INPUT -s 192.168.200.100 -j DROP`
- **Isolamento dell'Asset Compromesso:** Disconnettere temporaneamente l'host `192.168.200.150` dalla rete di produzione. Essendo un sistema "Metasploitable", la sua sola presenza rappresenta un rischio inaccettabile in un ambiente non protetto.

6.2 Interventi di Bonifica e Hardening (Breve Termine)

- **Chiusura delle Porte Non Necessarie:** Ridurre la superficie di attacco disattivando i servizi non critici. Se un servizio non è indispensabile, la sua porta deve essere chiusa.
- **Cifratura dei Protocolli:** Sostituire protocolli obsoleti e "in chiaro" rilevati durante la scansione (come Telnet o FTP) con controparti sicure (SSH, SFTP).
- **Cambio Credenziali:** Sebbene l'attacco rilevato fosse solo una scansione, è prassi cautelativa procedere al cambio di tutte le password amministrative dell'host target, ipotizzando che l'attaccante possa aver già tentato accessi silenti in precedenza.

6.3 Strategie di Prevenzione (Lungo Termine)

- **Difesa in Profondità (Defense in Depth):** Non affidarsi a un singolo firewall. Implementare più livelli di sicurezza, inclusi Antivirus/EDR sugli endpoint e segmentazione della rete tramite VLAN.
- **Implementazione di un IDS/IPS (Intrusion Detection/Prevention System):** Configurare sistemi come Snort o Suricata per bloccare automaticamente gli IP che mostrano pattern di "Port Scanning" prima che possano mappare l'intera rete.
- **Vulnerability Management:** Avviare scansioni programmate (es. con OpenVAS o Nessus) per identificare e patchare le vulnerabilità prima che lo faccia un attaccante esterno.

Spiegazione per i non tecnici: Immaginate la sicurezza della vostra azienda come quella di un castello. Le "Azioni Immediate" sono il ponte levatoio che si

alza per chiudere fuori l'intruso. Le "Strategie a Lungo Termine" sono le sentinelle sulle mura, i fossati e le serrature rinforzate su ogni singola porta interna. Non ci fidiamo solo del muro esterno, ma proteggiamo ogni singola stanza.

---

7. Conclusioni e Valutazione Finale

L'analisi del traffico di rete ha confermato senza ombra di dubbio un'attività di **ricognizione ostile mirata**. L'attaccante ha dimostrato di avere strumenti professionali e l'intento chiaro di mappare le vulnerabilità dell'infrastruttura.

Sintesi del Rischio Residuo

Nonostante il blocco dell'IP sorgente, il rischio residuo rimane **Moderato**. L'attaccante ora conosce l'esistenza del target `192.168.200.150` e potrebbe tentare un nuovo approccio utilizzando indirizzi IP diversi o tecniche più sofisticate (scansioni lente o frammentate).

L'incidente è stato rilevato in una fase precoce, evitando che la ricognizione si trasformasse in un'intrusione vera e propria. Tuttavia, la vulnerabilità intrinseca dell'host "Metasploitable" all'interno della rete suggerisce una revisione urgente delle policy di sicurezza interna.