REPORT S9/L5: Analisi Threat Intelligence & IOC

Studente: Vincenzo Zarola
Corso: Cybersecurity Specialist
Oggetto: Analisi di una cattura di rete per l'identificazione di Indicatori di Compromissione (IOC).

1. Obiettivo dell'Esercitazione

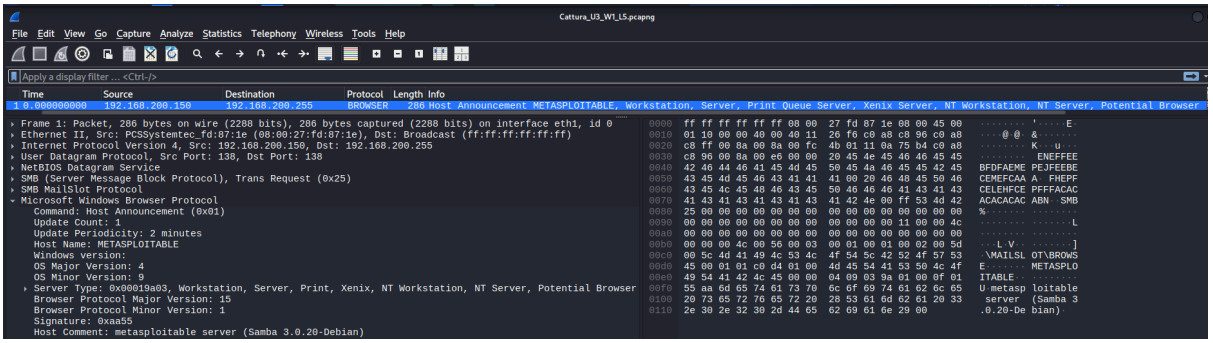
L'attività si concentra sull'analisi di un file di cattura (**Cattura_U3_W1_L5.pcapng**). L'obiettivo è identificare e analizzare eventuali IOC (Indicators of Compromise), ipotizzare i potenziali vettori di attacco e proporre strategie di difesa proattiva.

2. Identificazione e Analisi degli IOC

Dall'analisi approfondita dei pacchetti tramite Wireshark, sono stati isolati i seguenti indicatori di compromissione:

Information Leakage (Broadcast)

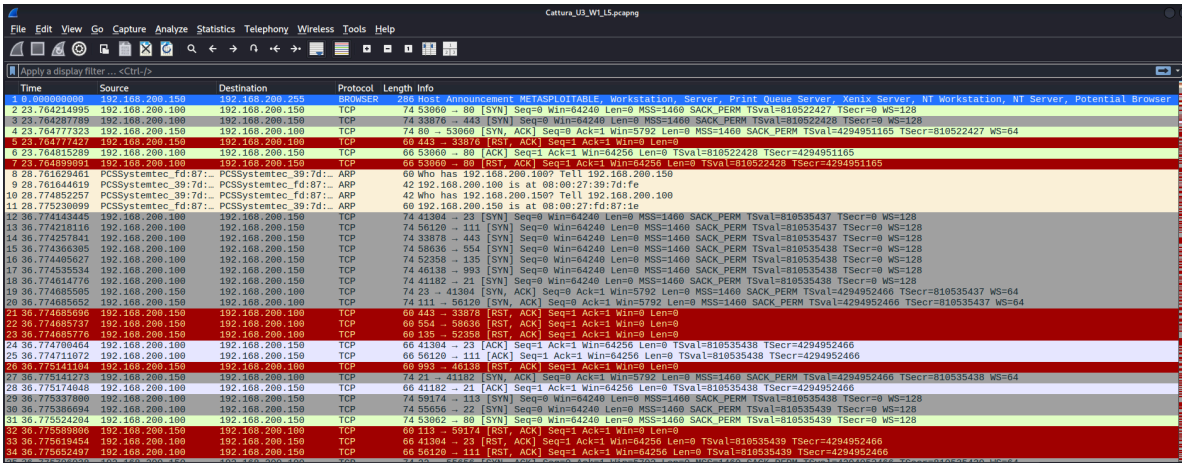
Il Pacchetto n°1 mostra un evento di "Host Announcement" inviato dall'indirizzo IP **192.168.200.150** verso il broadcast **192.168.200.255**.



- **Analisi:** Nel pannello di dettaglio del pacchetto, sotto il protocollo *Microsoft Windows Browser Protocol*, il sistema rivela in chiaro il proprio nome: **METASPLOITABLE**. Inoltre, il campo "Server Type" elenca servizi come *Workstation e Server*, esponendo la natura del sistema a chiunque sia in ascolto nella rete locale (Passive Reconnaissance).

Network Scanning (Active Reconnaissance)

A partire dal tempo **23.76s**, si osserva un traffico anomalo generato dall'host **192.168.200.100** verso **192.168.200.150**



- **Analisi:** L'host attaccante genera un volume elevato di pacchetti TCP [SYN] in un lasso di tempo ridottissimo (millisecondi). Questo pattern è la firma tipica di un **Port Scanner** automatizzato (come **Nmap**).
- **Risposta del Target:**
    - **Porte Chiuse:** Numerose risposte **[RST, ACK]** (righe rosse), che indicano tentativi di connessione falliti su porte non attive (es. porte 445, 995, 587).
    - **Porte Aperte:** Risposte **[SYN, ACK]** seguite da una chiusura immediata della connessione (RST) da parte dell'attaccante.

2 23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 → 80 [SYN] Seq=0
3 23.764287789	192.168.200.100	192.168.200.150	TCP	74 33876 → 443 [SYN] Seq=0
4 23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 → 53060 [SYN, ACK] Seq=0
5 23.764777427	192.168.200.150	192.168.200.100	TCP	60 443 → 33876 [RST, ACK] Seq=1
6 23.764815289	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1 Ack=1
7 23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK] Seq=1

Dall'analisi del Three-Way Handshake (visibile ad esempio nei pacchetti 2, 4 e 6), si nota che la connessione TCP viene completamente stabilita prima di essere resettata. Questo identifica la scansione come una **TCP Connect Scan (Nmap -sT)** e non come una SYN Scan (-sS), poiché l'attaccante invia il pacchetto ACK finale di conferma. Questa tecnica è meno furtiva e più facilmente rilevabile dai log di sistema rispetto a una scansione Stealth.

3. Ipotesi sui Vettori di Attacco

Basandosi sugli IOC rilevati e sulle porte risultate "APERTE" durante la scansione, possiamo ipotizzare che l'attaccante stia preparando un attacco mirato sfruttando i seguenti vettori:

1. **Vettore Telnet (Porta 23):** È stato rilevato un handshake completo sulla porta 23. Poiché Telnet trasmette dati in chiaro, l'attaccante potrebbe tentare un attacco di *Sniffing* o un *Brute Force* per ottenere le credenziali di accesso.
2. **Vettore Web (Porta 80):** La presenza della porta 80 aperta suggerisce la possibilità di attacchi verso l'applicazione web (es. SQL Injection, XSS) o tentativi di enumerazione delle directory (Gobuster).
3. **Vettore SMB (Porta 445):** Anche se alcuni tentativi sembrano resettati, la presenza di traffico SMB (visibile nel pacchetto 1 come protocollo sottostante) suggerisce che

l'attaccante potrebbe tentare exploit noti come *EternalBlue* o tentativi di accesso anonimo alle share di rete.

4. Azioni di Mitigazione e Risposta (Remediation)

Per ridurre l'impatto dell'attacco attuale e prevenire incidenti futuri, si consigliano le seguenti azioni:

A. Azioni Immediate (Containment)

- **Blocco IP:** Configurare una regola sul Firewall del router per bloccare tutto il traffico proveniente dall'IP **192.168.200.100**.
- **Analisi dei Log:** Verificare i log di sistema (Syslog/Event Viewer) della macchina **192.168.200.150** per confermare se, oltre alla scansione, ci siano stati tentativi di login (Event ID 4625).

B. Azioni Preventive (Hardening)

- **Disabilitazione Servizi Insicuri:** Il servizio Telnet (porta 23) deve essere immediatamente disattivato e sostituito con SSH (porta 22).
- **Disabilitazione NetBIOS:** Per evitare l'Information Leakage, disabilitare il protocollo NetBIOS over TCP/IP sulle interfacce di rete per impedire alla macchina di annunciare il proprio nome e ruolo in broadcast.
- **Implementazione SIEM/IDS:** Implementare un sistema di rilevamento intrusioni con regole specifiche per rilevare pattern di "Port Scanning" e allertare il team di sicurezza in tempo reale.
- **Automazione della Risposta (SOAR):** Integrare una soluzione SOAR configurando un **Playbook** automatico che, alla ricezione dell'alert "**Port Scan Detected**" dal SIEM, blocchi immediatamente l'IP attaccante sul Firewall senza intervento umano.