Obiettivo:

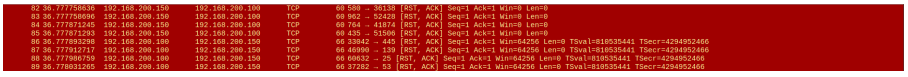
Analizzate la cattura `WireShark` attentamente e rispondere ai seguenti quesiti:
● Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso .
● In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati .
● Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

1. Identificazione e Analisi degli IOC

Dall'analisi del traffico di rete, ho identificato diversi **Indicatori di Compromissione(IoC)** che suggeriscono un attacco in corso :

IOC 1: Scansione di Rete (Reconnaissance)

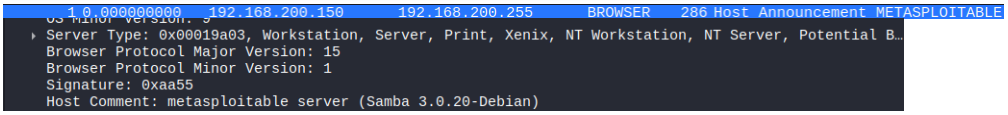
- **Evidenza:** Un volume anomalo di pacchetti TCP **SYN/ACK** provenienti dal target e diretti a un singolo host , senza che segua il pacchetto **ACK** finale per completare la connessione (che viene invece interrotta con un **RST**).



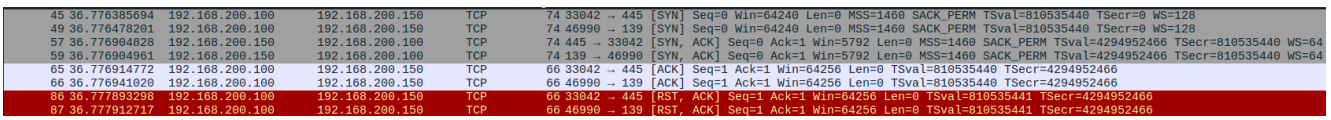
- **Analisi:** Questo è il comportamento distintivo di una scansione **Nmap SYN Scan** (nota come `-sS` o *half-open scan*).
- **Significato:** L'attaccante stava mappando la superficie d'attacco del target per trovare porte aperte e servizi esposti, non è interessato a stabilire una connessione ma solo di prendere nota di chi ha risposto.

IOC 2: Service Fingerprinting (Enumerazione)

- **Evidenza:** Traffico SMB (Server Message Block) che identifica il servizio come `metasploitable server (Samba 3.0.20-Debian)` .



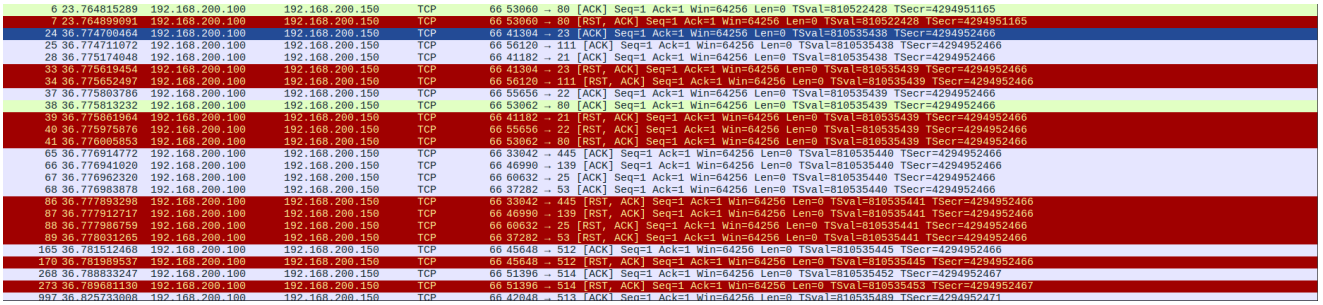
- **Analisi:** Dopo aver trovato la porta aperta (probabilmente la 139 o 445) con la scansione precedente, l'attaccante ha interagito con essa per carpirne l'identità. Il server ha risposto fornendo il suo nome (`metasploitable`) la sua versione software esatta: **Samba 3.0.20**.



- **Significato:** Questo è l'IOC critico. Il server ha fornito all'attaccante l'informazione esatta di cui aveva bisogno per trovare un exploit noto.

2. Analisi delle Connessioni Complete

Tramite un ordinamento dei log per lunghezza riusciamo ad avere evidenza delle connessioni che hanno completato il 3-way-handshake.



6	23.764815289	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66 45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
170	36.781989537	192.168.200.100	192.168.200.150	TCP	66 45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
268	36.788833247	192.168.200.100	192.168.200.150	TCP	66 51396 → 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535452 TSecr=4294952467
273	36.789681130	192.168.200.100	192.168.200.150	TCP	66 51396 → 514 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535453 TSecr=4294952467
997	36.825733008	192.168.200.100	192.168.200.150	TCP	66 42048 → 513 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535489 TSecr=4294952471

L'attaccante ha usato queste connessioni per la scansione delle versioni (`-sV`) possiamo valutare la gravità di ciò che l'attaccante ha trovato:

- **Porte 139/445 (NetBIOS/SMB):** Identificate come **Critiche**. Questa connessione ha permesso all'attaccante di scoprire il servizio `Samba 3.0.20` (IOC 2), un vettore noto per ransomware ed exploit RCE (Remote Code Execution) come la CVE-2007-2447.
- **Porte 23 (Telnet) e 512/513/514 (R-Services):** Identificate come **Legacy/Insicuro**. L'attaccante ha confermato la presenza di protocolli obsoleti, non cifrati, che espongono le credenziali in chiaro.
- **Porta 21 (FTP):** Rischio di trasferimento file in chiaro e attacchi brute-force.
- **Porta 22 (SSH):** Rischio di attacchi brute-force sulle password e potenziale furto di chiavi.
- **Porta 80 (HTTP):** Rischio di enumerazione delle versioni del web server e di web exploit.
- **Porte 25 (SMTP), 53 (DNS), 111 (RPCbind):** Rischi di enumerazione di utenti, zone transfer e mappatura dei servizi RPC.

In sintesi, l'attaccante non solo ha trovato le porte aperte, ma ha stabilito una connessione con ciascuna di esse, confermando la presenza di servizi multipli, molti dei quali critici o insicuri.

3. Ipotesi sul Vettore di Attacco

Il vettore di attacco è una ricognizione attiva in due fasi:

1. **Fase 1 (Ricognizione):** L'attaccante esegue una **scansione Nmap SYN (`-sS`)** sull'IP del server per identificare rapidamente *tutte* le porte aperte (IOC 1).
2. **Fase 2 (Enumerazione):** L'attaccante esegue una **scansione delle versioni (`-sV`)** *solo* sulle porte aperte trovate. Questo richiede connessioni TCP complete (confermate dai pacchetti `[ACK]` puri).
3. **Fase 3 (Analisi Vulnerabilità):** L'attaccante ora ha una lista di servizi e versioni (come da tabella). L'informazione `Samba 3.0.20` è un allarme rosso, poiché è legata alla vulnerabilità critica **CVE-2007-2447**.

L'attaccante ha completato la sua ricognizione. Il prossimo passo logico sarebbe lanciare un exploit contro la versione vulnerabile di Samba.

4. Azioni di Remediation e Hardening

L'analisi ha rivelato una superficie d'attacco ampia e non protetta, che ha permesso all'attaccante di enumerare con successo molteplici servizi critici e obsoleti. Il piano di remediation deve essere strutturato in tre fasi: contenimento immediato, hardening tattico e hardening strategico.

Fase 1: Remediation Immediata (Correzione delle Vulnerabilità Note)

1. **Isolamento e Patching:** L'host deve essere immediatamente isolato in una VLAN di quarantena per impedirne l'exploit. La vulnerabilità critica `Samba 3.0.20` (CVE-2007-2447) deve essere risolta:
   - **Soluzione 1 (Patching):** Eseguire un aggiornamento completo del sistema.
   - **Soluzione 2 (Mitigazione):** Se il patching non è possibile, disabilitare la funzione vulnerabile modificando `/etc/samba/smb.conf` e commentando la direttiva `username map script`
2. **Blocco dell'IP Attaccante:** Come primissima azione, l'IP sorgente della scansione (`192.168.200.100`) deve essere immediatamente aggiunto a una *blocklist* sul firewall perimetrale o sull'IPS (Intrusion Prevention System).

Fase 2: Hardening Tattico (Principio del Minimo Privilegio)

L'obiettivo è ridurre la superficie d'attacco a *zero* tranne che per i servizi esplicitamente richiesti.

1. **Disabilitazione dei Servizi Obsoleti:** I servizi `Legacy/Insicuro` identificati (Telnet, R-Services, FTP) non devono essere esposti. Non è sufficiente bloccarli con un firewall; devono essere disabilitati o disinstallati.
2. **Firewalling State-Aware (Host-based):** Implementare un firewall a livello host (`ufw` o `firewalld`) con una politica di **default-deny**

Fase 3: Hardening Strategico (Defense-in-Depth)

Queste misure rendono la ricognizione molto più difficile.

1. **Oscuramento dei Banner di Servizio:** Per impedire l'IOC 2 (Enumerazione delle Versioni), modificare le configurazioni per non rivelare le versioni del software:
   - **Samba (`/etc/samba/smb.conf`):** `server string = Production Server` (Rimuove la versione di Samba/Debian)
   - **SSH (`/etc/ssh/sshd_config`):** `DebianBanner no` (Nasconde il banner specifico del sistema operativo)
   - **Apache (`/etc/apache2/conf-available/security.conf`):** `ServerTokens Prod` `ServerSignature Off`

2. **Controllo degli Accessi Avanzato: Port Knocking** Questa è una tecnica eccellente per proteggere i servizi di amministrazione come **SSH (porta 22)**.
    - **Analogia (La Bussata Segreta):** Pensa al firewall come a una porta blindata senza serratura visibile. L'attaccante (Nmap) vede solo un muro. L'amministratore legittimo esegue una "bussata segreta" (invia pacchetti a una sequenza di porte chiuse, es. 7000, 8000, 9000). Un demone (`knockd`) sul server ascolta questa sequenza e, se corretta, modifica dinamicamente le regole del firewall (`iptables`) per aprire la porta SSH *solo* all'IP dell'amministratore.
    - **Perché è efficace:**
        - Rende la porta SSH (o qualsiasi porta protetta) **invisibile** alle scansioni Nmap. Per l'attaccante, la porta 22 *non esiste*.
        - Elimina completamente gli attacchi brute-force, poiché l'attaccante non può nemmeno *raggiungere* il servizio per tentare una password.

5. Conclusione e Valutazione del Rischio

L'analisi del traffico di rete ha confermato un'attività di ricognizione ostile, mirata e metodica contro l'host `192.168.200.150`. L'attore della minaccia ha completato con successo l'intera fase di *Reconnaissance* ed *Enumeration*.

- Utilizzando una scansione `SYN` per la scoperta iniziale, seguita da una scansione di versione (`-sV`) sulle porte aperte, l'attaccante ha costruito una mappa dettagliata della superficie d'attacco. Questa mappa include numerosi servizi obsoleti, insicuri e non cifrati.
- L'indicatore di compromissione (IOC) più critico è l'identificazione positiva del servizio **Samba 3.0.20-Debian**. Questa versione è affetta dalla nota vulnerabilità di Esecuzione di Codice in Remoto **CVE-2007-2447**, per la quale esistono exploit pubblici e automatizzati.

Valutazione Finale

Allo stato attuale, l'incidente è classificato come **precursore di un attacco**. L'attaccante possiede ora un'intelligence completa e ha verificato la presenza di un vettore di exploit diretto. Il rischio di una compromissione totale del sistema (ottenimento di una *reverse shell* con privilegi `root`) è da considerarsi **imminente**.

Si raccomanda l'applicazione **immediata** e completa del piano di remediation e hardening descritto nella Sezione 4.