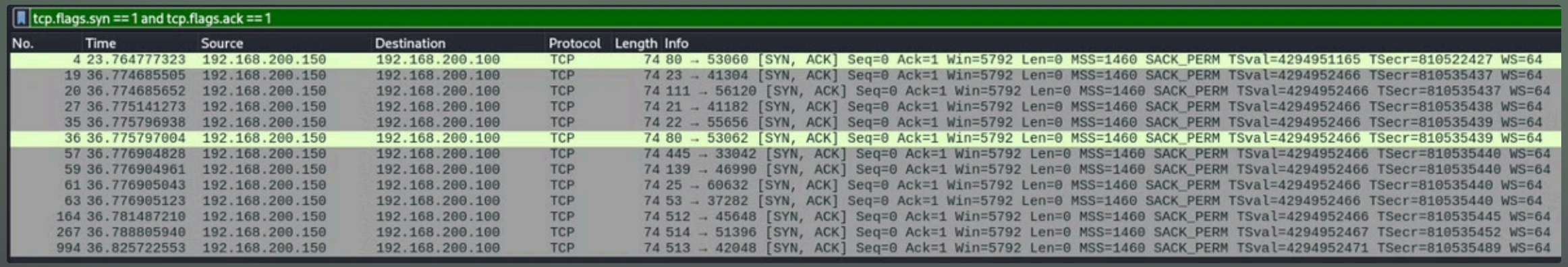
Threat Intelligence & IOC: Analisi di una Cattura di Rete

Nell'esercitazione di oggi analizzeremo una cattura di rete effettuata con Wireshark, concentrandoci sull'identificazione e analisi degli Indicatori di Compromissione (IOC) che evidenziano potenziali attacchi in corso.

Esamineremo attentamente i dati per formulare ipotesi sui vettori di attacco utilizzati e proporremo azioni concrete per mitigare l'impatto dell'attacco attuale e prevenire simili minacce in futuro.



tcp.flags.syn == 1 and tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length	Info
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	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=4294952466 TSecr=810535437 WS=64
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
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
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
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
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
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
267	36.788805940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64

Identificazione degli IOC: Scansione delle Porte

Pattern di Scansione

Numerosi pacchetti TCP con flag [SYN] inviati da 192.168.200.100 verso 192.168.200.150 su varie porte (80, 443, 23, 21, ecc.), seguiti da risposte [SYN, ACK] o [RST, ACK].

Comportamento Tipico

Questo comportamento è caratteristico di una scansione delle porte, dove un potenziale attaccante cerca di identificare servizi attivi sul sistema bersaglio.

IOC Rilevato

Elevato numero di tentativi [SYN] su porte diverse in un breve intervallo di tempo, indicativo di un'attività di reconnaissance.

Analisi delle Risposte del Sistema Target

Risposte [RST, ACK]

Molte porte rispondono con [RST, ACK], indicando che il servizio non è attivo o che la macchina target rifiuta la connessione.

L'alto volume di tali risposte conferma che il sistema è sotto scansione attiva, fornendo all'attaccante informazioni sulle porte chiuse.

Connessioni Riuscite

Alcune porte rispondono con [SYN, ACK] seguite da [ACK], completando il Three-Way Handshake. Queste connessioni riuscite (es. porta 80, 23, 22) indicano servizi attivi.

Questo rappresenta un IOC significativo, poiché l'attaccante potrebbe sfruttare questi servizi aperti per ulteriori attacchi.

```
 8 28.761629461  PCSSystemtec_fd:87:… PCSSystemtec_39:7d:… ARP      60 Who has 192.168.200.100? Tell 192.168.200.150
 9 28.761644619  PCSSystemtec_39:7d:… PCSSystemtec_fd:87:… ARP      42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257  PCSSystemtec_39:7d:… PCSSystemtec_fd:87:… ARP      42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099  PCSSystemtec_fd:87:… PCSSystemtec_39:7d:… ARP      60 192.168.200.150 is at 08:00:27:fd:87:1e
```

Traffico ARP e Mappatura della Rete

Risoluzione degli Indirizzi

I pacchetti ARP (8-11) mostrano una risoluzione degli indirizzi IP 192.168.200.100 e 192.168.200.150 con i rispettivi MAC address (08:00:27:39:7d:fe e 08:00:27:fd:87:1e).

Comportamento Normale ma Sospetto

Questo è un comportamento normale in una rete locale, ma in combinazione con la scansione delle porte, indica che l'attaccante sta mappando la rete per identificare dispositivi attivi.

Fase di Reconnaissance

La combinazione di traffico ARP e scansione delle porte suggerisce una fase di reconnaissance strutturata, dove l'attaccante sta costruendo una mappa completa della rete target.

Ipotesi sui Vettori di Attacco

Scansione delle Porte

192.168.200.100 sta inviando un elevato numero di pacchetti TCP con flag [SYN] verso 192.168.200.150, su numerose porte in poco tempo.

Mappatura dei Servizi

L'obiettivo è identificare quali porte sono aperte e ospitano servizi in ascolto, come confermato dalle risposte [SYN, ACK] ricevute su porte comuni.

Preparazione all'Attacco

Questa attività di reconnaissance è probabilmente il preludio a un attacco più mirato, dove l'aggressore sfrutterà le vulnerabilità dei servizi identificati.

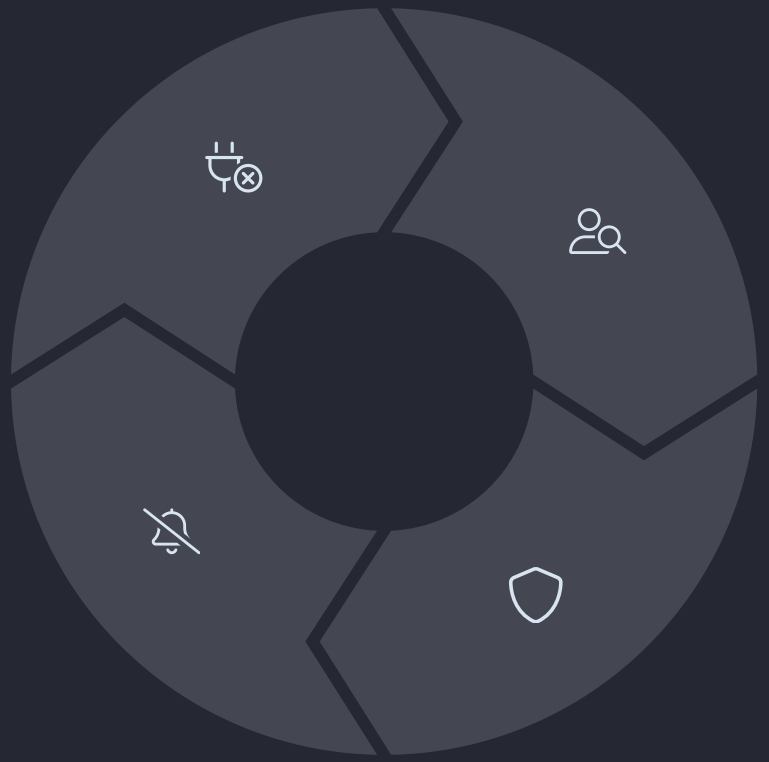
Azioni per Mitigare l'Attacco Attuale

Isolamento del Dispositivo

Scollegare 192.168.200.100 dalla rete per contenere l'attività malevola

Implementazione IDS

Installare un sistema di rilevamento delle intrusioni per monitorare il traffico



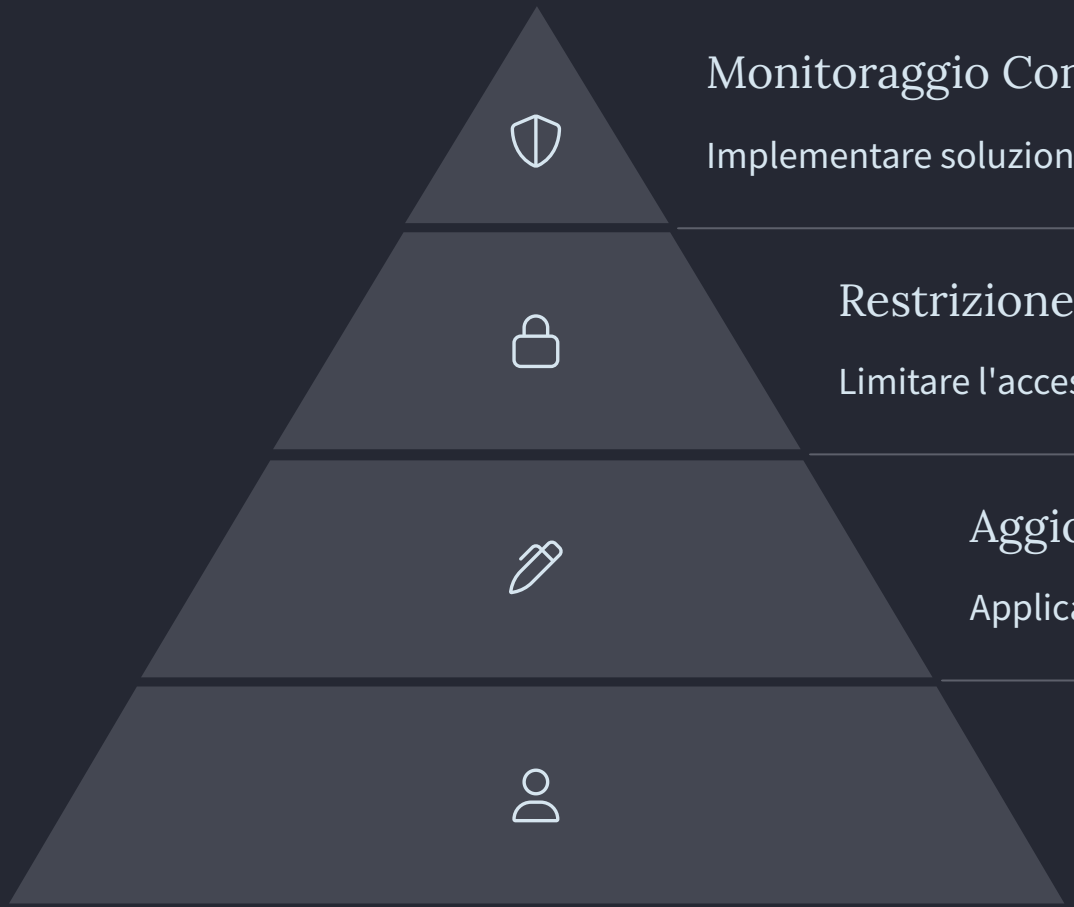
Verifica dei Log

Analizzare i log di 192.168.200.150 per identificare tentativi di accesso o anomalie

Modifica Firewall

Configurare il firewall per bloccare tentativi di scansione delle porte

Prevenzione di Attacchi Futuri



Monitoraggio Continuo

Implementare soluzioni di monitoraggio avanzate

Restrizione delle Porte

Limitare l'accesso solo alle porte necessarie

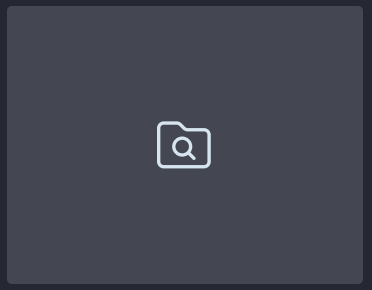
Aggiornamenti di Sicurezza

Applicare patch e mantenere i dispositivi aggiornati

Formazione del Personale

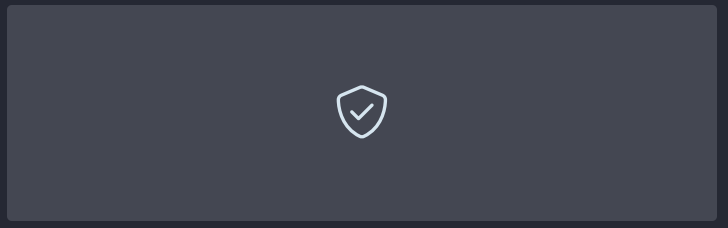
Educare gli utenti sulle minacce e le best practice

Conclusioni



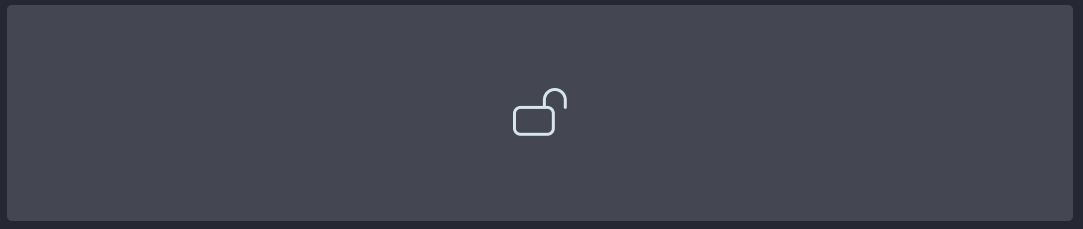
Reconnaissance Identificata

La cattura di rete evidenzia un sistema (192.168.200.150, "METASPLOITABLE") sottoposto a una scansione delle porte



Azioni Immediate

Modificare le regole firewall e isolare il dispositivo sospetto



Misure Preventive

Implementare restrizione delle porte e monitoraggio continuo

L'analisi condotta ha permesso di identificare chiaramente un'attività di reconnaissance attraverso la scansione delle porte. Le azioni immediate e le misure preventive proposte sono fondamentali per mitigare l'attuale minaccia e proteggere la rete da future attività simili, garantendo un ambiente più sicuro e resiliente.