

# 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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53868 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818522427 TSecr=0 WS=128
3	23.764277709	192.168.200.100	192.168.200.150	TCP	74	53876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53868 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=818522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 53876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53868 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=818522428 TSecr=4294951165
7	23.765099091	192.168.200.100	192.168.200.150	TCP	60	53868 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	23.761623461	PCSSystemtec.fid:87...	PCSSystemtec.39:7d...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	23.761644619	PCSSystemtec.fid:87...	PCSSystemtec.fid:87...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	23.774852257	PCSSystemtec.39:7d...	PCSSystemtec.fid:87...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	23.775230899	PCSSystemtec.fid:87...	PCSSystemtec.39:7d...	ARP	60	192.168.200.150 is at 08:00:27:7d:87:1e
12	36.774183445	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56128 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	53878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535437 TSecr=0 WS=128
15	36.774366395	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535438 TSecr=0 WS=128
16	36.774485027	192.168.200.100	192.168.200.150	TCP	74	52356 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818535438 TSecr=0 WS=128
19	36.77465565	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=818535437 WS=64
20	36.77465652	192.168.200.150	192.168.200.100	TCP	74	111 → 56128 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=818535437 WS=64
21	36.77465696	192.168.200.150	192.168.200.100	TCP	60	443 → 53878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.77465737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.77465776	192.168.200.150	192.168.200.100	TCP	60	135 → 52356 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774740804	192.168.200.100	192.168.200.150	TCP	60	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=818535438 TSecr=4294952466
25	36.774741192	192.168.200.100	192.168.200.150	TCP	66	56128 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=818535438 TSecr=4294952466

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 (Protocollo) **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

26	36	775141184	192.168.200.150	192.168.200.100	TCP	60	993	-	46138	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0	
27	36	775141273	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
28	36	775174948	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
29	36	775337880	192.168.200.100	192.168.200.150	TCP	74	59174	-	113	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128	
30	36	775386694	192.168.200.100	192.168.200.150	TCP	74	55656	-	22	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128	
31	36	775524204	192.168.200.100	192.168.200.150	TCP	74	53062	-	80	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128	
32	36	775589896	192.168.200.150	192.168.200.100	TCP	60	113	-	59174	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0	
33	36	775619454	192.168.200.150	192.168.200.100	TCP	66	41384	-	23	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	TSval=810535438 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=810535438 TSecr=4294952466
35	36	775796938	192.168.200.150	192.168.200.100	TCP	74	22	-	55656	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
36	36	775797904	192.168.200.150	192.168.200.100	TCP	74	80	-	53062	[SYN, ACK]	Seq=0	Ack=1	Win=5792	Len=0	MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
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=810535438 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=810535438 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=810535438 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=810535438 TSecr=4294952466
41	36	776059583	192.168.200.100	192.168.200.150	TCP	66	53062	-	80	[RST, ACK]	Seq=1	Ack=1	Win=64256	Len=0	TSval=810535438 TSecr=4294952466
42	36	776179338	192.168.200.100	192.168.200.150	TCP	74	50684	-	199	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128	
43	36	776233880	192.168.200.100	192.168.200.150	TCP	74	54228	-	995	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128	
44	36	776338610	192.168.200.100	192.168.200.150	TCP	74	34648	-	587	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128	
45	36	776385694	192.168.200.100	192.168.200.150	TCP	74	33942	-	445	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128	
46	36	776492588	192.168.200.100	192.168.200.150	TCP	74	49814	-	250	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128	
47	36	776451284	192.168.200.150	192.168.200.100	TCP	60	199	-	58684	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0	
48	36	776451357	192.168.200.150	192.168.200.100	TCP	60	995	-	54228	[RST, ACK]	Seq=1	Ack=1	Win=0	Len=0	
49	36	776478201	192.168.200.100	192.168.200.150	TCP	74	46990	-	139	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128	
50	36	776498366	192.168.200.100	192.168.200.150	TCP	74	33942	-	143	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128	

Frame 26: Packet, 66 bytes on wire (480 bits), 66 bytes captured (480 bits) on interface eth1, id 0  
Ethernet II, Src: PCSystemtec-fd:87:1e (08:00:27:fd:87:1e), Dst: PCSystemtec-39:7d:fe (08:00:27:39:7d)  
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100  
Transmission Control Protocol, Src Port: 993, Dst Port: 46138, Seq: 1, Ack: 1, Len: 0

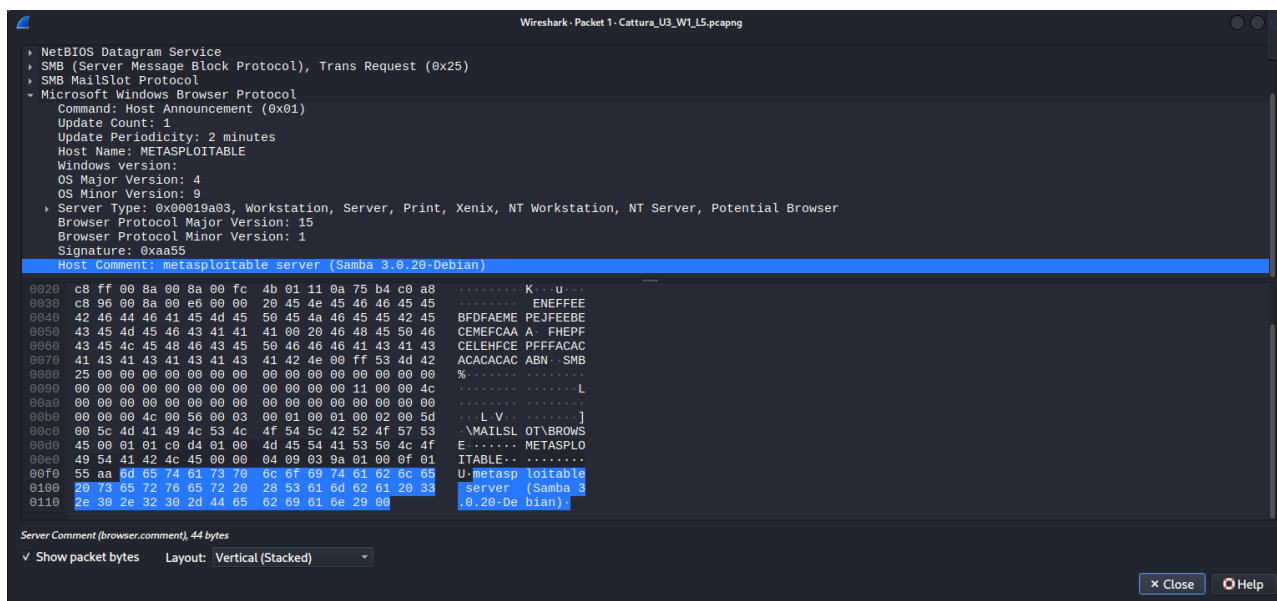
- Riga **No.26** viene chiusa la **porta 993** dall'ip **192.168.200.150** della vittima
- Righe **No.27-28** viene effettuato l'handshake per la **porta 21** (FTP),SYN e **ACK**, la **porta 21** è aperta.
- Righe **No.29** a **No.31** si effettua una scansione delle **porte 113,22,80** da parte dell'attaccante
- 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**

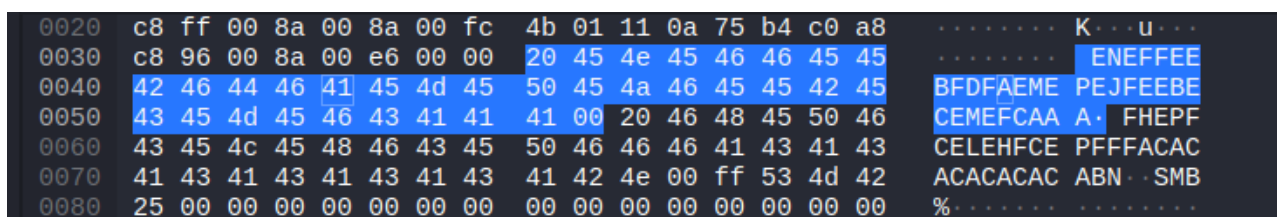
## ANALISI DEGLI IOC (Indicators of Compromise)

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 MIDDLE (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.

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