

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 anormale 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).

No.	Time	Source	Destination	Protocol	Length	Info
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
88	36.777986750	192.168.200.100	192.168.200.150	TCP	66	60832 → 25 [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	46998 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 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
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
67	36.776962329	192.168.200.100	192.168.200.150	TCP	66	60832 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941920	192.168.200.100	192.168.200.150	TCP	66	46998 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 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
110	36.776905353	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
39	36.775961964	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
38	36.775912332	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
37	36.775893786	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
34	36.775654297	192.168.200.100	192.168.200.150	TCP	66	56128 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
33	36.775619458	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
23	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
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56128 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
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
6	23.764109093	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
2083	36.878896748	192.168.200.100	192.168.200.150	TCP	66	481 → 39642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2082	36.878897901	192.168.200.100	192.168.200.150	TCP	66	48 → 60840 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2080	36.878712875	192.168.200.100	192.168.200.150	TCP	66	726 → 34876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2079	36.878712828	192.168.200.100	192.168.200.150	TCP	66	326 → 42528 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2078	36.878712720	192.168.200.100	192.168.200.150	TCP	66	358 → 54288 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2076	36.878693126	192.168.200.100	192.168.200.150	TCP	66	893 → 44182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2075	36.878693055	192.168.200.100	192.168.200.150	TCP	66	873 → 57278 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2071	36.878336675	192.168.200.100	192.168.200.150	TCP	66	871 → 59962 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2070	36.878336632	192.168.200.100	192.168.200.150	TCP	66	1017 → 36474 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2069	36.878336568	192.168.200.100	192.168.200.150	TCP	66	945 → 34888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2066	36.878211666	192.168.200.100	192.168.200.150	TCP	66	716 → 44212 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2065	36.878210907	192.168.200.100	192.168.200.150	TCP	66	191 → 48264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2060	36.877725385	192.168.200.100	192.168.200.150	TCP	66	353 → 53904 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2058	36.877725340	192.168.200.100	192.168.200.150	TCP	66	588 → 44642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2057	36.877725292	192.168.200.100	192.168.200.150	TCP	66	356 → 44032 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2056	36.877725247	192.168.200.100	192.168.200.150	TCP	66	446 → 60426 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2055	36.877725143	192.168.200.100	192.168.200.150	TCP	66	573 → 44860 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2049	36.877247584	192.168.200.100	192.168.200.150	TCP	66	844 → 48334 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2048	36.877247484	192.168.200.100	192.168.200.150	TCP	66	452 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2047	36.877127994	192.168.200.100	192.168.200.150	TCP	66	643 → 47788 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2046	36.877127876	192.168.200.100	192.168.200.150	TCP	66	868 → 59614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2043	36.877099785	192.168.200.100	192.168.200.150	TCP	66	634 → 41288 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2039	36.876759793	192.168.200.100	192.168.200.150	TCP	66	226 → 43164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Interpretazione dell'immagine

L'immagine di cui sopra, mostra una panoramica 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").

No.	Time	Source	Destination	Protocol	Length	Info
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64
267	36.788895940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
63	36.77695123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61	36.776959843	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59	36.776949861	192.168.200.150	192.168.200.100	TCP	74	139 → 46998 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
57	36.776948226	192.168.200.150	192.168.200.100	TCP	74	445 → 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
36	36.775797064	192.168.200.150	192.168.200.100	TCP	74	88 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55658 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
27	36.775441273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
19	36.774685585	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	88 → 53968 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64

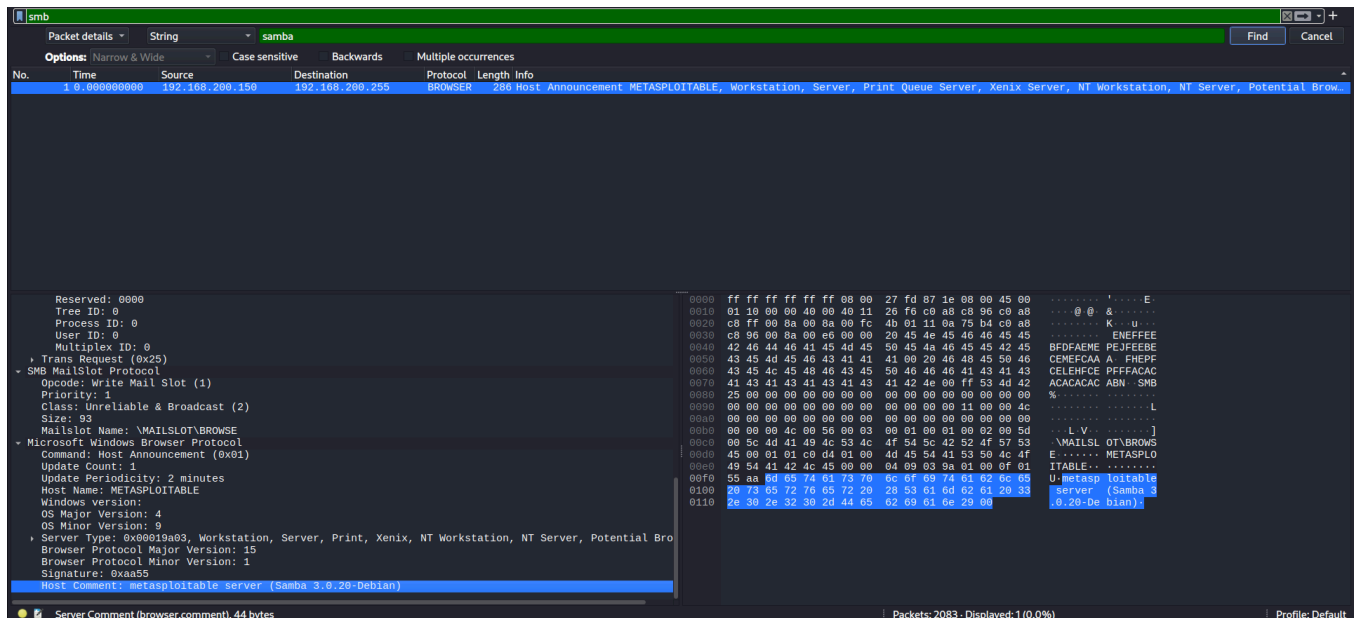
Che cos'è Wireshark?

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 **Immedieate** (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.