Report Tecnico: Analisi Threat Intelligence & IOC

Studente: Giuseppe Monaco

---

1. Introduzione

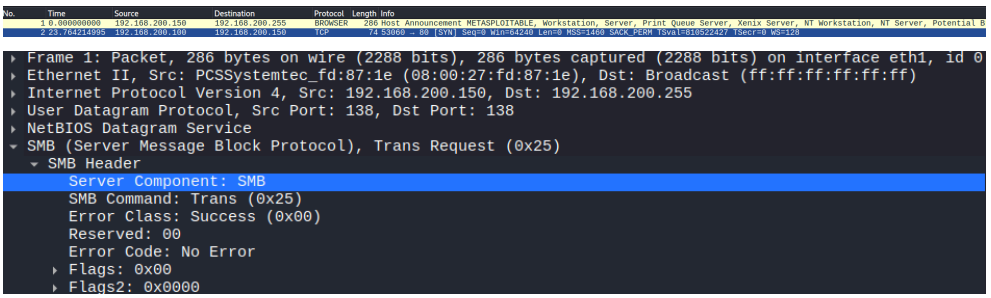
Il presente report documenta i risultati dell'analisi condotta sul file di log di rete fornito. L'obiettivo primario è isolare eventuali anomalie di traffico, identificare le entità coinvolte nella comunicazione e determinare se siano in corso tentativi di intrusione o attività di ricognizione ostile. L'esame è stato svolto mediante l'ausilio di *Wireshark* per l'ispezione dei pacchetti.

---

2. Identificazione degli Attori di Rete

L'analisi dei metadati e dei payload dei pacchetti ha permesso di delineare la topologia della comunicazione, individuando due nodi principali:

- **Host Sorgente (Minaccia):** `192.168.200.100`
    - Questo IP è l'iniziatore di quasi tutte le connessioni TCP, inviando richieste ad alta frequenza. Identificato come la macchina attaccante (Kali Linux).
- **Host Destinazione (Bersaglio):** `192.168.200.150`
    - Questo IP risponde passivamente alle sollecitazioni.
    - *Information Leakage:* Al pacchetto n. 1, l'host invia un broadcast SMB rivelando il proprio hostname: **METASPLOITABLE**. Questo ha permesso l'identificazione immediata della natura vulnerabile del sistema

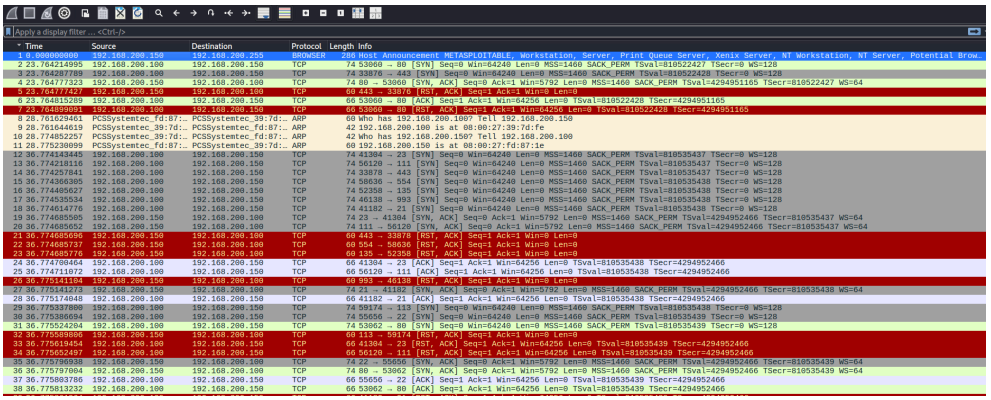


Analisi dell'immagine: Come evidenziato nello screenshot sopra:

- **Protocollo:** `BROWSER` (SMB)
- **Info:** Il pacchetto contiene la stringa *"Host Announcement METASPLOITABLE, Workstation, Server..."*.
- **Dettaglio Tecnico:** La vittima (`192.168.200.150`) sta inviando un pacchetto broadcast (`192.168.200.255`) rivelando il proprio Hostname (**METASPLOITABLE**) e il servizio utilizzato (**SMB**). Questo permette all'attaccante di identificare il bersaglio senza toccarlo attivamente.

3. Analisi Tecnica dell'Incidente: Port Scanning

Successivamente, si osserva un traffico massivo TCP indicativo di una scansione delle porte automatizzata.



Analisi dell'immagine: Lo screenshot evidenzia il pattern comportamentale di uno strumento di scansione (es. Nmap):

1. **Righe Grigie (Richiesta SYN):** L'attaccante (`192.168.200.100`) invia pacchetti **SYN** in rapida successione verso porte diverse della vittima (es. porte 199, 995, 587). È il tentativo di connessione iniziale.
2. **Righe Rosse (Risposta RST - Porta Chiusa):** La vittima (`192.168.200.150`) risponde con **RST, ACK** (Reset). Il colore rosso in Wireshark indica che la connessione è stata rifiutata, confermando all'attaccante che la porta è **CHIUSA**.
3. **Righe Grigio Chiaro/Verdi (Risposta SYN/ACK - Porta Aperta):** Dove la vittima risponde con **SYN, ACK**, indica che un servizio è in ascolto (Porta **APERTA**).

L'attività massiva osservata nei log identifica una tecnica specifica nota come **TCP SYN Scan** (o "Half-open scan").

- **SYN Scan:** È una tecnica di scansione in cui l'attaccante invia un pacchetto **SYN** (richiesta di sincronizzazione) come se volesse iniziare una connessione legittima. Tuttavia, non appena riceve una risposta positiva (**SYN-ACK**) dalla vittima, non completa il "three-way handshake" inviando l'ACK finale, ma tronca la comunicazione con un pacchetto **RST** (Reset).

L'obiettivo finale di questa operazione è il **Port Mapping** (mappatura delle porte). L'attaccante sta "bussando" a tutte le porte della macchina vittima per censire quali servizi sono attivi (es. Server Web, Database, File Sharing). Ogni porta aperta scoperta (evidenziata dai pacchetti SYN-ACK nei log) rappresenta una potenziale "porta d'ingresso" vulnerabile da attaccare nella fase successiva.

4. Valutazione della Superficie d'Attacco

Sulla base delle porte risultate aperte ("Open"), è stata stilata una lista dei vettori di rischio che l'attaccante potrebbe sfruttare nelle fasi successive:

1. **Accesso Remoto Insicuro (Porta 23 - Telnet):**
    - *Analisi:* Servizio critico obsoleto. A differenza di SSH, Telnet non cifra la connessione.
    - *Impatto:* Un attaccante in ascolto sulla rete può leggere username e password in chiaro.
2. **File Sharing Legacy (Porte 139/445 - SMB):**
    - *Analisi:* La versione rilevata (Samba) è spesso soggetta a vulnerabilità gravi (es. *Exploit Username Map Script*).
    - *Impatto:* Rischio elevatissimo di esecuzione remota di codice (RCE) e compromissione totale del server.
3. **Trasferimento File (Porta 21 - FTP):**
    - *Analisi:* Protocollo spesso configurato male (es. accesso anonimo abilitato).
    - *Impatto:* Possibile esfiltrazione di dati o caricamento di file malevoli.
4. **Servizi Web (Porta 80 - HTTP):**
    - *Analisi*: Presenza di un Web Server in chiaro. Su macchine come Metasploitable, questo ospita tipicamente applicazioni web vulnerabili (es. DVWA, Mutillidae).
    - *Impatto***:** Esposizione a vulnerabilità applicative come SQL Injection, XSS o Remote File Inclusion (RFI).
5. **Gestione Remota Sicura (Porta 22 - SSH):**
    - *Analisi***:** Sebbene sia il sostituto sicuro di Telnet , la sua presenza indica un punto di ingresso amministrativo.

    - *Impatto*: Anche se il traffico è cifrato, il servizio rimane esposto ad attacchi di Brute-Force se protetto solo da password deboli (es. msfadmin:msfadmin).

---

5. Strategie di Difesa e Mitigazione

L'analisi conferma che la macchina `192.168.200.150` è un bersaglio attivo di ricognizione. L'attaccante ha identificato con successo la natura vulnerabile del sistema ("Metasploitable").

Azioni Consigliate:

- **Hardening dei Servizi:** Rimuovere immediatamente i protocolli che trasmettono in chiaro (**Telnet, FTP**) migrando verso alternative cifrate (**SSH, SFTP**).
- **Segmentazione e Firewalling:** Configurare regole di firewall per bloccare scansioni rapide (rate-limiting) e impedire l'accesso alle porte SMB (139, 445) da IP non amministrativi.
- **Gestione sicura di SMB:** La best practice prevede la chiusura delle porte 139 e 445 per prevenire vettori di attacco noti. Se l'infrastruttura richiede tale protocollo, è mandatorio eseguire l'upgrade all'ultima release stabile e imporre l'autenticazione obbligatoria per tutti gli utenti.