Report di Analisi Forense del Traffico di Rete: Identificazione di Indicatori di Compromissione (IOC) e Valutazione della Minaccia

Data del Report: 30 Maggio 2025

Autore: Stefano Gugliotta

Riferimento Cattura di Rete: Cattura_U3_W1_L5.pcapng

---

1. Introduzione e Obiettivo dell'Analisi

Il presente documento costituisce un report di analisi forense del traffico di rete, basato sull'esame del file Cattura_U3_W1_L5.pcapng. L'obiettivo primario di questa analisi è l'identificazione di potenziali Indicatori di Compromissione (IOC) che possano suggerire attività malevole o sospette in corso all'interno dell'ambiente di rete monitorato. In aggiunta, il report mira a formulare ipotesi fondate sui vettori di attacco plausibilmente impiegati e a proporre un set di azioni immediate e strategiche per mitigare gli impatti di eventuali attacchi attuali e per rafforzare la postura di sicurezza complessiva, prevenendo incidenti futuri di natura simile.

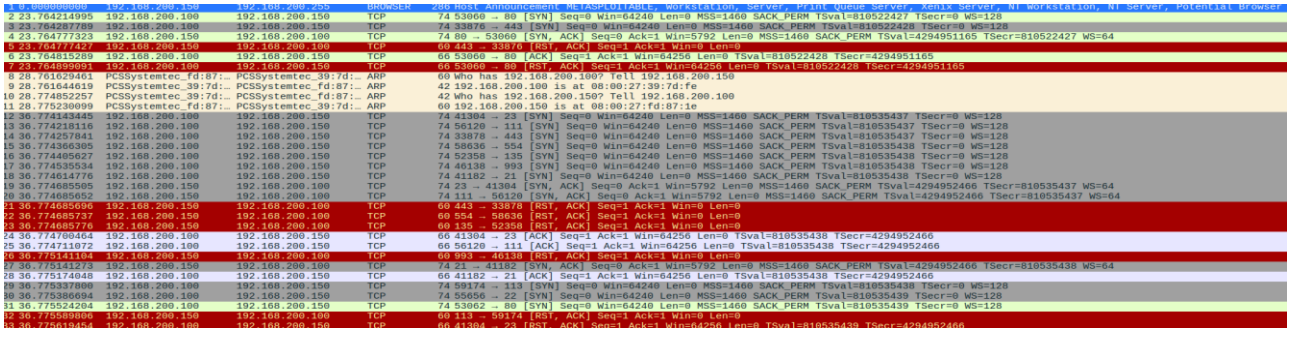
L'analisi è stata condotta metodicamente utilizzando Wireshark, uno strumento standard del settore per l'analisi dei pacchetti di rete, concentrandosi in particolare sul traffico registrato fino al frame (log) 262, come indicato dalla metodologia di esercizio.

2. Identificazione e Analisi degli Indicatori di Compromissione (IOC)

L'esame approfondito della cattura di rete ha immediatamente evidenziato un'attività di traffico TCP anomala e persistente tra due indirizzi IP appartenenti alla medesima sottorete interna 192.168.200.0/24. Questi due host sono stati identificati come:

- **Host Sorgente Sospetto:** 192.168.200.100
- **Host di Destinazione/Target:** 192.168.200.150

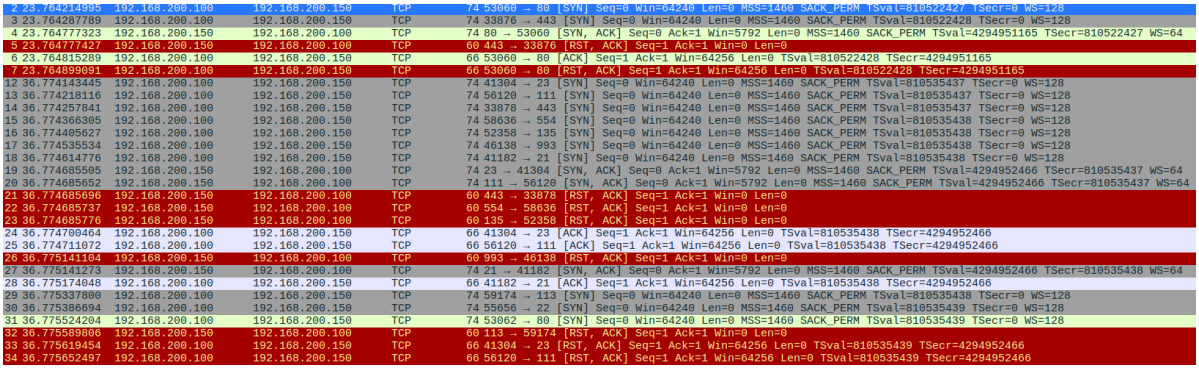
Gli indicatori di compromissione (IOC) più evidenti, relativi all'attività di scansione di rete, sono stati osservati **a partire dal frame 12** e si sono manifestati con persistenza e continuità fino e oltre il frame 262. Tali IOC sono i seguenti:



- **Schema Persistente di SYN e RST/ACK:** Il volume predominante del traffico tra gli host 192.168.200.100 e 192.168.200.150 è caratterizzato da una successione rapida e

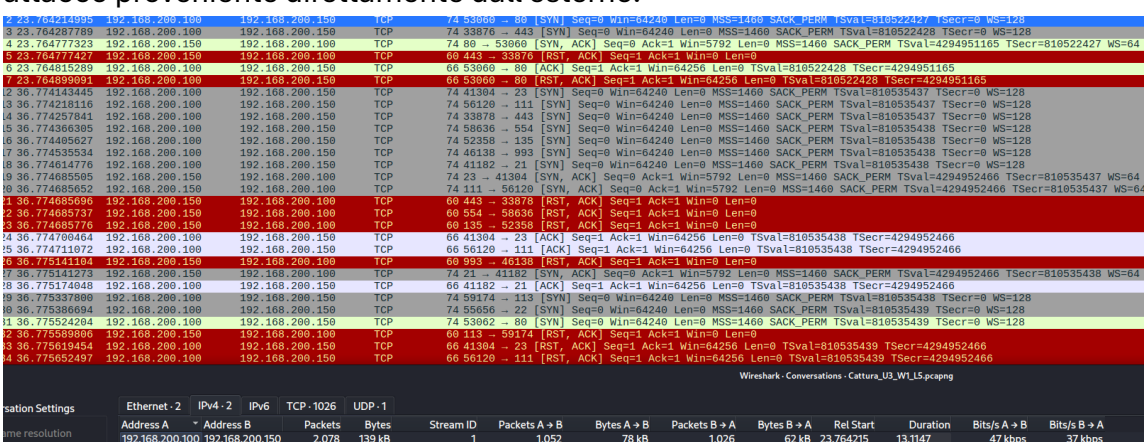
unidirezionale di pacchetti TCP con il flag SYN (richiesta di inizio connessione) da 192.168.200.100 verso 192.168.200.150. A ciascun SYN inviato, l'host di destinazione 192.168.200.150 risponde prontamente con un pacchetto RST, ACK (Reset, Acknowledgement). Questo schema, ripetuto per decine di tentativi, è un chiaro segnale di un'attività di sondaggio.

- **Tentativi di Connessione su un Ampio Spettro di Porte TCP:** L'host sorgente (192.168.200.100) dimostra un'intenzione di stabilire connessioni su un numero estremamente elevato e variegato di porte TCP sul target 192.168.200.150. Questo include sia porte ben note associate a servizi comuni (es. 445 per SMB/CIFS, 139 per NetBIOS Session Service) sia una moltitudine di porte non standard o appartenenti a range elevati (es. 55666, 55777). Tale approccio indiscriminato è tipico della scansione sistematica.

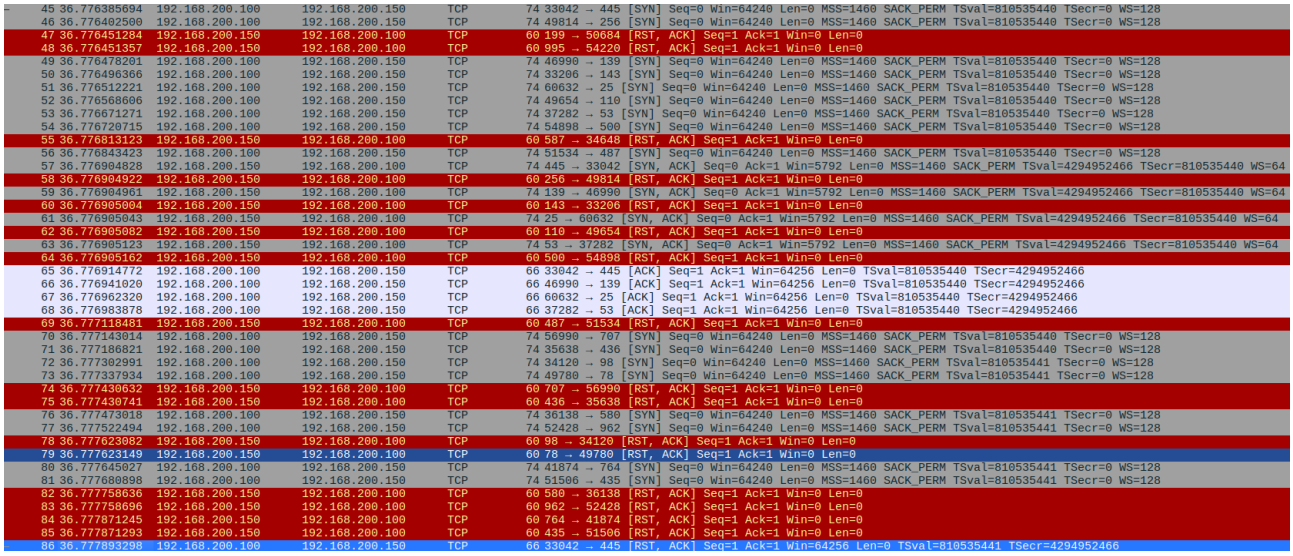


- **Assenza di Three-Way Handshake Completato:** È fondamentale notare l'assoluta assenza di un "three-way handshake" TCP completo (la sequenza SYN -> SYN/ACK -> ACK) in relazione a queste numerose richieste. La risposta RST, ACK da parte del target indica che le porte sono chiuse o che un firewall intermedio sta attivamente rifiutando o chiudendo immediatamente ogni tentativo di connessione non autorizzato, impedendo l'instaurazione di una sessione TCP.

- **Localizzazione dell'Attività Anomala:** L'attività sospetta è quasi esclusivamente concentrata tra i due indirizzi IP specificati, entrambi residenti nella medesima sottorete interna. Ciò suggerisce una possibile interazione ostile (o un sistema compromesso) all'interno del perimetro di rete dell'organizzazione, piuttosto che un attacco proveniente direttamente dall'esterno.



In sintesi, la combinazione di questi IOC dipinge un quadro chiaro di un'attività di ricognizione mirata e sistematica.



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	36.776451284	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	36.776729715	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 → 487 [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	36.777118481	192.168.200.150	192.168.200.100	TCP	60 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74 58990 → 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
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 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

3. Ipotesi sui Potenziali Vettori di Attacco Utilizzati

Sulla base degli indicatori di compromissione analizzati, l'ipotesi più robusta e fondata riguardo al potenziale vettore di attacco è la seguente:

- **Vettore Principale: Port Scanning (Scansione delle Porte):**
    - Il pattern di traffico osservato (SYN seguito da RST, ACK) è la firma inequivocabile di una **scansione delle porte TCP**, in particolare una "SYN scan" (anche nota come "half-open scan" o "stealth scan"). Questa tecnica permette all'aggressore di determinare lo stato di una porta (aperta, chiusa, filtrata) sul sistema target senza dover completare il three-way handshake TCP, rendendo l'attività potenzialmente meno rilevabile dai log di sistema standard che registrano solo le connessioni complete.
    - Questo processo è un passaggio fondamentale nella fase di **ricognizione** di un attacco cibernetico, conformemente ai modelli della "kill chain" del cyber-attacco. L'obiettivo dell'attaccante in questa fase è quello di creare una mappa dei servizi attivi e delle porte aperte sul target (192.168.200.150). Una volta che queste informazioni sono state raccolte, l'aggressore può passare alla fase successiva, cercando vulnerabilità note (CVE) nei servizi identificati o tentando attacchi di forza bruta contro i servizi autenticati (es. SSH, RDP, SMB).
    - Lo strumento più comunemente associato a questo tipo di scansione e che presenta il comportamento osservato è **Nmap** (Network Mapper), un potente scanner di rete ampiamente utilizzato sia da professionisti della sicurezza (per penetration test) che da attori malevoli. L'attività persistente fino al frame 262 suggerisce un tentativo metodico e prolungato di mappatura del target.

4. Raccomandazioni e Azioni Correttive

Per mitigare gli impatti dell'attacco di ricognizione in corso e per rafforzare la postura di sicurezza contro futuri tentativi simili, si raccomandano le seguenti azioni, suddivise per priorità temporale:

A. Azioni Immediate (Risposta all'Incidente / Contenimento):

1. **Identificazione e Isolamento del Sistema Sorgente (192.168.200.100):**
    - Priorità assoluta: Identificare la natura dell'host 192.168.200.100. Valutare se si tratti di un dispositivo legittimo compromesso (es. workstation infetta, server vulnerabile), un utente non autorizzato che esegue attività malevole, o un sistema mal configurato che genera traffico anomalo.
    - In caso di conferma di attività ostile o compromissione, isolare immediatamente l'host 192.168.200.100 dalla rete. Questo può essere realizzato bloccando la porta fisica dello switch a cui è collegato, applicando una regola di deny sul firewall o segmentando temporaneamente l'host in una VLAN di quarantena. L'obiettivo è interrompere immediatamente l'attività di scansione e prevenire qualsiasi escalation.
2. **Verifica dello Stato del Target (192.168.200.150):**
    - Eseguire un'analisi forense e una scansione di vulnerabilità approfondite su 192.168.200.150. Verificare i log di sistema per eventuali tentativi di accesso successivi alla scansione o indicatori di sfruttamento di vulnerabilità.
    - Controllare l'integrità dei file di sistema e la presenza di malware o rootkit.
3. **Allerta e Coordinamento del Team di Sicurezza:**
    - Comunicare tempestivamente questa attività sospetta al Security Operations Center (SOC) o al team IT/Sicurezza responsabile. Avviare la procedura standard di risposta agli incidenti, inclusa la documentazione dettagliata di tutte le azioni intraprese.

B. Azioni Preventive (Rafforzamento della Sicurezza a Lungo Termine):

1. **Segmentazione di Rete e Regole Firewall Granulari:**
    - Implementare una robusta **segmentazione di rete** (es. attraverso VLAN, sottoreti dedicate e firewall interni/ACL sugli switch L3) per limitare la comunicazione tra host e sottoreti ai soli flussi strettamente necessari (principio del minimo privilegio nella comunicazione). Se 192.168.200.100 e 192.168.200.150 non hanno una necessità operativa di comunicare su un'ampia gamma di porte, le regole del firewall dovrebbero bloccare esplicitamente tale traffico.

- Configurare i firewall per implementare regole di denial by default (negano tutto ciò che non è esplicitamente permesso) e per applicare funzionalità avanzate di **Rate Limiting** e **Flood Protection**. Queste funzionalità possono rilevare e mitigare automaticamente le scansioni di porta aggressive o altri tipi di traffico anomalo.

2. **Hardening dei Sistemi Operativi e delle Applicazioni:**
    - Su tutti i sistemi, inclusi i potenziali target come 192.168.200.150, applicare il principio del **minimo privilegio funzionale**: chiudere tutte le porte non essenziali e disabilitare i servizi di rete non strettamente necessari. Questo riduce drasticamente la superficie di attacco.
    - Mantenere tutti i sistemi operativi, le applicazioni e i software di rete costantemente **aggiornati** con le ultime patch di sicurezza. Questo corregge le vulnerabilità note (CVE) che potrebbero essere sfruttate una volta che una scansione ha identificato servizi aperti e vulnerabili.
3. **Implementazione e Ottimizzazione di Sistemi IDS/IPS:**
    - Assicurarsi che i sistemi di Intrusion Detection System (IDS) e Intrusion Prevention System (IPS) siano correttamente configurati e dotati di firme aggiornate. Questi sistemi dovrebbero essere in grado di rilevare e, idealmente, bloccare automaticamente le attività di scansione delle porte (come quelle generate da Nmap), generando allarmi ad alta priorità.
4. **Monitoraggio e Logging Avanzato con SIEM:**
    - Centralizzare i log di sicurezza (provenienti da firewall, IDS/IPS, server, router, switch e endpoint) in un sistema di **Security Information and Event Management (SIEM)**. Un SIEM consente un monitoraggio proattivo, la correlazione degli eventi attraverso diverse fonti di log e la rilevazione tempestiva di pattern anomali che potrebbero indicare scansioni di rete, tentativi di accesso non autorizzati o altre attività malevole.
5. **Audit di Sicurezza Regolari e Penetration Testing:**
    - Condurre regolarmente **scansioni di vulnerabilità** interne ed esterne, e **penetration test** (simulazioni di attacco). Questo approccio proattivo permette di identificare le debolezze della rete e dei sistemi prima che possano essere scoperte e sfruttate da attori malevoli.

Conclusioni Finali:

L'analisi forense del traffico di rete ha rivelato la presenza di una persistente e sistematica attività di scansione delle porte all'interno della sottorete 192.168.200.0/24, originata da 192.168.200.100 e mirata a 192.168.200.150. Questa attività costituisce una fase cruciale di ricognizione preliminare a un potenziale attacco informatico più sofisticato. È di

fondamentale importanza che l'organizzazione agisca con tempestività per contenere questa attività e implementare le raccomandazioni di sicurezza proposte, rafforzando in modo proattivo la propria postura di sicurezza per prevenire incidenti futuri e proteggere gli asset critici.