ESERCIZIO S9 L5



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

SVOLGIMENTO

Introduzione

Questo report analizza in dettaglio una cattura di rete, con l'obiettivo di identificare indicatori di compromissione (IOC), ipotizzare i **vettori di attacco** e suggerire azioni di **mitigazione**.

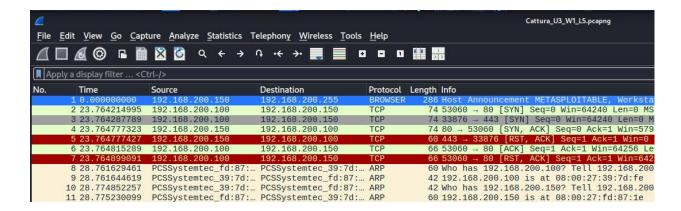
Si rileva facilmente il fatto che sono presenti solo **due dispositivi** coinvolti dove il dispositivo con **IP 192.168.200.100** invia pacchetti per lo più **SYN** ricevuti dalla macchina vittima con **IP 192.168.200.150**.

Scenario:

Indirizzo IP dell'attaccante: 192.168.200.100

Indirizzo IP del bersaglio: **192.168.200.150** (con un sistema identificato come METASPLOITABLE).

Sezioni analizzate:



Analizzo l'apertura della cattura : L'attaccante avvia una scansione SYN. I pacchetti 2-3 inviano richieste [SYN] al bersaglio. I pacchetti da 4 a 7 mostrano le risposte di una scansione "half-open" con [SYN, ACK] del bersaglio e un [RST, ACK] dell'attaccante e del bersaglio.

La porta **80** risulta aperta in quanto il bersaglio risponde col SYN ACK (pacchetto 4) e l'attaccante conferma la comunicazione con l'ACK (pacchetto 6)

RST = è un segnale del protocollo TCP che chiude le comunicazioni quando qualcosa non va. *Per esempio: pacchetto arrivato su una porta dove non c'è nessun servizio.* Interrompe quindi le comunicazioni e può essere utilizzato per condurre un attacco RST Flood.

Un **RST flood** è un attacco in cui un aggressore invia **tantissimi** pacchetti TCP con il flag RST verso una vittima o verso endpoint di comunicazione. L'effetto può essere:

Interrompere connessioni legittime (client-server) facendo chiudere sessioni importanti.

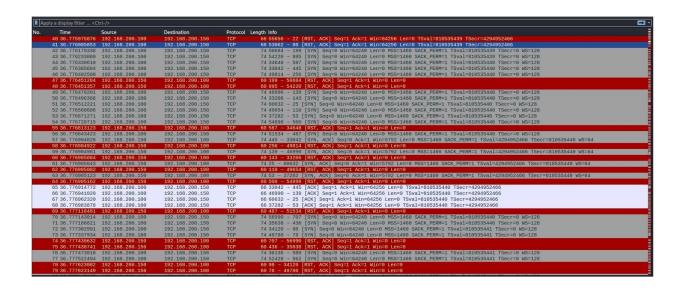
Creare instabilità nelle applicazioni (drop di sessioni, riconnessioni continue).

Sovraccaricare le risorse di rete o dei dispositivi che devono processare e registrare tutti quei pacchetti.

Spesso l'attaccante **spoofa** (falsifica) gli indirizzi sorgente, così è difficile risalire alla fonte e le risposte finiscono altrove.

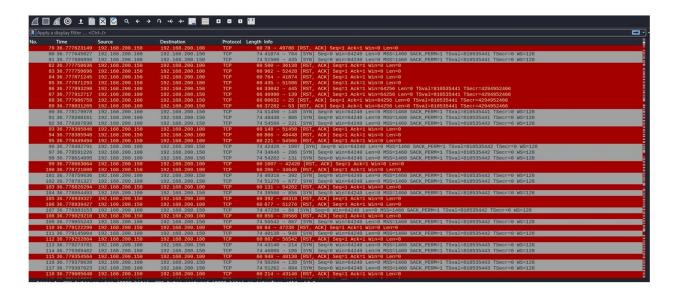
Un'analisi più approfondita mostra anche **pacchetti ARP (Address Resolution Protocol)**. L'attaccante sta usando i pacchetti ARP per scoprire l'indirizzo MAC (livello 2) del bersaglio partendo dal suo indirizzo IP (livello 3).

Questo è un passo fondamentale prima di avviare la scansione TCP, in quanto l'attaccante ha bisogno dell'indirizzo MAC per inviare i pacchetti a livello fisico.



La scansione continua con lo stesso metodo **SYN Scan**. L'attaccante continua a testare un'ampia gamma di porte, confermato dal susseguirsi di richieste **[SYN]** e risposte **[RST]** per le porte chiuse.

Le righe **65-68** mostrano un **ACK Scan**, dove l'attaccante sta testando i filtri del firewall inviando pacchetti **[ACK]** a porte comuni come **445(SMB)** e **139 (NetBios)**.

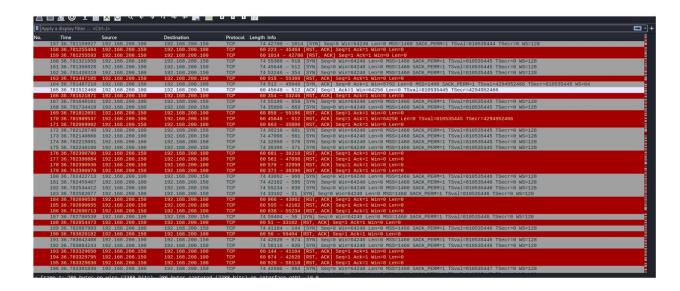


La scansione prosegue con un ritmo elevato. L'attaccante sta eseguendo una scansione estesa e automatizzata su un ampio range di porte.

Le righe dominanti, colorate di rosso, indicano che la maggior parte delle porte testate sono chiuse (RST,ACK e nessuna risposta al SYN che segnala la presenza di un blocco o filtro). Questo permette all'attaccante di **delimitare** rapidamente i potenziali obiettivi, **escludendo le porte non attive.**



La scansione SYN continua. L'attaccante sta procedendo in modo sistematico, testando un vasto intervallo di porte. Le risposte [RST, ACK] come nella riga 119 indicano che le porte sono chiuse. L'attaccante sta metodicamente mappando la rete del bersaglio per completare la sua fase di ricognizione.



Questa cattura rivela che l'attaccante ha identificato un obiettivo specifico e sta testando una porta non comune.

Il punto chiave è il **pacchetto 165**. L'attaccante ha inviato un pacchetto **[SYN]** alla porta di destinazione **512**. La risposta del bersaglio, un pacchetto **[SYN, ACK]**, conferma che la porta **512** è aperta e in ascolto.

La porta **TCP 512** è assegnata al servizio chiamato **exec** (noto anche come **rexec**, Remote Execution). È un vecchio servizio Unix che permetteva a un utente di far eseguire comandi su una macchina remota: il client si connette e invia credenziali + comando, il server **(rexecd)** esegue il comando e rimanda indietro l'output.

Come funziona

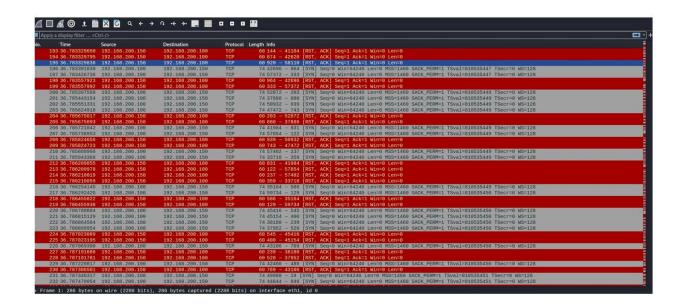
Il client apre una connessione TCP verso la porta 512 del server.

Invia al server nome utente e password (testo in chiaro) e il comando da eseguire.

Se l'autenticazione va a buon fine, il server avvia il comando e inoltra standard input/output/error sulla connessione.

Il fatto che venga scansionata una porta così specifica e obsoleta suggerisce che l'attaccante stia cercando **vulnerabilità** in sistemi **non aggiornati** o configurati in modo non sicuro.

Indicando che la porta è aperta, viene offerto un potenziale punto di ingresso per l'esecuzione di comandi da remoto che probabilmente l'attaccante potrà sfruttare.



L'attaccante sta completando la sua scansione. La grande quantità di pacchetti e la ripetizione del comportamento dimostrano che si tratta di un'azione sistematica e automatizzata. La scansione ha fornito all'attaccante una mappa completa delle porte aperte e chiuse del bersaglio, che ora userà per pianificare il suo prossimo passo, che sarà probabilmente l'attacco effettivo.

Utilizzo filtri Wireshark:

Scelgo di utilizzare il filtro di Wireshark per visualizzare i SYN/ACK quindi le risposte che indicano che la porta interessata è aperta:

tcp.flags.syn == 1 && tcp.flags.ack == 1

lo.	Time	Source	Destination	Protocol	ol 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=81053543 Informati
	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=6
	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=6-
	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=66
	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
1	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=6-
	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=6

Porte aperte: 20, 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514.

Servizi e Valutazione del Rischio

Porta 20/21 - FTP (File Transfer Protocol)

Descrizione: Utilizzato per il trasferimento di file. Spesso configurato in modo insicuro.

Rischio: Se l'autenticazione è debole (ad esempio, l'uso di credenziali predefinite o anonime), un attaccante potrebbe caricare o scaricare file, inclusi potenziali **malware** o **backdoor**. Le versioni obsolete del server FTP possono avere vulnerabilità note.

• Porta 22 - SSH (Secure Shell)

Descrizione: Un protocollo crittografato per l'accesso remoto. È considerato sicuro.

Rischio: Nonostante sia sicuro, un attaccante può tentare un attacco brute-force se la password è debole o se l'autenticazione basata su chiavi non è implementata correttamente.

• Porta 23 - Telnet

Descrizione: Un protocollo obsoleto per l'accesso remoto.

Rischio: Estremamente alto. Telnet trasmette tutte le informazioni, inclusi nome utente e password, in chiaro. Un attaccante che intercetta il traffico può rubare le credenziali.

Porta 25 - SMTP (Simple Mail Transfer Protocol)

Descrizione: Utilizzato per l'invio di email.

Rischio: Se non è configurato correttamente, può essere sfruttato per inviare email di spam o phishing.

• Porta 53 - DNS (Domain Name System)

Descrizione: Traduce nomi di dominio in indirizzi IP.

Rischio: Se il server DNS è mal configurato, può essere vulnerabile a attacchi di cache poisoning, che reindirizzano gli utenti a siti malevoli, o può essere utilizzato per attacchi DDoS.

• Porta 80 - HTTP (Hypertext Transfer Protocol)

Descrizione: Il protocollo base per la navigazione web.

Rischio: Le vulnerabilità qui dipendono dal server web (es. Apache) e dalle applicazioni (es. CMS come WordPress). Un attaccante può cercare vulnerabilità note (come **SQL injection** o **Cross-Site Scripting**) o tentare di sfruttare versioni obsolete del software.

• Porta 111 - RPC (Remote Procedure Call)

Descrizione: Permette a un programma di eseguire codice su un sistema remoto.

Rischio: Un servizio che necessita di una stretta gestione della sicurezza. Se mal configurato, può essere sfruttato ottenere il controllo del sistema.

Porte 139 (NetBIOS) e 445 (SMB/CIFS)

Descrizione: Protocolli per la condivisione di file e stampanti in ambienti Windows.

Rischio: Elevato. Queste porte sono state storicamente l'obiettivo di attacchi critici come quello del worm **WannaCry**. Se il sistema non è patchato, un attaccante può facilmente ottenere il controllo.

Porte 512 (Exec), 513 (Rlogin), 514 (Rshell)

Descrizione: Servizi obsoleti per l'esecuzione di comandi remoti.

Rischio: Estremamente alto. Simili a Telnet, questi servizi trasmettono **dati in chiaro** e non prevedono **meccanismi di autenticazione robusti**. L'attaccante può tentare l'esecuzione di comandi da remoto, ottenendo il controllo totale del sistema. La presenza di questi servizi su un sistema esposto indica una grave lacuna di sicurezza.

Ipotesi sui Potenziali Vettori di Attacco Utilizzati

L'attaccante sta eseguendo un'attività di ricognizione per aggirare le difese e preparare la fase di exploitation.

Vettore di Attacco 1: SYN Scan L'attaccante invia pacchetti **[SYN]** al bersaglio. Quando una porta è aperta, il bersaglio risponde con un **[SYN, ACK]**, e l'attaccante risponde subito con un **[RST]**. Questo comportamento gli permette di identificare le porte aperte senza apparire nei log di connessione del bersaglio, rendendo la scansione difficile da rilevare. L'attaccante sta cercando servizi specifici, per trovare potenziali punti di ingresso per l'esecuzione di codice da remoto.

Vettore di Attacco 2: ACK Scan L'attaccante invia pacchetti con il solo flag **[ACK]** a porte note (come la **445** per **SMB** e la **139** per **NetBIOS**). Questo non ha lo scopo di scoprire se le porte sono aperte, ma di capire se sono filtrate da un firewall.

Se riceve un [RST], la porta è considerata "non filtrata" (il firewall non la blocca, anche se il servizio è inattivo).

Se non riceve alcuna risposta, la porta è "filtrata" (il firewall la sta bloccando attivamente).

Attacco DoS - RST Flood : La presenza di 47 richieste SYN dalla riga 1196 a 1243 mi ha fatto pensare ad un piccolo test di DoS, quasi come per verificare la reazione e capire se quel tipo di attacco possa funzionare in futuro. Rimane comunque veramente poco probabile non essendo presente lo spoofing dell'IP e date le poche richieste inviate.

Indicatori di compromissione (IOC)

IP Malevolo: 192.168.200.100

IP Vittima: 192.168.200.150

Tecnica Usata: Invio pacchetti TCP

L'attaccante ha tentato di sfruttare il three way handshake TCP + invio di pacchetti RST di chiusura immediata + SYN ACK + ACK

Azioni Consigliate per la Mitigazione

Azione Immediata: Bloccare l'indirizzo IP dell'attaccante (192.168.200.100) a livello del firewall.

Mitigazione a Lungo Termine:

Implementare un IDS/IPS: Un sistema di rilevamento e prevenzione delle intrusioni (IDS/IPS) è in grado di rilevare e bloccare automaticamente sia gli SYN Scan che gli ACK Scan.

Disabilitare tutti i servizi non necessari, specialmente quelli obsoleti e insicuri come exec (porta 512). Questo riduce drasticamente la superficie di attacco.

Mantenere tutti i sistemi e le applicazioni aggiornati per correggere le vulnerabilità note.

Rivedere e rafforzare le regole del firewall, in particolare per le porte esposte verso l'esterno, assicurandosi che il traffico non necessario sia filtrato.

CONCLUSIONE

Per concludere, l'analisi del traffico di rete ha rivelato un'attività di ricognizione da parte dell'attaccante.

L'attaccante ha utilizzato una combinazione di due diverse tecniche di scansione: una **SYN Scan** per identificare le porte aperte e un **ACK Scan** per mappare le regole del firewall.

L'attaccante sta cercando attivamente di aggirare le difese del bersaglio. La scoperta di servizi obsoleti e insicuri come **exec** (**porta 512**) indica l'obiettivo di sfruttare vulnerabilità note per ottenere l'accesso remoto al sistema.

Le azioni di mitigazione, come il blocco immediato dell'IP dell'attaccante, l'installazione di un IDS/IPS e l'**hardening del sistema**, sono fondamentali per prevenire che questa fase di ricognizione si trasformi in un attacco riuscito.