Threat Intelligence & IOC

Introduzione

Il presente documento ha lo scopo di analizzare un file di cattura di rete (.pcapng) per identificare potenziali attività malevole intercorse tra due host. L'analisi è stata condotta in ambiente virtualizzato Kali Linux utilizzando il software Wireshark per l'ispezione profonda dei pacchetti.

Obiettivi dell'analisi

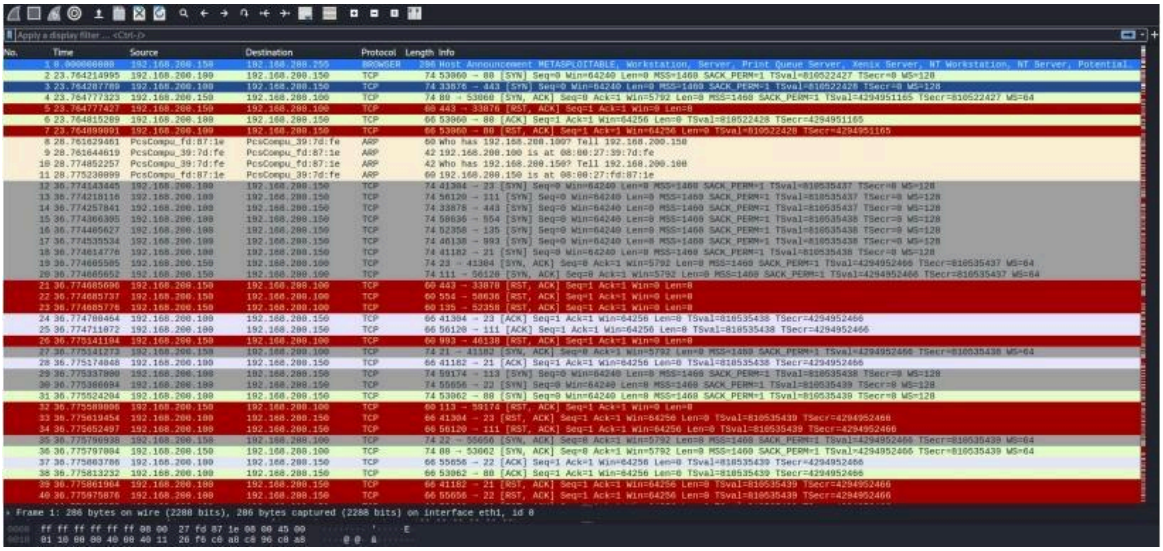
- Identificare gli host coinvolti (Attaccante e Vittima)
- Rilevare anomalie nel traffico di rete
- Isolare gli Indicatori di Compromissione (IOC)
- Mappare i servizi esposti e vulnerabili

Analisi dei Flussi e Identificazione Host

Dall'analisi preliminare dei log, è stato possibile distinguere i ruoli dei dispositivi nella rete:

Indirizzo IP Attaccante (Source): 192.168.200.100

Indirizzo IP Vittima (Destination): 192.168.200.150



Broadcast iniziale e identificazione sistema

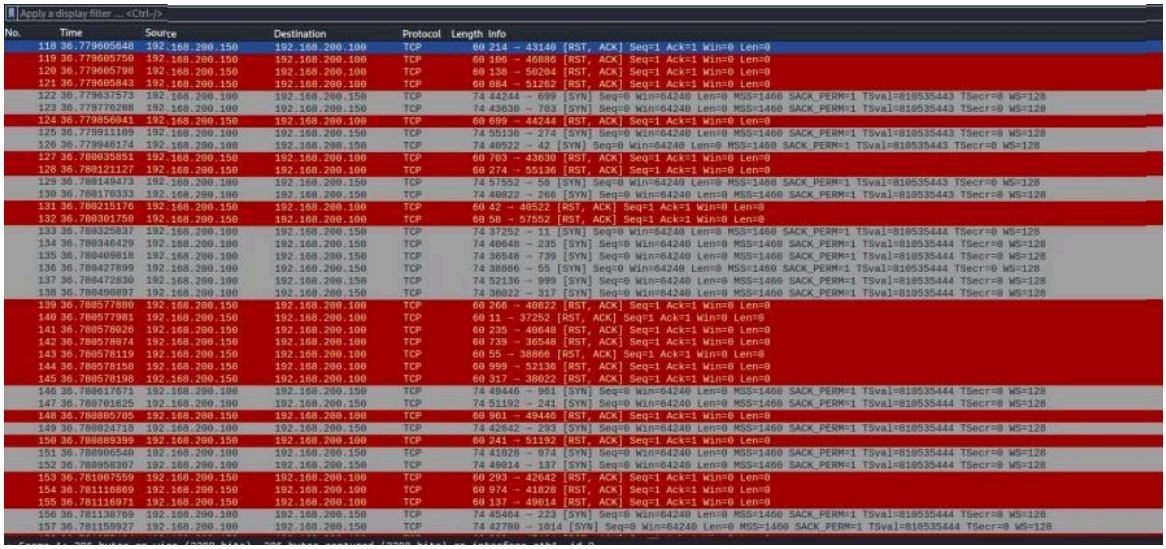
Il log iniziale (Riga 0) mostra un messaggio **broadcast** che identifica la macchina come "**Metasploitable**", un sistema volutamente vulnerabile utilizzato per test di sicurezza.*Traffico iniziale e scambi ARP tra attaccante e vittima*

Risoluzione indirizzi (ARP)

Nelle righe da 8 a 11, si osserva traffico **ARP (Address Resolution Protocol)**, necessario alle macchine per identificare i rispettivi indirizzi MAC e iniziare la comunicazione a livello 2 del modello OSI.

Analisi dell'Attacco: Scansione Porte

L'anomalia principale è rappresentata da una raffica di pacchetti TCP con flag **[SYN]** inviati dall'attaccante verso la vittima in un brevissimo lasso di tempo (pochi millisecondi).



Sequenza di pacchetti SYN durante la fase di port scanning

Caratteristiche dell'attacco

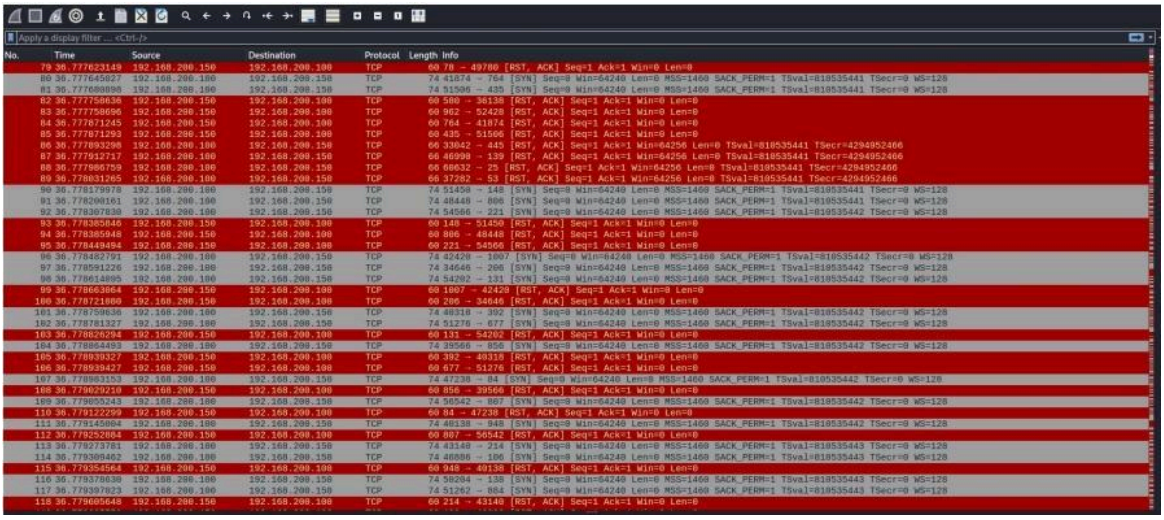
Questa attività è classificabile come **Port Scan**, presumibilmente eseguito tramite il tool **Nmap**. L'attaccante non sta scansionando tutte le porte sequenzialmente, ma mira alle porte "Well-Known" (es. 21, 22, 23, 25, 53, 80, 111, 139, 445), suggerendo l'uso di un comando di scansione veloce.

Risposta del sistema target

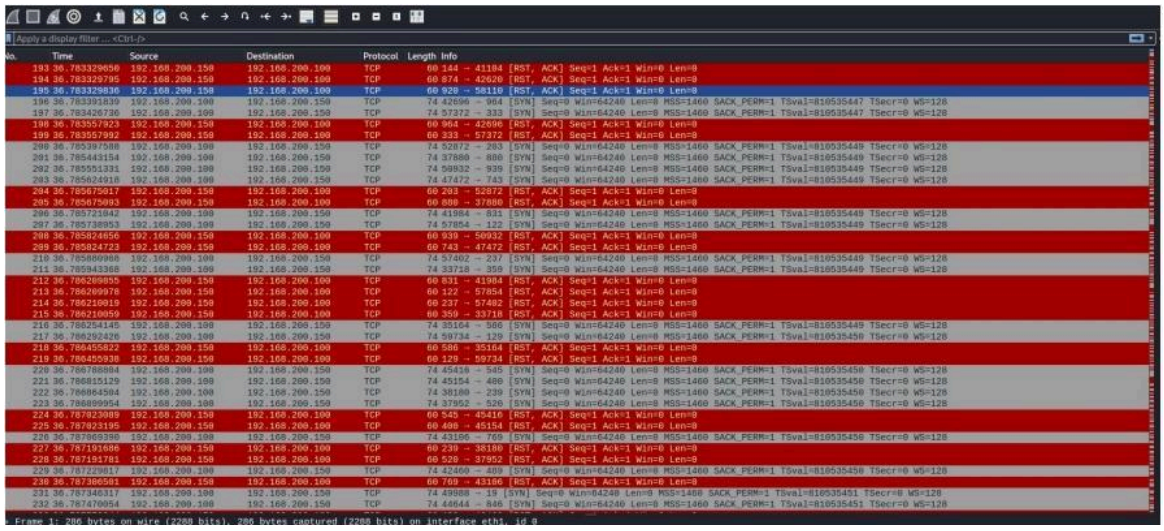
Analizzando le risposte della vittima, possiamo distinguere i servizi attivi da quelli inattivi:

- **Porte Chiuse (Closed)**: La vittima risponde con un pacchetto **[RST, ACK]** (Reset). Questo indica che nessun servizio è in ascolto su quella porta.

- **Porte Aperte (Open)**: La vittima risponde con **[SYN, ACK]**, accettando la connessione e completando il three-way handshake TCP.



Risposte RST e ACK alle scansioni su porte chiuse



Risposte SYN-ACK indicanti porte aperte con servizi attivi

Porte identificate come aperte

Porta	Servizio	Risposta
21	FTP	[SYN, ACK]
22	SSH	[SYN, ACK]
23	Telnet	[SYN, ACK]
25	SMTP	[RST, ACK]
53	DNS	[RST, ACK]
80	HTTP	[SYN, ACK]

111	RPCbind	[SYN, ACK]
139	NetBIOS-SSN	[RST, ACK]
445	SMB	[RST, ACK]

Risultati della scansione porte

Analisi dei Servizi Vulnerabili: Threat Intelligence

Dall'analisi delle risposte positive **([SYN, ACK])**, sono stati identificati i seguenti servizi attivi, che rappresentano vettori di attacco critici per la macchina Metasploitable:

Porta 23 – Telnet

Telnet è un protocollo datato che invia tutto il traffico, comprese le credenziali di accesso, in formato non cifrato.

Livello di criticità: Alto

Impatto: Un aggressore presente sulla stessa rete può catturare il traffico, ricostruire username e password tramite attività di sniffing e arrivare fino ai privilegi di root sulla macchina bersaglio (attacco Man-in-the-Middle).

Esempi di vulnerabilità note: CVE-2011-4862, CVE-2020-10188

Mitigazione consigliata: Disabilitare il servizio Telnet e utilizzare esclusivamente SSH per l'accesso remoto sicuro.

Porte 139 e 445 – Samba/SMB

Le porte 139 e 445 sono usate dai servizi Samba/SMB per la condivisione di cartelle e stampanti in ambito di rete locale.

Livello di criticità: Critico

Impatto: Lo stack SMB è stato spesso al centro di exploit che consentono esecuzione di codice da remoto, rappresentando un vettore privilegiato per campagne ransomware e worm, come dimostrato dagli attacchi WannaCry ed EternalBlue.

Esempi di vulnerabilità note: CVE-2017-0144 (EternalBlue), CVE-2017-7494 (SambaCry)

Mitigazione consigliata: Aggiornare immediatamente a versioni non vulnerabili o chiudere completamente le porte se il servizio non è strettamente necessario.

Porta 21 – FTP

FTP, analogamente a Telnet, trasferisce spesso le credenziali di autenticazione e i dati applicativi in chiaro.

Livello di criticità: Medio/Alto

Impatto: Oltre alla possibilità di intercettare username e password, implementazioni obsolete di server FTP possono includere backdoor (ad esempio vsftpd 2.3.4) o permettere accessi anonimi a directory sensibili del sistema.

Esempi di vulnerabilità note: CVE-2011-2523 (backdoor in vsftpd)

Mitigazione consigliata: Migrare a protocolli sicuri come SFTP o FTPS e disabilitare ogni forma di accesso anonimo.

Porta 111 – RPCbind

Il servizio RPCbind associa i numeri di programma RPC alle porte utilizzate sulla rete, fungendo da "registro" per i servizi RPC.

Livello di criticità: Medio

Impatto: Un uso improprio di RPCbind permette a un attaccante di enumerare i servizi RPC disponibili, ottenendo informazioni utili per preparare un attacco mirato e aumentando la superficie di esposizione (information disclosure).

Esempi di vulnerabilità note: CVE-2017-8779 (vulnerabilità rpcbind)

Mitigazione consigliata: Limitare l'accesso al servizio tramite regole di firewall, consentendo le richieste solo da host fidati, e, ove possibile, vincolare l'ascolto all'interfaccia di loopback.

Conclusioni e Raccomandazioni

L'analisi forense ha confermato che l'host **192.168.200.150** è stato oggetto di una ricognizione attiva (**Port Scanning**) da parte dell'host **192.168.200.100**, la quale ha esposto numerosi servizi obsoleti e non sicuri.

Azioni raccomandate per la messa in sicurezza

Priorità Critica (Immediate)

1. **Dismissione Servizi Insicuri**: Disattivare immediatamente Telnet (23) e sostituirlo con SSH (22), che garantisce la cifratura del traffico end-to-end
2. **Hardening SMB**: Se la condivisione file non è strettamente necessaria, chiudere le porte 139/445. Se necessaria, aggiornare il servizio all'ultima versione e disabilitare l'accesso anonimo
3. **Configurazione Firewall**: Implementare regole di firewall per bloccare il traffico in ingresso su porte non essenziali e limitare l'accesso alle sole sottoreti di gestione autorizzate

Priorità Alta (Breve termine)

1. Implementazione sistema IDS/IPS per rilevamento port scanning
2. Segmentazione della rete per isolare sistemi critici
3. Implementazione logging centralizzato e SIEM
4. Configurazione rate limiting su servizi esposti

Priorità Media (Medio termine)

1. Vulnerability assessment periodici con scanner automatizzati
2. Implementazione di policy di patch management
3. Security awareness training per il personale
4. Implementazione di network access control (NAC)
