Relazione di Analisi Forense di Rete: Indagine su Sospetta Compromissione

1. Introduzione

In seguito alla lezione teorica sulla **Threat Intelligence**, mi è stato assegnato il compito di analizzare una cattura di traffico di rete (Cattura_U3_W1_L3.pcapng) per identificare potenziali Indicatori di Compromissione (IOC). L'obiettivo di questa analisi è rilevare evidenze di attacchi in corso, ipotizzare i vettori di attacco utilizzati e formulare raccomandazioni per la mitigazione. Il contesto suggerisce che potrei trovare traffico anomalo indicativo di malware, esfiltrazione dati o scansioni di rete.

2. Strumenti Utilizzati

- **Wireshark:** Analizzatore di protocollo di rete per l'ispezione profonda dei pacchetti.
- **VirtualBox (Ambiente Virtualizzato):** Per eseguire l'analisi in sicurezza, isolando eventuali file o script malevoli estratti.

3. Analisi Tecnica e Identificazione degli IOC

Per iniziare l'indagine devo avere una visione d'insieme del traffico. Non cerco un ago nel pagliaio alla cieca; uso la statistica per orientarmi.

Panoramica delle conversazioni e Protocolli

La prima cosa che faccio è guardare la gerarchia dei protocolli per capire "chi parla con chi" e "in che lingua".

- **Azione su Wireshark:** Vado su Statistics -> Protocol Hierarchy.
- **Cosa cerco:** Una quantità sproporzionata di traffico su protocolli inusuali o molto traffico HTTP/HTTPS/DNS verso destinazioni sconosciute.

Ecco cosa mi salta all'occhio guardando l'immagine e come lo interpreterei:

1. **Dominio assoluto del TCP:** la riga "Transmission Control Protocol" (TCP) occupa il 99.8% dei pacchetti (2078 su 2083).
2. **Assenza di "Application Layer":** Questa è la parte più sospetta (l'IOC potenziale). Sotto la voce TCP, non vedo ramificazioni verso protocolli come HTTP, TLS, SSH o FTP. La colonna "End Packets" segna 2078.
    a. **Cosa significa:** Wireshark ci sta dicendo: "Vedo tantissimi pacchetti di trasporto (TCP), ma non vedo dati applicativi riconoscibili al loro interno".
3. **Rumore di fondo:** C'è un singolo pacchetto UDP (NetBIOS). Questo è normale "rumore" di Windows, possiamo ignorarlo. Non è lì l'attacco.

La mia ipotesi basata solo su questo screen è se abbiamo quasi solo traffico TCP senza dati veri e propri (senza HTTP, ecc.), è molto probabile che stiamo osservando una **Scansione delle Porte (Port Scanning)** o un attacco **DoS (Denial of Service)** di tipo SYN Flood. Qualcuno sta probabilmente bussando a tutte le porte della vittima per vedere cosa è aperto, senza instaurare una vera connessione completa.

Conferma dell'Ipotesi

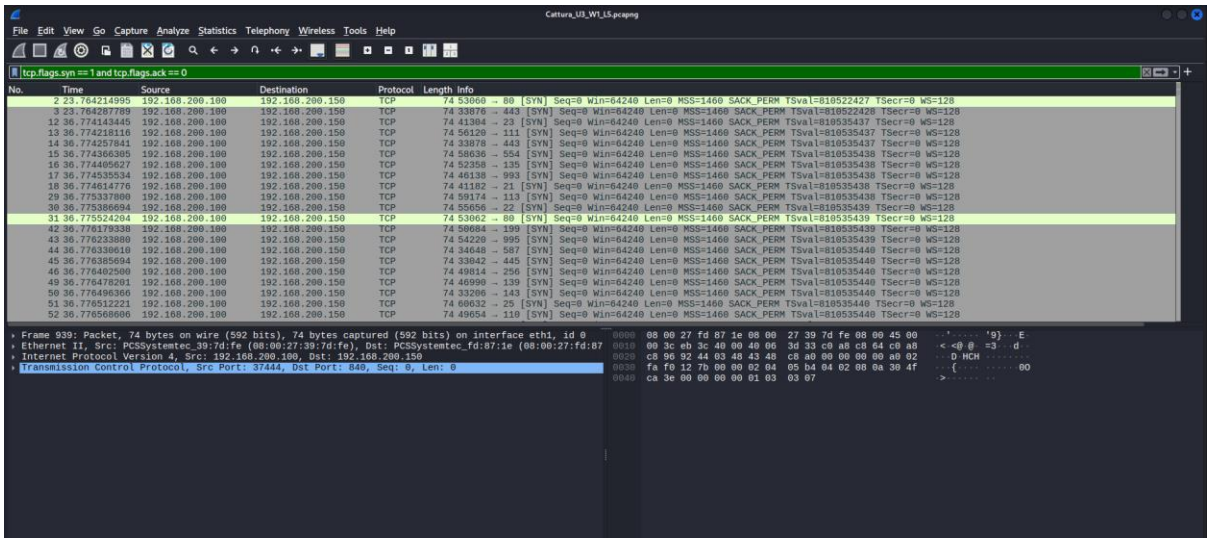
Ora devo confermare se si tratta davvero di una scansione. Se ho ragione, vedremo tantissimi pacchetti con la bandierina (Flag) "SYN" attivata.

Ecco cosa devo fare ora nella macchina virtuale:

1. Chiudo la finestra delle statistiche.
2. Nella barra dei filtri in alto scrivo questo codice per filtrare solo i pacchetti di richiesta connessione: tcp.flags.syn == 1 and tcp.flags.ack == 0

Cosa devo guardare:

- Guarda la colonna **Destination**. L'indirizzo IP di destinazione è sempre lo stesso (la vittima)?
- Guardo la colonna **Info** o **Port**. Le porte cambiano in sequenza (es. 80, 81, 82...) o sono tutte fisse su una porta?
- Guardo la colonna **Source**. Chi è che sta mandando tutti questi pacchetti? Quello è il nostro attaccante.



Analisi Tecnica

1. **Dalla "Protocol Hierarchy":**

- Confermo che il 99.8% del traffico è solo TCP puro. Non c'è traffico HTTP, FTP o Mail visibile come "dati". Questo esclude attacchi web

complessi (come SQL Injection) e conferma un attacco a livello di rete/trasporto.

2. **Dalla Cattura Filtrata:**

- **IP Attaccante (Source):** 192.168.200.100
- **IP Vittima (Destination):** 192.168.200.150
- **Il Comportamento:** la colonna "Info" con le porte di destinazione:
- Vedo pacchetti verso la porta **80** (Web)
- Verso la porta **443** (HTTPS)
- Verso la porta **23** (Telnet - molto vecchia e insicura!)
- Verso la porta **111**, **25** (SMTP), **993** (IMAP).

Conclusione: L'indirizzo .100 sta "bussando" freneticamente a tutte le porte possibili dell'indirizzo .150 per vedere quali sono aperte. Questa è una **Scansione delle Porte (Port Scanning/Reconnaissance)**.

4. Ipotesi sui Vettori di Attacco

Basandomi sugli IOC rilevati, ipotizzo che:

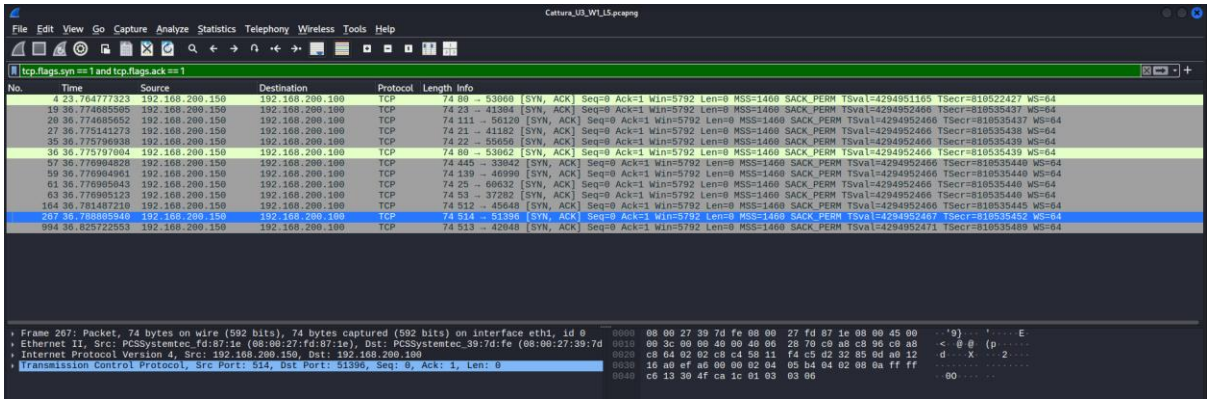
1. L'attaccante si trovi all'interno della stessa sottorete locale (IP privato 192.168.200.x) o abbia compromesso una macchina adiacente.
2. Il vettore utilizzato è un **TCP SYN Scan**. L'attaccante invia pacchetti SYN, se la porta è aperta la vittima risponde con SYN-ACK. Questo permette all'attaccante di mappare la superficie di attacco del server bersaglio per preparare un attacco mirato successivo.

Prossimo Passo: Vedo se l'attacco ha avuto successo

Ho visto che l'attaccante ha bussato. Ora devo vedere se la vittima ha risposto (cioè se ha porte aperte che possono essere sfruttate).

Su Wireshark:

1. Scrivo questo nuovo filtro: tcp.flags.syn == 1 and tcp.flags.ack == 1
2. Questo filtro mostra le risposte "Sì, sono aperta" della vittima.



Analizzando il risultato fornito da (tcp.flags.syn == 1 and tcp.flags.ack == 1), vedo chiaramente che la macchina vittima (192.168.200.150) sta rispondendo attivamente all'attaccante.

Cosa ho scoperto: La vittima ha risposto con pacchetti [SYN, ACK]. In TCP questo significa: "Sì, la porta è aperta, prego entra". Guardando la colonna **"Src Port"** vedo che sono aperte delle porte **estremamente pericolose**:

- **Porta 23 (Telnet):** Protocollo obsoleto che trasmette tutto in chiaro. È un invito a nozze per rubare password.
- **Porta 21 (FTP):** Anche questo spesso insicuro.
- **Porta 445 (SMB):** Spesso vulnerabile a exploit critici (come EternalBlue).
- **Porte 512, 513, 514 (exec/login/shell):** Vecchi servizi Unix noti per essere insicuri (r-services).

5. Ipotesi sui Vettori di Attacco

Sulla base degli IOC raccolti, ricostruisco il seguente scenario: L'attaccante (192.168.200.100) sta eseguendo una fase di **Information Gathering** attiva. Non è ancora nella fase di intrusione vera e propria (Exploitation), ma l'attaccante ha ora tutte le informazioni necessarie per lanciare un attacco mirato. Il vettore di attacco futuro più probabile sarà un **Brute Force** sulle porte Telnet (23) o FTP (21) per ottenere credenziali valide, oppure l'uso di un **Exploit** specifico per il servizio SMB (445) per ottenere l'esecuzione di codice remoto (RCE).

6.Conclusioni e Raccomandazioni

L'analisi ha evidenziato una grave carenza di hardening sul server vittima. Per ridurre gli impatti dell'attacco attuale e prevenirne di futuri raccomando le seguenti azioni immediate:

1. **Chiusura Servizi Obsoleti:** Disabilitare immediatamente il servizio **Telnet (Porta 23)** e i servizi "R" (512-514), sostituirli obbligatoriamente con SSH (Porta 22).
2. **Firewalling:** Configurare il firewall perimetrale o dell'host per bloccare tutto il traffico proveniente dall'IP 192.168.200.100.
3. **Network Segmentation:** Verificare perché l'IP .100 ha accesso diretto a tutte queste porte di gestione. Isolare il server in una VLAN dedicata.
4. **Patch Management:** Verificare la versione del servizio SMB sulla porta 445 e applicare le patch di sicurezza dato che è un vettore frequente per malware.