Report S9-L5 - Considerazione di un attacco

A cura di Canole Iris

Obiettivo

Il presente report ha lo scopo di analizzare un file di cattura di rete (`.pcapng`) fornito, al fine di simulare un'attività di **Threat Intelligence** e rilevamento delle minacce.

Nello specifico, gli obiettivi principali dell'analisi sono:

1. **Analisi del Traffico di Rete:** Esaminare i pacchetti catturati tramite Wireshark per individuare pattern di traffico anomalo o sospetto.
2. **Identificazione degli IOC:** Rilevare e isolare eventuali Indicatori di Compromissione (IOC - *Indicators of Compromise*) che confermino un attacco in corso o avvenuto.
3. **Ipotesi sui Vettori di Attacco:** Determinare, in base alle evidenze raccolte, le tecniche e i vettori utilizzati dall'attaccante (es. scansioni, exploit di vulnerabilità).
4. **Proposta di Remediation:** Fornire raccomandazioni pratiche e immediate per mitigare l'attacco rilevato e mettere in sicurezza l'infrastruttura da tentativi futuri.

L'obiettivo è capire **chi** sta attaccando, **come** lo sta facendo e **come fermarlo**, basandosi sulle evidenze trovate nel file.

Identificazione e Analisi degli IOC

Attore e Vittima

- **IP Attaccante:** `192.168.200.100`
- **IP Vittima:** `192.168.200.150`

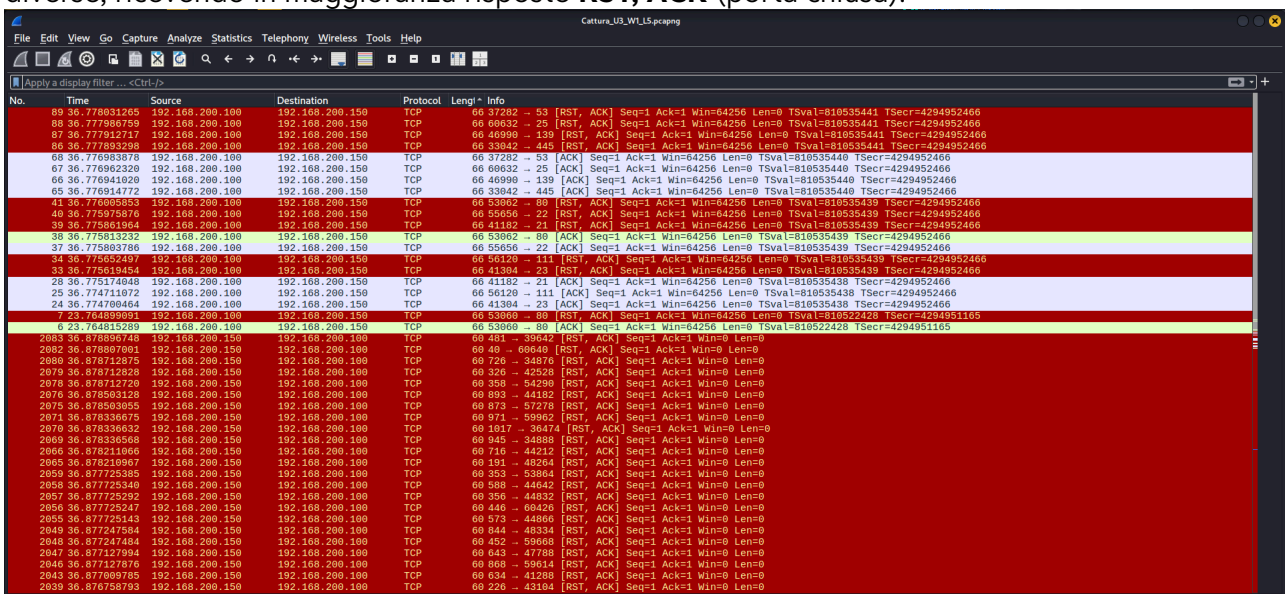
> ✨ **Identificazione Attaccante vs Vittima**
>
> Per distinguere i ruoli si analizza la colonna *Info* o i *Flags* TCP:
>
> - **L'Attaccante** (`192.168.200.100`) è l'host che invia pacchetti con il solo flag **[SYN]** attivato (richiesta di connessione). È riconoscibile perché la porta di *Destinazione* cambia continuamente in ogni pacchetto sequenziale.
> - **La Vittima** (`192.168.200.150`) è l'host che risponde inviando pacchetti con i flag **[RST, ACK]** (rifiuto) o **[SYN, ACK]** (conferma). La sua attività è puramente di

risposta alle porte sollecitate dall'attaccante.

Dall'analisi dei pacchetti catturati con Wireshark, sono emersi i seguenti indicatori di compromissione:

1. **Attività di Scansione (SYN Scan)**

   È stato rilevato un volume anomalo di traffico TCP originato dall'IP `192.168.200.100` verso l'IP `192.168.200.150`. L'attaccante invia pacchetti con flag **SYN** in rapida successione verso porte diverse, ricevendo in maggioranza risposte **RST, ACK** (porta chiusa).



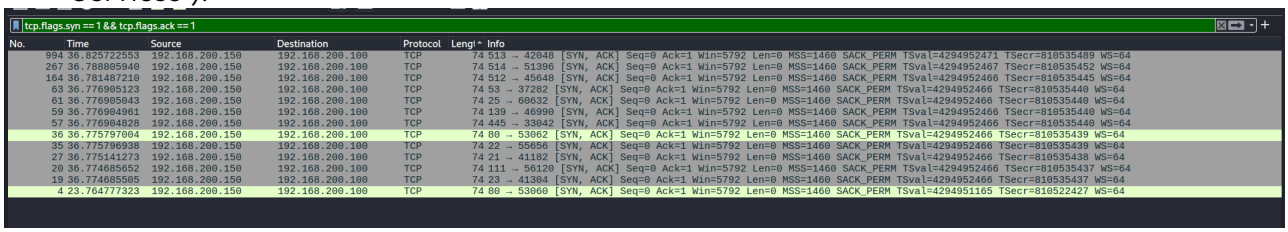
> **Interpretazione dell'immagine**
>
> L'immagine di cui sopra, mostra una panoamica del traffico TCP.
>
> In particolare:
>
> - Riga rossa → PORTA CHIUSA `[RST, ACK]` (Reset).
> - Riga Grigia → TRAFFICO TCP NORMALE. Si hanno due scenari:
>   - Se si legge `[SYN]`**:** È la **domanda** dell'attaccante
>   - Se si legge `[SYN, ACK]`**:** È la **risposta positiva** della vittima **PORTA APERTA**.
> - Riga Verde → FILTRO ATTIVO / HTTP

2. **Servizi Esposti (Porte Aperte)**

   Applicando il filtro su Wireshark `tcp.flags.syn == 1 && tcp.flags.ack == 1`, è stato possibile isolare le porte **aperte**, ovvero quelle dove la vittima ha risposto confermando la disponibilità del servizio. La superficie di attacco rilevata è estremamente estesa e critica:

   - **Porta 21 (FTP):** Trasferimento file in chiaro.

- **Porta 22 (SSH):** Shell remota cifrata.
- **Porta 23 (Telnet):** Shell remota in chiaro.
- **Porta 25 (SMTP):** Server di posta.
- **Porta 53 (DNS):** Servizio Domain Name System.
- **Porta 80 (HTTP):** Web Server.
- **Porta 111 (RPCbind):** Mappatura procedure remote.
- **Porta 139 / 445 (NetBIOS/SMB):** Condivisione file.
- **Porte 512 / 513 / 514 (exec, login, shell):** Servizi di amministrazione remota legacy ("R-Services").

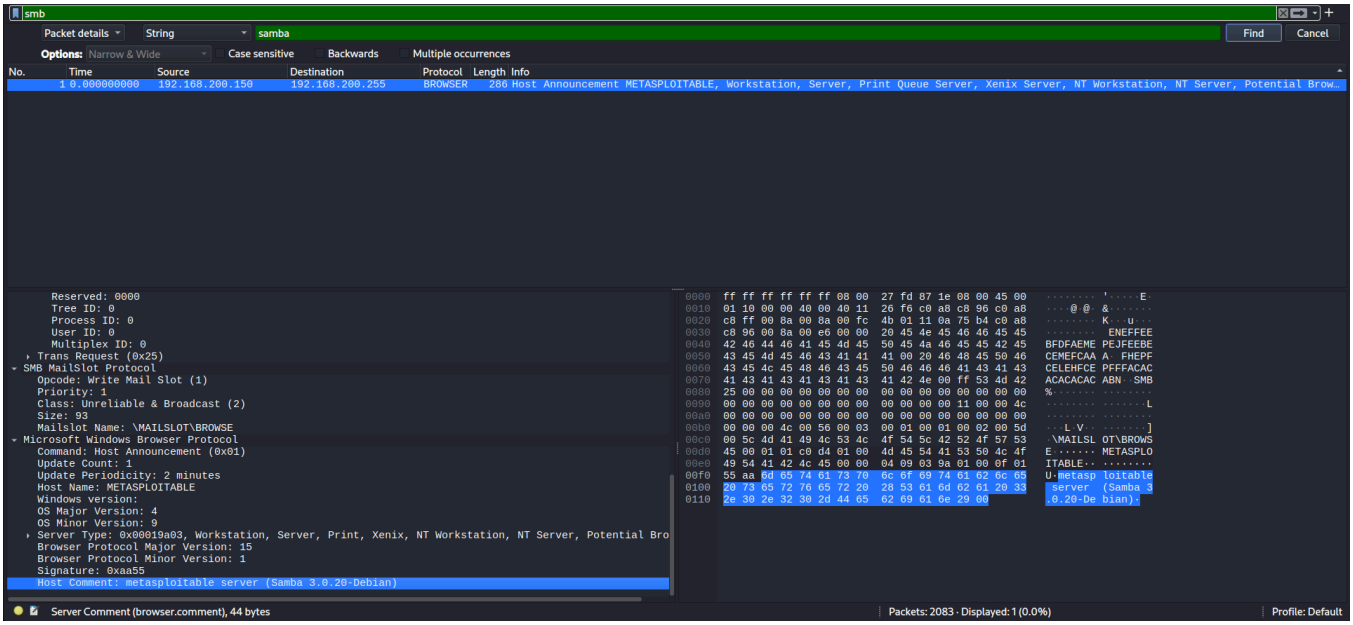


> **Che cos'è Wireshark?**
>
> **Wireshark** è l'analizzatore di protocolli di rete (*packet sniffer*) open-source più diffuso al mondo. Funziona intercettando il traffico dati che transita su un'interfaccia di rete e lo decodifica in un formato leggibile dall'uomo.

Information Disclosure (Software Versioning)

L'analisi del payload dei pacchetti SMB (Porta 445) ha permesso di intercettare il banner del servizio, esponendo informazioni sensibili:

- **Sistema Operativo:** `Unix/Debian`.
- **Versione Software:** `Samba 3.0.20-Debian`.
- **Nome Host:** `METASPLOITABLE`.



> **La Criticità dell'Information Disclosure**
>
> Risalire alle informazioni esposte dai servizi (come la versione esatta di un software o il sistema operativo) è un passaggio cruciale nella catena di un attacco informatico (Cyber Kill Chain).
>
> Questo fenomeno, noto come **Information Disclosure**, permette all'attaccante di passare da un tentativo "alla cieca" a un **attacco mirato**. Conoscendo la versione specifica (es. *Samba 3.0.20*), l'attaccante può consultare database pubblici di vulnerabilità (come **CVE** o **Exploit-DB**) per individuare falle di sicurezza note e scaricare il codice malevolo (exploit) esatto per quella versione, garantendosi il successo dell'intrusione con il minimo sforzo.

Ipotesi sui Vettori di Attacco

Sulla base degli IOC raccolti, lo scenario di attacco imminente prevede:

1. **Exploit RCE su Samba (`Critico`):** La versione `Samba 3.0.20` identificata è affetta dalla vulnerabilità *CVE-2007-2447 ("Username Map Script")*. È altamente probabile che l'attaccante sfrutterà questa falla per ottenere una shell di root inviando un payload malevolo, aggirando l'autenticazione.
2. **Trust Exploitation su R-Services:** La presenza delle porte **512/513/514** indica l'uso di protocolli legacy (`rlogin/rsh`) che spesso autenticano basandosi solo sull'IP sorgente (misconfiguration file `.rhosts`), permettendo accesso immediato senza password.
3. **Brute Force su Telnet/FTP:** I servizi sulle porte **21** e **23** trasmettono credenziali in chiaro, esponendo il sistema a sniffing o attacchi a dizionario.

Raccomandazioni e Mitigazione

Azioni Immediate (Contenimento)

- **Isolamento:** Disconnettere l'host `192.168.200.150` dalla rete aziendale (o spostarlo in una VLAN isolata per analisi forense).
- **Blocco Traffico:** Configurare il firewall per bloccare l'IP `192.168.200.100`.

Azioni di Hardening (Remediation)

1. **Dismissione Protocolli Insicuri:** Poiché il servizio **SSH (Porta 22)** è attivo e funzionante, è necessario disabilitare immediatamente **Telnet (23)**, **FTP (21)** e la suite **R-Services (512-514)**, migrando tutta l'amministrazione su canali cifrati.
2. **Patch Management:** Aggiornare urgentemente Samba a una versione supportata per mitigare la CVE-2007-2447.
3. **Network Segregation:** Assicurarsi che macchine vulnerabili di default (come *Metasploitable*) non siano mai esposte su reti di produzione.

Conclusioni

L'indagine ha confermato che l'host `192.168.200.150` rappresenta un rischio critico per l'organizzazione. L'attaccante ha completato con successo la fase di ricognizione, ottenendo tutte le informazioni necessarie (porte aperte e versioni software vulnerabili) per sferrare un attacco distruttivo nel breve termine.

Le evidenze raccolte non lasciano spazio a dubbi: il sistema è una "facile preda". L'intervento di bonifica proposto (isolamento e patching) non è solo consigliato, ma imperativo per prevenire una violazione dei dati o la compromissione totale del sistema tramite l'exploit noto di Samba.