

Threat Intelligence & IOC

Progetto Unit 3 - Week 1

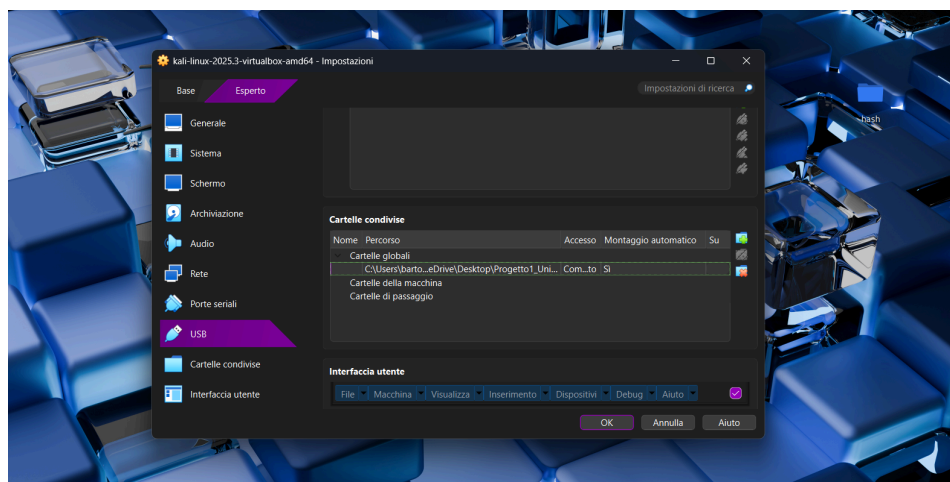
1. Obiettivi

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.

```
Session Actions Edit View Help
└─# cd /media

└─(root@kali)-[/media]
└─# ls
sf_Progetto1_Unit3

└─(root@kali)-[/media]
└─# cd sf_Progetto1_Unit3

└─(root@kali)-[/media/sf_Progetto1_Unit3]
└─# ls
'Cartella condivisa'

└─(root@kali)-[/media/sf_Progetto1_Unit3]
└─# cd 'Cartella condivisa'

└─(root@kali)-[/media/sf_Progetto1_Unit3/Cartella condivisa]
└─# ls
Cattura_U3_W1_L5.pcapng

└─(root@kali)-[/media/sf_Progetto1_Unit3/Cartella condivisa]
└─# cd 'Cartella condivisa'

└─(root@kali)-[/media/sf_Progetto1_Unit3/Cartella condivisa]
└─# cd /media/sf_Progetto1_Unit3/Cartella condivisa
cd: no such file or directory: condivisa condivisa

└─(root@kali)-[/media/sf_Progetto1_Unit3/Cartella condivisa]
└─# ls -la
total 212
drwxrwx— 1 root vboxsf 0 Feb 6 05:53 .
drwxrwx— 1 root vboxsf 4096 Feb 6 05:53 ..
-rwxrwx— 1 root vboxsf 209024 Feb 6 05:39 Cattura_U3_W1_L5.pcapng

└─(root@kali)-[/media/sf_Progetto1_Unit3/Cartella condivisa]
└─# mv Cattura_U3_W1_L5.pcapng /home/kali/Desktop

└─(root@kali)-[/media/sf_Progetto1_Unit3/Cartella condivisa]
└─# cd /home/kali/Desktop

└─(root@kali)-[/home/kali/Desktop]
└─# ls
Cattura_U3_W1_L5.pcapng hash

└─(root@kali)-[/home/kali/Desktop]
└─# chmod ugo+rw Cattura_U3_W1_L5.pcapng

└─(root@kali)-[/home/kali/Desktop]
└─# chown kali Cattura_U3_W1_L5.pcapng

└─(root@kali)-[/home/kali/Desktop]
```

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.

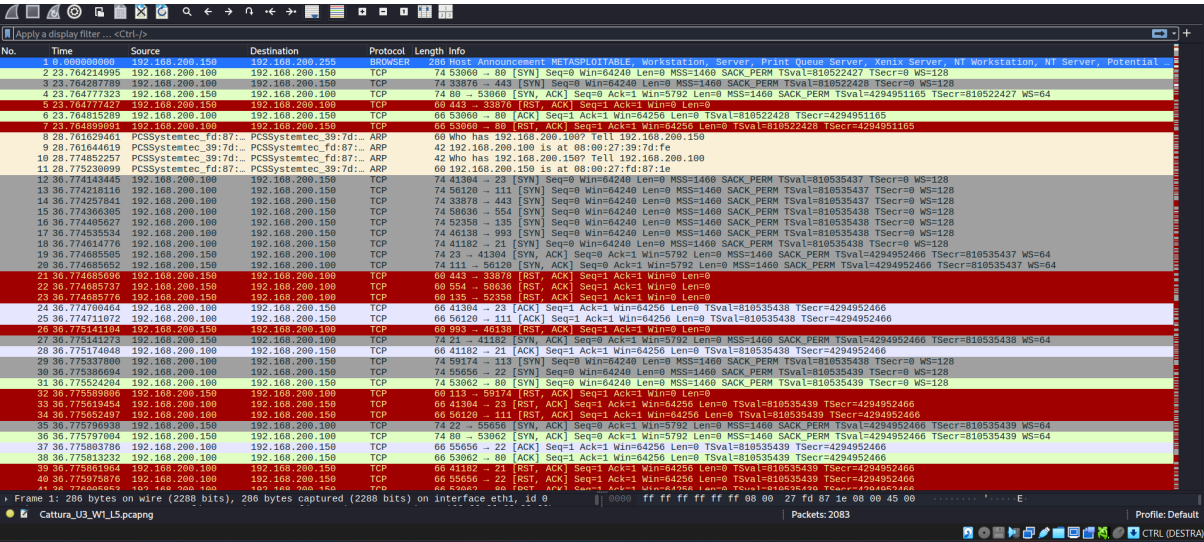
3. Analisi Tecnica e IOC (Indicators of Compromise)

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**.



No.	Time	Source	Destination	Protocol	Length	Info
41	36.77695583	192.168.200.100	192.168.200.150	TCP	60	55942 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4204952466
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	34640 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776358594	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	36.776402508	192.168.200.100	192.168.200.150	TCP	74	40814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	36.776515104	192.168.200.100	192.168.200.150	TCP	60	189 → 50584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.100	192.168.200.150	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	33200 → 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	36.776568696	192.168.200.100	192.168.200.150	TCP	74	49554 → 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	54888 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.100	192.168.200.150	TCP	60	587 → 34640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843123	192.168.200.100	192.168.200.150	TCP	74	51531 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
57	36.776904828	192.168.200.100	192.168.200.150	TCP	74	445 → 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
58	36.776945022	192.168.200.100	192.168.200.150	TCP	60	256 → 49514 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776949581	192.168.200.100	192.168.200.150	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	36.776959094	192.168.200.100	192.168.200.150	TCP	60	143 → 33200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776959843	192.168.200.100	192.168.200.150	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	36.776959892	192.168.200.100	192.168.200.150	TCP	60	110 → 49554 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776959123	192.168.200.100	192.168.200.150	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	36.776959162	192.168.200.100	192.168.200.150	TCP	60	500 → 54888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776944712	192.168.200.100	192.168.200.150	TCP	60	33842 → 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	60	46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36.776962329	192.168.200.100	192.168.200.150	TCP	60	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983078	192.168.200.100	192.168.200.150	TCP	60	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69	36.777118481	192.168.200.100	192.168.200.150	TCP	60	487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143614	192.168.200.100	192.168.200.150	TCP	74	50990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
71	36.777186021	192.168.200.100	192.168.200.150	TCP	74	33638 → 430 [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 → 90 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
73	36.777370334	192.168.200.100	192.168.200.150	TCP	74	49780 → 70 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
74	36.777435033	192.168.200.100	192.168.200.150	TCP	60	139 → 46990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430741	192.168.200.100	192.168.200.150	TCP	60	436 → 33638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473918	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	2428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
78	36.777623982	192.168.200.100	192.168.200.150	TCP	60	98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.100	192.168.200.150	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777658522	192.168.200.100	192.168.200.150	TCP	74	51534 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
81	36.777688808	192.168.200.100	192.168.200.150	TCP	74	54888 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128

No.	Time	Source	Destination	Protocol	Length	Info
82	36.777758630	192.168.200.100	192.168.200.150	TCP	60	580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.100	192.168.200.150	TCP	60	962 → 2428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.100	192.168.200.150	TCP	60	764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.100	192.168.200.150	TCP	60	435 → 51590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	60	33842 → 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	60	46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777980759	192.168.200.100	192.168.200.150	TCP	60	60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031005	192.168.200.100	192.168.200.150	TCP	60	37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90	36.778179970	192.168.200.100	192.168.200.150	TCP	74	51450 → 140 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128
91	36.778280161	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	192.168.200.100	192.168.200.150	TCP	60	148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385848	192.168.200.100	192.168.200.150	TCP	60	806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449404	192.168.200.100	192.168.200.150	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	192.168.200.100	192.168.200.150	TCP	60	1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721080	192.168.200.100	192.168.200.150	TCP	60	206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759530	192.168.200.100	192.168.200.150	TCP	74	51510 → 332 [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	192.168.200.100	192.168.200.150	TCP	60	131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778844493	192.168.200.100	192.168.200.150	TCP	74	33566 → 658 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
105	36.778939327	192.168.200.100	192.168.200.150	TCP	60	392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.100	192.168.200.150	TCP	60	677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778958153	192.168.200.100	192.168.200.150	TCP	74	41223 → 64 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
108	36.778922910	192.168.200.100	192.168.200.150	TCP	60	856 → 39586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.778955243	192.168.200.100	192.168.200.150	TCP	74	58542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
110	36.778919222	192.168.200.100	192.168.200.150	TCP	60	807 → 58542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145084	192.168.200.100	192.168.200.150	TCP	74	48138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535442 TSecr=0 WS=128
112	36.779252884	192.168.200.100	192.168.200.150	TCP	60	887 → 50542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779278781	192.168.200.100	192.168.200.150	TCP	74	43110 → 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	36.779345464	192.168.200.100	192.168.200.150	TCP	60	948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779376830	192.168.200.100	192.168.200.150	TCP	74	50504 → 183 [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	192.168.200.100	192.168.200.150	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779605160	192.168.200.100	192.168.200.150	TCP	60	106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779688700	192.168.200.100	192.168.200.150	TCP	60	183 → 50504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
110	36.779606750	192.168.200.150	192.168.200.100	TCP	60	190 - 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779607500	192.168.200.150	192.168.200.100	TCP	60	190 - 52384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779605843	192.168.200.150	192.168.200.100	TCP	60	884 - 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779537573	192.168.200.150	192.168.200.150	TCP	74	44244 - 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
123	36.779776289	192.168.200.150	192.168.200.150	TCP	74	43630 - 763 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
124	36.779556041	192.168.200.150	192.168.200.150	TCP	60	639 - 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779511109	192.168.200.150	192.168.200.150	TCP	74	55130 - 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
126	36.779946174	192.168.200.150	192.168.200.150	TCP	74	40822 - 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
127	36.780035551	192.168.200.150	192.168.200.100	TCP	60	793 - 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60	274 - 55130 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780132043	192.168.200.150	192.168.200.150	TCP	74	51552 - 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
130	36.780178333	192.168.200.150	192.168.200.150	TCP	74	40822 - 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535443 TSecr=0 WS=128
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60	42 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780303759	192.168.200.150	192.168.200.100	TCP	60	58 - 51552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325537	192.168.200.150	192.168.200.150	TCP	74	3125 - 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
134	36.780346429	192.168.200.150	192.168.200.150	TCP	74	40640 - 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
135	36.780409818	192.168.200.150	192.168.200.150	TCP	74	30540 - 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
136	36.780427899	192.168.200.150	192.168.200.150	TCP	74	38866 - 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
137	36.780472830	192.168.200.150	192.168.200.150	TCP	74	52130 - 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
138	36.780490997	192.168.200.150	192.168.200.150	TCP	74	30922 - 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
139	36.780577880	192.168.200.150	192.168.200.150	TCP	60	206 - 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60	11 - 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60	235 - 40640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60	739 - 30540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60	55 - 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578158	192.168.200.150	192.168.200.100	TCP	60	999 - 52130 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.150	192.168.200.150	TCP	60	317 - 30922 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780517671	192.168.200.150	192.168.200.150	TCP	74	49440 - 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
147	36.780571625	192.168.200.150	192.168.200.150	TCP	74	51172 - 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
148	36.780595705	192.168.200.150	192.168.200.100	TCP	60	961 - 49440 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	36.780824718	192.168.200.150	192.168.200.150	TCP	74	42642 - 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
150	36.780893930	192.168.200.150	192.168.200.100	TCP	60	242 - 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780909049	192.168.200.150	192.168.200.150	TCP	74	41135 - 914 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
152	36.780958307	192.168.200.150	192.168.200.150	TCP	74	49014 - 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
153	36.781007350	192.168.200.150	192.168.200.150	TCP	74	40640 - 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
154	36.781116809	192.168.200.150	192.168.200.150	TCP	60	914 - 41820 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781116971	192.168.200.150	192.168.200.150	TCP	60	137 - 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	36.781150769	192.168.200.150	192.168.200.150	TCP	74	45454 - 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
157	36.781150927	192.168.200.150	192.168.200.150	TCP	74	42709 - 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
158	36.781255484	192.168.200.150	192.168.200.150	TCP	60	223 - 45454 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	36.781255484	192.168.200.150	192.168.200.150	TCP	60	45454 - 45454 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
159	36.781255484	192.168.200.150	192.168.200.100	TCP	60	223 - 45454 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	36.781255593	192.168.200.150	192.168.200.100	TCP	60	1014 - 42709 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
169	36.781321950	192.168.200.150	192.168.200.150	TCP	74	55360 - 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
161	36.781350828	192.168.200.150	192.168.200.150	TCP	74	45648 - 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
162	36.781326319	192.168.200.150	192.168.200.150	TCP	74	53240 - 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
163	36.781487105	192.168.200.150	192.168.200.150	TCP	60	918 - 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	36.781487218	192.168.200.150	192.168.200.150	TCP	74	512 - 45648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
165	36.781512409	192.168.200.150	192.168.200.150	TCP	60	45648 - 512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166	36.781621871	192.168.200.150	192.168.200.150	TCP	60	354 - 53240 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	36.781640351	192.168.200.150	192.168.200.150	TCP	74	55180 - 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
168	36.781734418	192.168.200.150	192.168.200.150	TCP	74	35806 - 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
169	36.781812691	192.168.200.150	192.168.200.150	TCP	60	858 - 55180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	36.781899537	192.168.200.150	192.168.200.150	TCP	60	45648 - 512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
171	36.782009902	192.168.200.150	192.168.200.150	TCP	60	663 - 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	36.782120740	192.168.200.150	192.168.200.150	TCP	74	38210 - 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
173	36.782140866	192.168.200.150	192.168.200.150	TCP	74	47098 - 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
174	36.782215091	192.168.200.150	192.168.200.150	TCP	74	32950 - 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
175	36.782248180	192.168.200.150	192.168.200.150	TCP	74	38396 - 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535445 TSecr=0 WS=128
176	36.782309108	192.168.200.150	192.168.200.150	TCP	60	371 - 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	36.782398084	192.168.200.150	192.168.200.150	TCP	60	561 - 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	36.782398084	192.168.200.150	192.168.200.150	TCP	60	570 - 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	36.782399078	192.168.200.150	192.168.200.150	TCP	60	371 - 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	36.782422713	192.168.200.150	192.168.200.150	TCP	74	44306 - 960 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
181	36.782459407	192.168.200.150	192.168.200.150	TCP	74	42162 - 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
182	36.782534412	192.168.200.150	192.168.200.150	TCP	74	55234 - 830 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
183	36.782582077	192.168.200.150	192.168.200.150	TCP	74	33102 - 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
184	36.782690536	192.168.200.150	192.168.200.150	TCP	60	960 - 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	36.782690555	192.168.200.150	192.168.200.150	TCP	60	505 - 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	36.782690673	192.168.200.150	192.168.200.150	TCP	60	830 - 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	36.782780538	192.168.200.150	192.168.200.150	TCP	74	59484 - 50 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
188	36.782851713	192.168.200.150	192.168.200.150	TCP	60	50 - 59484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	36.782897993	192.168.200.150	192.168.200.150	TCP	74	41114 - 114 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
190	36.783020182	192.168.200.150	192.168.200.150	TCP	60	50 - 59484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	36.783084209	192.168.200.150	192.168.200.150	TCP	74	45648 - 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
192	36.783084243	192.168.200.150	192.168.200.150	TCP	74	58110 - 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535446 TSecr=0 WS=128
193	36.783239550	192.168.200.150	192.168.200.150	TCP	60	144 - 41184 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	36.783329795	192.168.200.150	192.168.200.150	TCP	60	974 - 6260 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	36.783239836	192.168.200.150	192.168.200.150	TCP	60	920 - 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	36.783391839	192.168.200.150	192.168.200.150	TCP	74	42696 - 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535447 TSecr=0 WS=128
197	36.783426736	192.168.200.150	192.168.200.150	TCP	74	517372 - 333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535447 TSecr=0 WS=128
198	36.783567599	192.168.200.150	192.168.200.150	TCP	60	964 - 42696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- **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: $\text{Rischio} = \text{Probabilità} \times \text{Impatto}$

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.