Progetto Settimanale S9L5 - Threat Intelligence & IOC
Sergio Falcone

INTRODUZIONE

Analizzate la cattura di rete effettuata con 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

PREFAZIONE

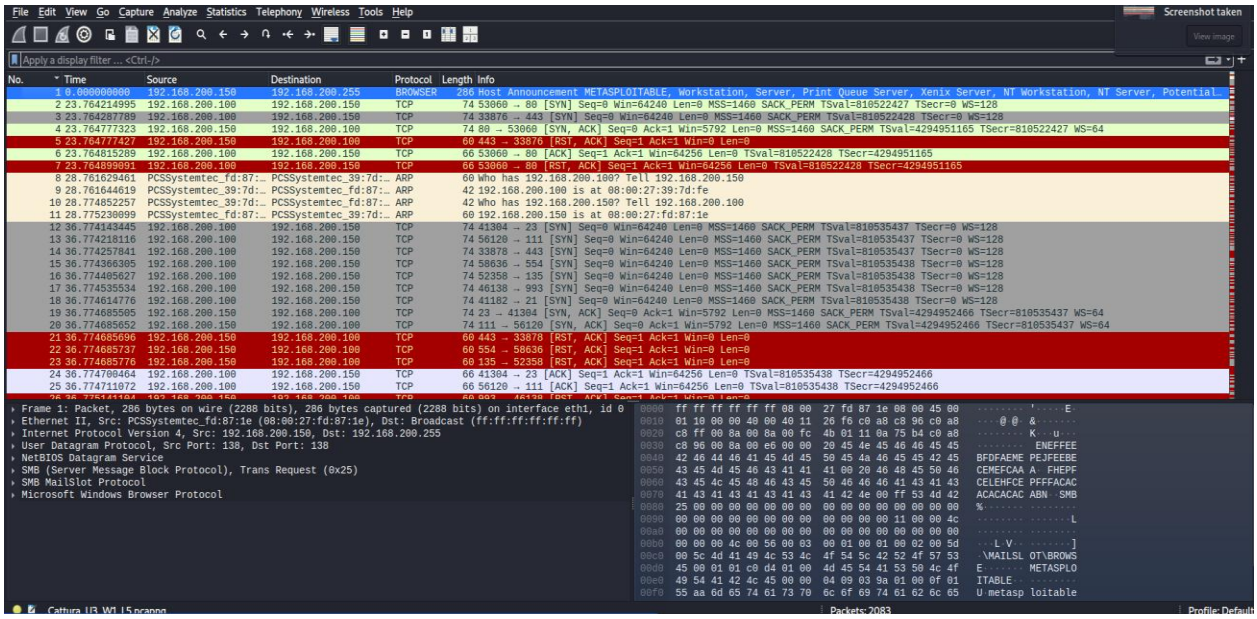
L'esercizio si svolgerà all'interno della **Macchina Virtuale Kali Linux**.

Tratta l'analisi della cattura di rete attraverso lo strumento **Wireshark**, analizzatore di protocollo di rete (**packet analyzer**) open-source, usato per catturare, ispezionare e analizzare il traffico di rete in tempo reale oppure, come in questo caso, da file registrati.

Sarà analizzata la cattura di rete (sezione Esecuzione Fase 1 e 2) eventuali **IOC (Indicators of Compromise**), (sezione Analisi degli IOC), evidenze che indicano che un sistema, una rete o un'organizzazione potrebbero essere stati compromessi da un attacco informatico.

Saranno fatte ipotesi su potenziali vettori di attacco (sezione Potenziali Vettori di Attacco) e consigliate azioni per ridurre gli impatti dell'attacco attuale e futuri (sezione Consigli di Sicurezza Immediati e Consigli di Sicurezza Futuri)

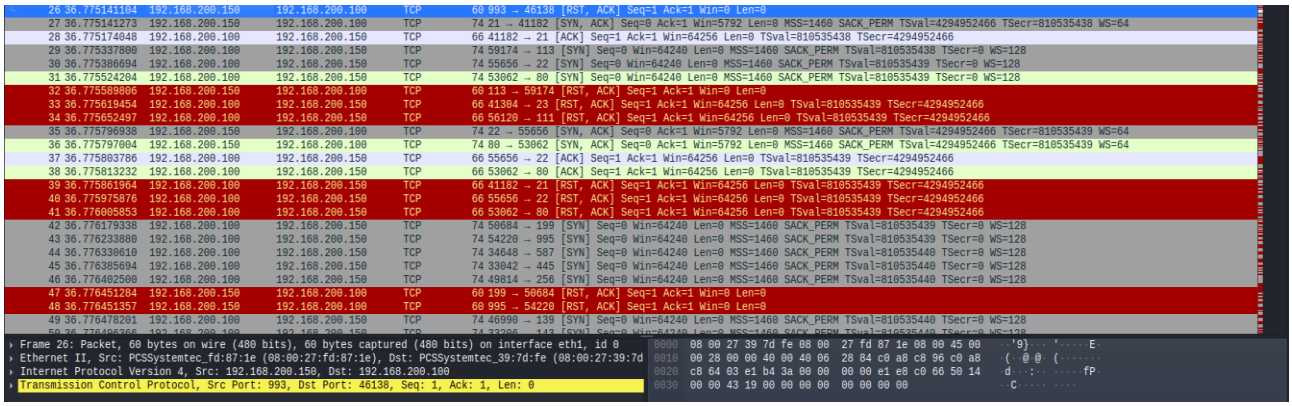
ESECUZIONE: Parte 1



Il seguente Screenshot vede alla riga **No.1** l'IP **192.168.200.150** annunciarsi come host macchina **Metasploitable** (Protocollo Browser). Questo dettaglio indica un **IOC** (Indicatore di Compromissione), poiché viene indicata la presenza di una macchina nota per la sua vulnerabilità

- Le righe **No. 2-3** vedono l'**attaccante** con Ip **192.168.200.100** tentare di aprire una connessione **SYN** (Synchronize) attraverso le porte **80** e **443**, protocolli **http** e **https**, viene indicato il protocollo (Protocol) **TCP** utile al funzionamento della connessione.
  Il tentativo ha avuto successo.
- Righe **No.2-4** vede completato il "**Three-way Handshake**" (**SYN, SYN/ACK, ACK**). La connessione è stabilita.
- Righe **No.5** e **7** vedono il reset della sessione (si nota un pacchetto [**RST, ACK**] nella riga 7), suggerendo un controllo del servizio.
- Righe **No.8** a **No.11** vedono il **Protocollo ARP**.
  Gli host si scambiano richieste **ARP** ("Who 192.168.200.100") per mappare gli indirizzi IP ai rispettivi indirizzi MAC fisici.
- Da riga **No.12** a Riga **No.20** vede **l'ip 192.168.200.100 attaccante** (Source) effettuare una **scansione delle porte 23,11,443,554,135,993,21** sull'**ip 192.168.200.150** vittima (Destination) e la **risposta**, righe **No.19-20**, dell'ip della vittima che indica le **porte 23 e 111 aperte**.
- Da riga **No.21 a No.23** vede il rifiuto dell'**ip** della **vittima 192.168.200.150** di **permettere la connessione** tramite **porte 443,554,135 (RST, ACK)**
- Righe **No.24 e 25** si aprono le **connessioni 23 (telnet) e 111(RCP)**

ESECUZIONE: Parte 2



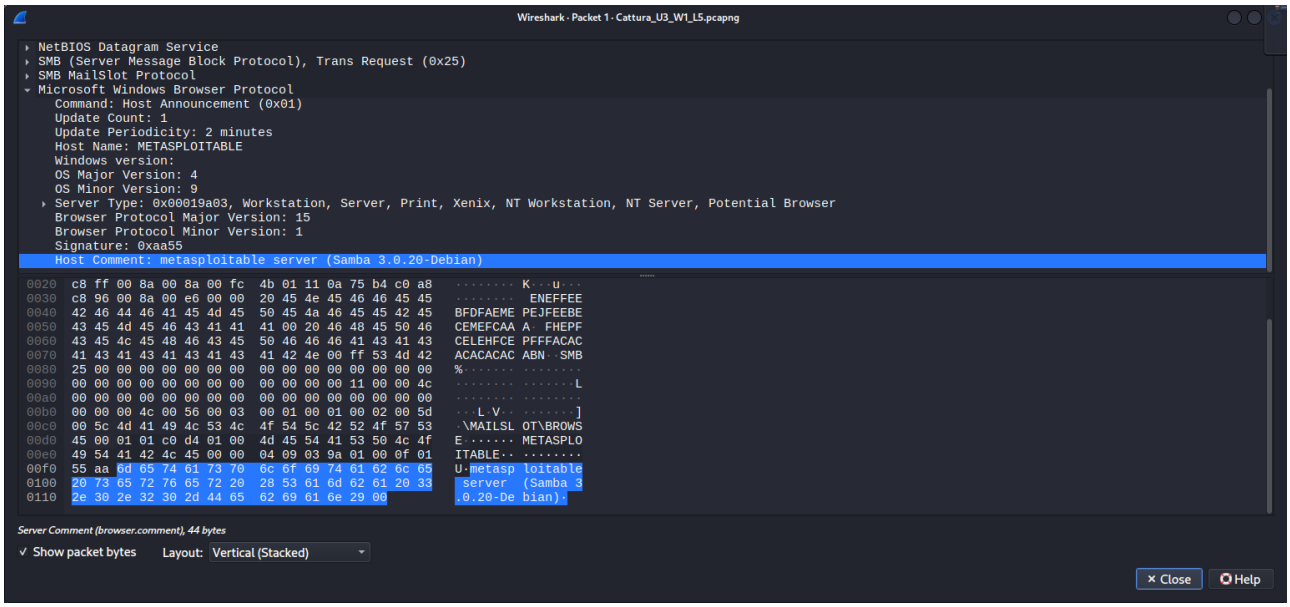
- Riga **No.26** viene chiusa la **porta 993** dall'ip **192.168.200.150** della vittima
- Righe **No.27-28** viene effettuato l'handshake per la **porta 21 (FTP),SYN e ACK**, la **porta 21** è aperta.
- Righe **No.29** a **No.31** si effettua una scansione delle **porte 113,22,80** da parte dell'attaccante
- Righe **No.32** a **No.34** la vittima rifiuta la connessione alla **porta 113**. L'attaccante chiude le **porte 23 e 111 (RST)**
- Righe da **No.35** a **No.38** viene completato l'**handshake** per le **porte 22 e 80**
- Righe No.**39 a No.41** l'**attaccante** chiude le connessioni sulle **porte 21,22,80**
- Righe No.**42 a No.46** scansione **delle porte 199,995,587,445,256** da parte dell'**attaccante**
- Righe **No.47,48** la **vittima** rifiuta la connessione sulle **porte 199 e 995**

La cattura di rete mostrata si comporta nello stesso modo fino alla riga No.2083

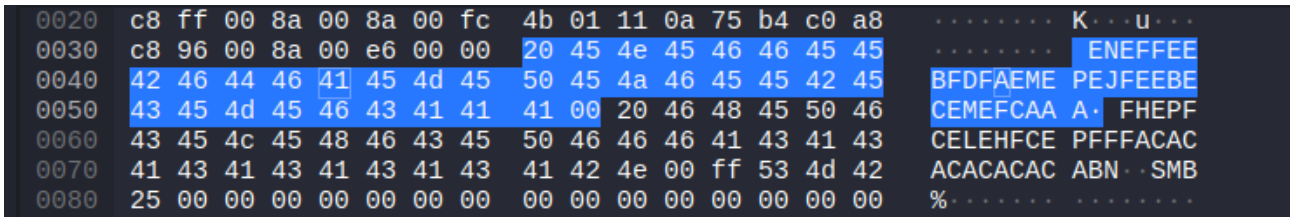
ANALISI DEGLI IOC (Indicators of Compromise)

L'analisi della cattura di rete mostra i segnali di un attacco in corso.

Viene effettuata una scansione aggressiva delle porte da parte di un attaccante **ip 192.168.200.100** con l'identificazione iniziale della **vittima** indicata nella riga **No.1**, la **Metasploitable** con **ip 192.168.200.150**, macchina vulnerabile utilizzata per scopi didattici e penetration test. Viene inoltre rilevato il banner del **server Samba 3.0.20-Debian**



Si riscontrano stringhe di caratteri offuscati e/o codificati, che suggeriscono un tentativo di **buffer overflow** o l'iniezione di **shellcode.**



L'apertura riuscita di sessioni su porte come la **23 (Telnet)** e la **21 (FTP)** (righe da **No.24 a 28**) rappresentano un evidente indicatore di compromissione.
I Pacchetti (**RST, ACK**) indicano inoltre che lo scanner chiude le connessioni una volta scoperte.

La seguente cattura di rete, con altissima probabilità, mostra lo strumento **NMAP** o un modulo scanner dello strumento **Metasploit,** il tutto avviene in pochissimi secondi.

POTENZIALI VETTORI DI ATTACCO

Vengono elencati i potenziali vettori di attacco:

- **BRUTE FORCE**: Attacco a forza bruta sulla vittima, **porte 21 (FTP), 22 (SSH) e 23 (Telnet)**
- **EXPLOITATION DI SERVIZI:** La **porta 111 (RPCBind)** e la **porta 80 (HTTP)** sulla macchina **Metasploitable** sono vettori noti per l'esecuzione di **codice remoto (RCE**) tramite vulnerabilità software non patchate.
- **MAN IN THE MIDLLE (MITM):** Poiché **Telnet** e **FTP** non sono cifrati, un attaccante posizionato sulla stessa sottorete (come suggerisce l'attività **ARP** nelle righe **No.8 a 11**) potrebbe intercettare le credenziali durante il transito.

CONSIGLI DI SICUREZZA IMMEDIATI

I **Consigli di Sicurezza** in caso di un attacco che si sta svolgendo in questo momento sono i seguenti:

- **Isolamento dell'Host:** Disconnettere immediatamente la macchina **192.168.200.150** dalla rete per impedire l'esfiltrazione di dati o il movimento laterale dell'attaccante.

- **Blocco IP Sorgente:** Configurare un **Firewall** per bloccare tutto il traffico proveniente dall'host **192.168.200.100**, macchina attaccante.

- **Chiusura Porte Critiche:** Disabilitare immediatamente **i servizi Telnet porta 23 e FTP porta 21** se non strettamente necessari per il debugging isolato.

CONSIGLI DI SICUREZZA FUTURI

I Consigli di Sicurezza per prevenire questi tipi di attacchi in futuro sono i seguenti:

- **Implementazione di un IDS/IPS:** Installare sistemi di rilevamento intrusioni per identificare e bloccare automaticamente gli scanner di porte.
- **Hardening del Sistema:** Sostituire protocolli obsoleti con alternative sicure (es. **SSH** invece di **Telnet, SFTP** invece di **FTP**) e applicare regolarmente le patch di sicurezza.
- **Utilizzo Rete Locale:** Utilizzare la macchina Metasploitable in Rete Locale.
- **Utilizzo e Configurazione di un Firewall:** Utilizzare e configurare il **Firewall** affinché blocchi tutto il traffico in entrata di default, attraverso le regole, permettendo solo le connessioni verso servizi strettamente necessari.
- **Segmentazione della Rete:** Isolare la macchina di test dal resto della rete attraverso una segmentazione della rete, ad esempio sugli Switch limitare il numero di indirizzi **MAC** che possono connettersi a una singola porta fisica