TRACCIA ESERCIZIO W9L5

EPICODE

Esercizio
Threat Intelligence & IOC

Traccia:

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

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.
Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare 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

Cattura_U3_W1_L3.pcapng

EPICODE

Esercizio
Threat Intelligence & IOC

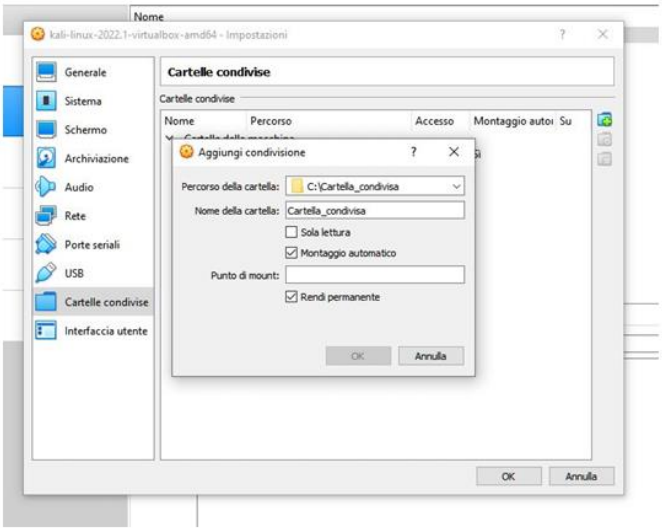
Progetto S9/L5 PDF

Traccia:

Per analizzare la cattura, spostate il file sulla vostra Kali Linux, e fate doppio-click, vi aprirà la cattura direttamente con Wireshark, dopo aver configurato i permessi per l'utente Kali.

Potete spostare il file sulla vostra Kali creando una cartella condivisa tra il vostro host e la Kali come la figura a destra.

Vi basterà creare la cartella sul vostro sistema operativo, e configurare la cartella sulla macchina virtuale, specificando il percorso della cartella sul vostro Host ed il nome della cartella.
Configurate la cartella con le opzioni in figura.



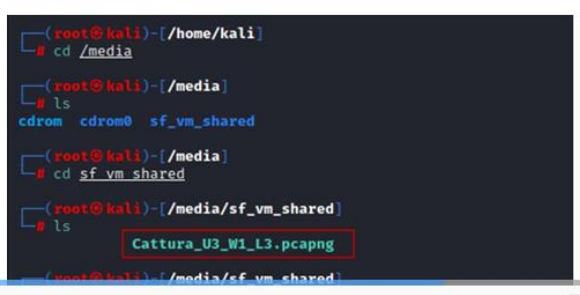
EPICODE

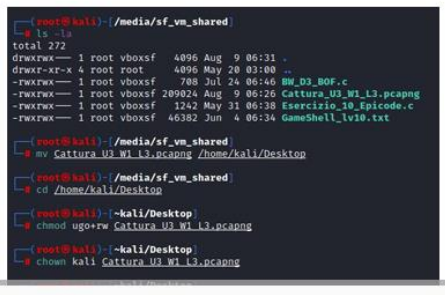
Progetto S9/L5 PDF

Esercizio
Threat Intelligence & IOC

Traccia:

Da Kali potete accedere alla cartella (ed ai file in essa contenuti) navigando il file system alla directory /media come da figura seguente. Come vedete il nostro file è nella cartella condivisa. Da qui possiamo spostare il file sul desktop con il comando «mv» specificando il nome del file ed il path di destinazione, come visto nelle lezioni sul file system di Linux (il comando che abbiamo usato noi è nella figura a destra).
Successivamente assicuratevi che l'utente Kali possa aprire il file assegnando i permessi necessari - riferimento figura in a destra. A questo punto fate doppio click per analizzare la cattura.

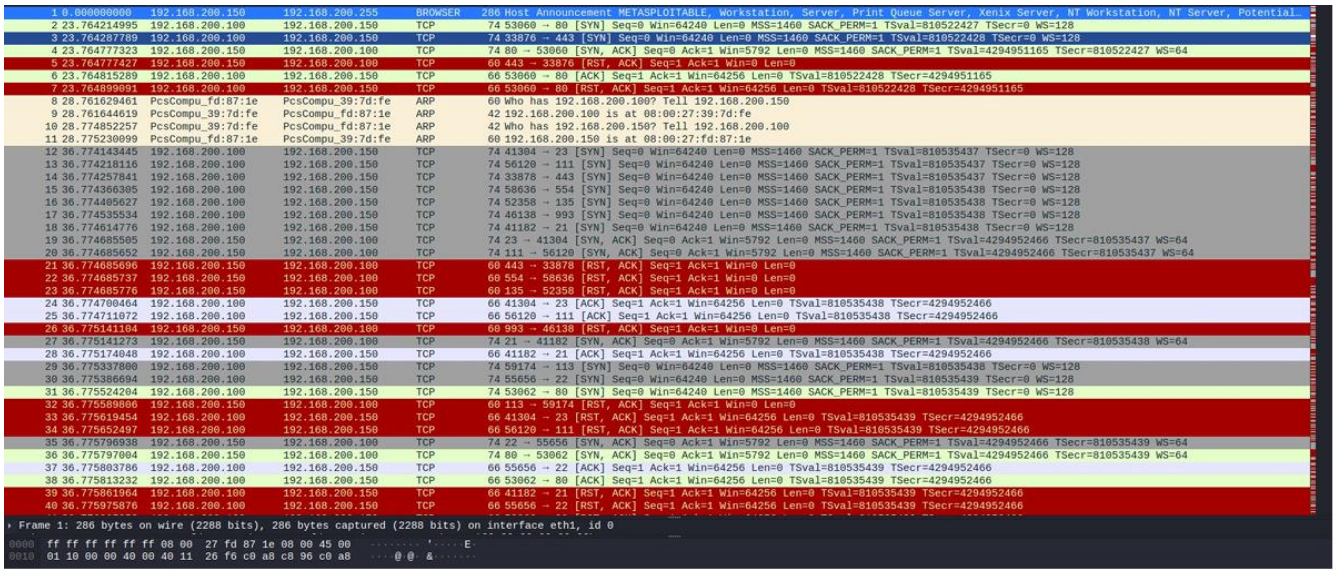




Report di Analisi del Traffico Wireshark

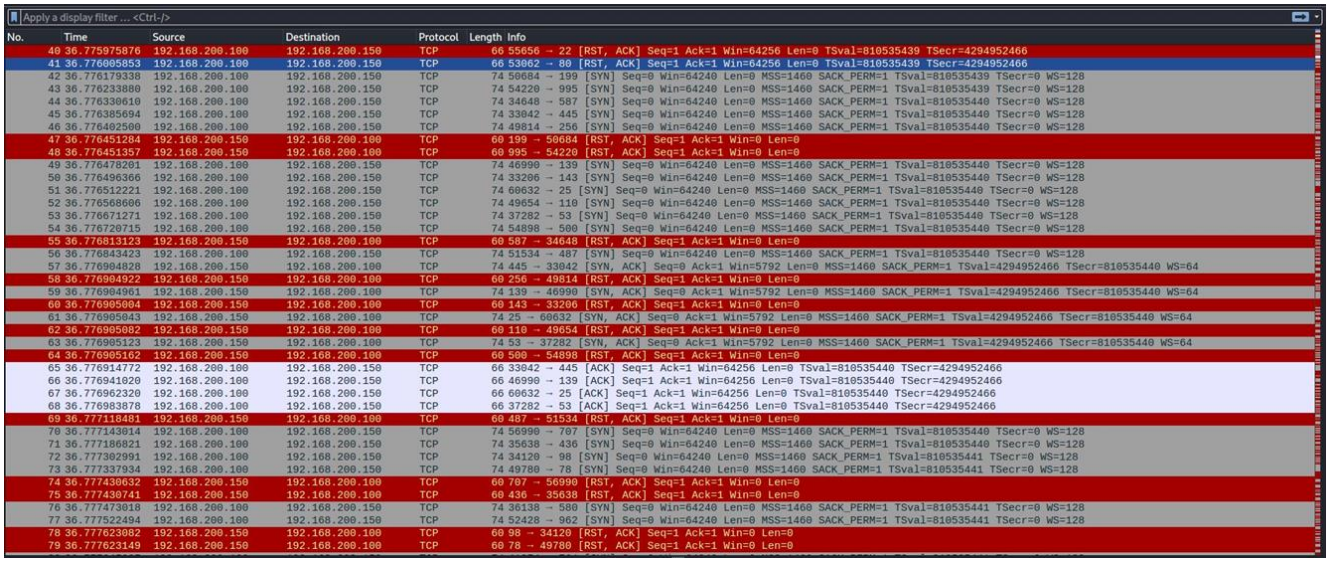
1. Contesto Generale

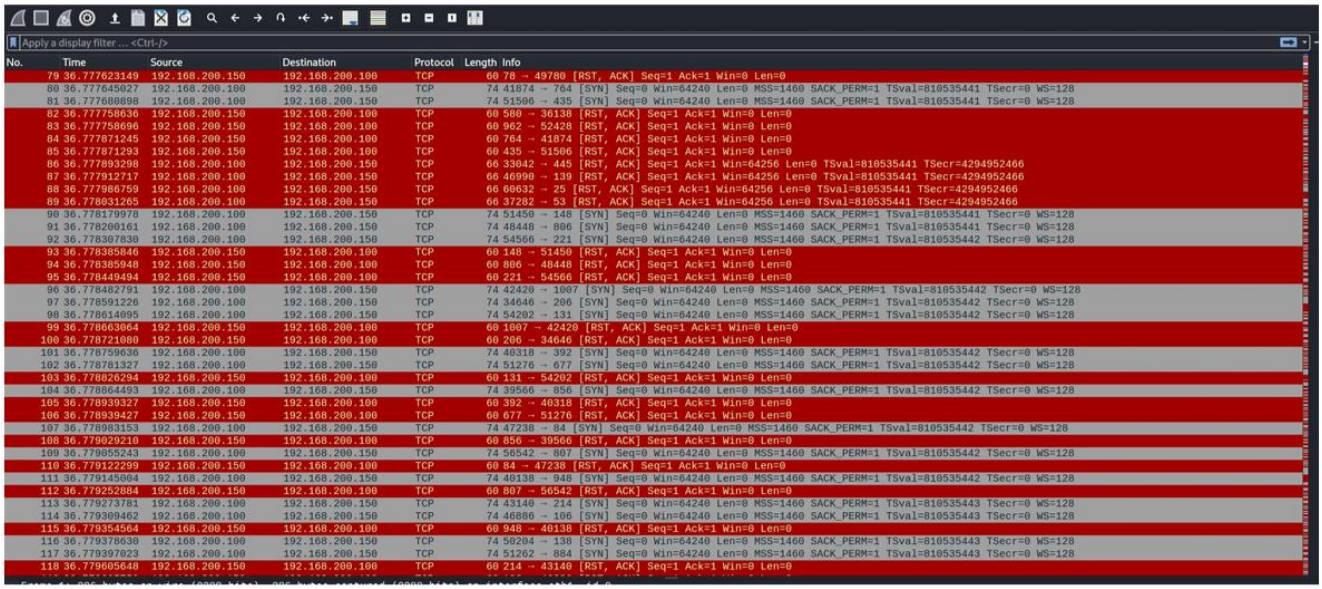
- **Tool di analisi**: Wireshark
- **Host coinvolti**:
    - 192.168.200.100 (potenziale attaccante)
    - 192.168.200.150 (potenziale bersaglio, probabilmente una macchina vulnerabile come Metasploitable)



2. Comportamenti Osservati

- Numerosi pacchetti TCP con flag SYN inviati da 192.168.200.100 a diverse porte TCP di 192.168.200.150.
- Risposte frequenti con flag RST, ACK da 192.168.200.150, indicando il rifiuto della connessione.
- Porte coinvolte: 80, 443, 41183, 49780, 50668, 34120, 1999, 55656, ecc.
- Trasmissione NetBIOS/BROWSER che identifica la macchina come "METASPLOITABLE", esponendo dettagli come: Workstation, NT Server, Print Queue Server, ecc.





No.	Time	Source	Destination	Protocol	Length	Info
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=1 TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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	435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	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	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535441 TSecr=0 WS=128
92	36.778367830	192.168.200.100	192.168.200.150	TCP	74	54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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=1 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=1 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=1 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=1 TSval=810535442 TSecr=0 WS=128
103	36.778826294	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=1 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=1 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=1 TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145004	192.168.200.100	192.168.200.150	TCP	74	40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
112	36.779252084	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=1 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=1 TSval=810535443 TSecr=0 WS=128
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378630	192.168.200.100	192.168.200.150	TCP	74	59204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 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

3. Indicatori di Compromissione (IOC)

Analisi Dettagliata

Durante l'analisi del traffico tra gli host 192.168.200.100 e 192.168.200.150, sono emersi diversi segnali che indicano attività potenzialmente malevole. Vediamo ciascun indicatore in modo piu' dettagliato.

TCP con flag RST, ACK multipli

Un numero elevato di pacchetti TCP di risposta contenenti i flag RST (Reset) e ACK (Acknowledgment) è stato osservato provenire dall'host 192.168.200.150. Questo comportamento è sintomatico del fatto che la macchina di destinazione sta **rifiutando attivamente le connessioni** in ingresso. In particolare, ciò avviene quando un host riceve una richiesta di connessione su una porta **non aperta** o **non in ascolto**, e decide quindi di chiudere subito il tentativo con un pacchetto di reset. Il ripetersi di questo pattern indica che un attaccante sta testando diverse porte nel tentativo di individuare servizi attivi, ma riceve sistematicamente rifiuti.

Port Scanning

Nel traffico analizzato, l'host 192.168.200.100 ha inviato richieste TCP (SYN) verso un'ampia gamma di porte sull'host 192.168.200.150 (tra cui le porte 80, 443, 1999, 41183, 50668, 34120 e molte altre). Questo comportamento è riconducibile a un **port scanning**, ovvero una tecnica utilizzata dagli attaccanti per **mappare i servizi attivi** su un sistema target. Lo scopo è identificare quali porte sono aperte e, quindi, quali applicazioni o servizi sono disponibili e potenzialmente vulnerabili a exploit successivi.

SYN Flood Passivo o Ricognizione Silenziosa

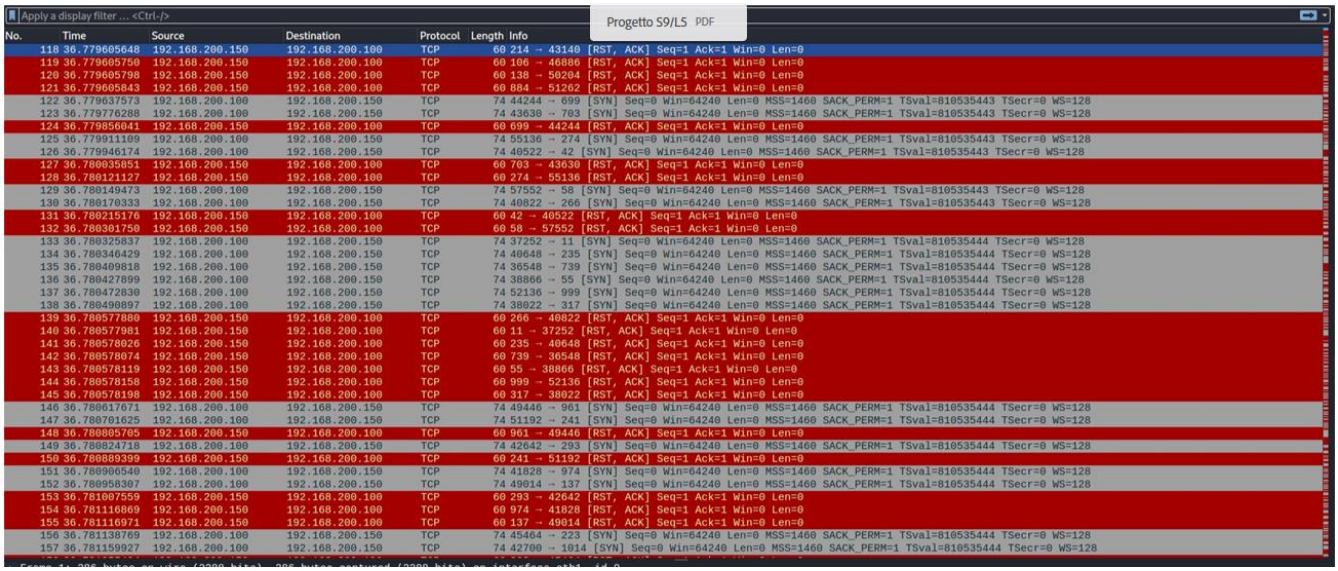
Molti dei pacchetti TCP inviati dall'host sospetto contengono solo il flag SYN e non sono seguiti da un completamento del classico **three-way-handshake** TCP. Questo comportamento può essere interpretato in due modi. Da un lato, potrebbe trattarsi di una semplice **ricognizione passiva** (stealth scan), in cui l'attaccante invia pacchetti SYN per rilevare risposte senza stabilire connessioni vere e

proprie. Dall'altro lato, se ripetuto su larga scala, può rappresentare l'inizio di un **attacco di tipo SYN Flood**, una forma di Denial of Service (DoS) mirata a esaurire le risorse del sistema target.

Annuncio NetBIOS con informazioni di sistema

Nel dump iniziale è presente un pacchetto di tipo **NetBIOS Name Service** (NBNS) broadcast in cui il sistema 192.168.200.150 annuncia sé stesso come "**METASPLOITABLE**" e include vari ruoli di sistema (ad esempio: Workstation, NT Server, Print Queue Server, ecc.). Queste informazioni, benché comuni nei broadcast interni di Windows e sistemi compatibili, sono **altamente sensibili** in ambienti di test o produzione, perché forniscono all'attaccante **dettagli preziosi sull'identità del sistema**, sulla sua funzione in rete e sui servizi che potrebbe ospitare. Un nome come "Metasploitable" è particolarmente critico, perché rivela apertamente che il sistema è vulnerabile per scopi di laboratorio o pentesting.

Questi elementi, se valutati nel loro insieme, disegnano un quadro coerente con una **fase iniziale di attacco informatico**, centrata sulla ricognizione e la raccolta di informazioni per pianificare exploit successivi. La rete dovrebbe essere attentamente monitorata, e i sistemi coinvolti analizzati con strumenti di sicurezza avanzati per prevenire compromissioni.



4. Ipotesi sugli Obiettivi dell'Attaccante

- **TCP Port Scanning**: L'attaccante cerca di determinare quali servizi sono attivi sulla macchina target.
- **Enumerazione dei Servizi**: Informazioni NetBIOS rivelano il nome host e servizi attivi, indicando che l'attaccante potrebbe usare exploit mirati.
- **Fase Preparatoria all'Intrusione**: Queste attività sono tipiche di una fase di ricognizione, prima di lanciare exploit su servizi vulnerabili.

5. Potenziali Vettori di Attacco

- **HTTP (porta 80)**: Potrebbe essere sfruttato per XSS, RFI, LFI, SQL Injection.
- **DoS SYN Flood**: Anche se non confermato in modo massivo, il pattern osservato potrebbe degenerare in un attacco DoS.

6. Raccomandazioni

- Monitorare l'host 192.168.200.100 per ulteriori comportamenti sospetti.
- Eseguire una scansione del sistema 192.168.200.150 per accertare l'integrità dei servizi esposti.
- Applicare policy di firewall per bloccare tentativi di connessione sospetti.
- Implementare un IDS/IPS per rilevare e mitigare attività di scansione.
- Disabilitare broadcast NetBIOS in ambienti non protetti.

Azioni specifiche:

- **Bloccare tutto il traffico in entrata non essenziale verso 192.168.200.150**, limitando l'accesso solo alle porte strettamente necessarie (es. 80/443 se è un web server).
- **Creare una regola di firewall per rifiutare connessioni da 192.168.200.100** se confermato come host sospetto.
- **Abilitare il logging dettagliato** su tentativi di connessione rifiutati o sospetti (specialmente SYN verso porte chiuse).
- **Isolare temporaneamente l'host target in una VLAN sicura o zona DMZ** per evitare ulteriori danni se compromesso.
- **Configurare limiti di connessioni (rate limiting)** e protezioni contro scansioni (come psad su Linux o sistemi UTM/firewall NG).

Prevenzione a lungo termine:

- **Attivare un IDS/IPS (come Snort o Suricata)** per rilevare pattern di scanning, SYN flood e tentativi di enumerazione.
- **Disabilitare protocolli inutili** e riduci le informazioni esposte (es. blocca NetBIOS/SMB in broadcast).
- **Eseguire patch e hardening del sistema target** (specialmente se si tratta di un ambiente come Metasploitable, che è vulnerabile di proposito).
- **Seguire il principio del minimo privilegio**: consenti solo il traffico necessario da host fidati

L'attività osservata è indicativa di una fase iniziale di un attacco informatico, in particolare la ricognizione. Un host nella rete (192.168.200.100) sta scandagliando un sistema potenzialmente vulnerabile (192.168.200.150) per identificare porte aperte e servizi.