

# 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

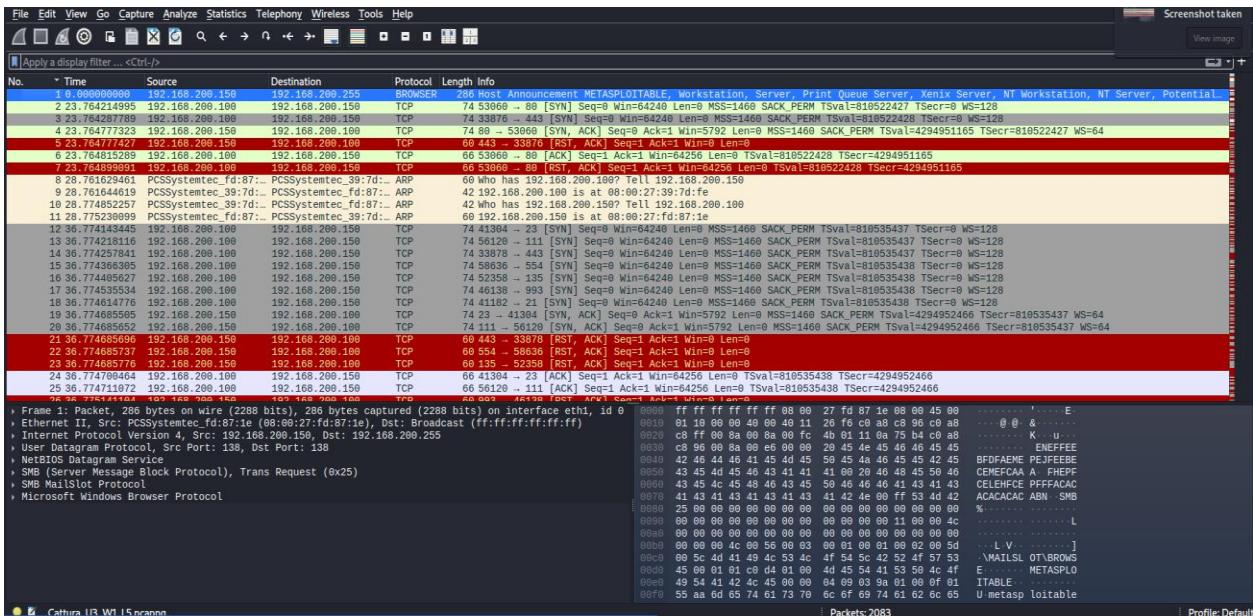
L’esercizio si svolgerà all’interno della **Macchina Virtuale Kali Linux**.

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

26 36 . /5141104 192.168.200.150	192.168.200.150	172.168.200.100	TCP	69 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
27 36 . 775141273 192.168.200.150	192.168.200.100	74 21 - 41182 [SYN, ACK] Seq=9 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=64	TCP	74 21 - 41182 [SYN, ACK] Seq=9 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=64	
28 36 . 775174948 192.168.200.150	192.168.200.100	66 41182 - 21 [ACK] Seq=10 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=128	TCP	66 41182 - 21 [ACK] Seq=10 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=128	
29 36 . 775337808 192.168.200.150	192.168.200.100	74 59174 - 113 [SYN] Seq=8 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=128	TCP	74 59174 - 113 [SYN] Seq=8 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=128	
30 36 . 775386694 192.168.200.150	192.168.200.100	74 55656 - 80 [SYN] Seq=9 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=128	TCP	74 55656 - 80 [SYN] Seq=9 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=128	
31 36 . 775524294 192.168.200.150	192.168.200.100	74 53962 - 80 [SYN] Seq=9 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=128	TCP	74 53962 - 80 [SYN] Seq=9 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=810535438 WS=128	
32 36 . 77558896 192.168.200.150	192.168.200.100	69 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	TCP	69 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
33 36 . 775619454 192.168.200.150	192.168.200.100	66 41394 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	TCP	66 41394 - 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
34 36 . 775652497 192.168.200.150	192.168.200.100	66 56128 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	TCP	66 56128 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
35 36 . 775796932 192.168.200.150	192.168.200.100	74 22 - 55656 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=64	TCP	74 22 - 55656 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=64	
36 36 . 77579700 192.168.200.150	192.168.200.100	74 80 - 53962 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=64	TCP	74 80 - 53962 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=64	
37 36 . 77583786 192.168.200.150	192.168.200.100	66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	TCP	66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
38 36 . 775813232 192.168.200.150	192.168.200.100	66 53962 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	TCP	66 53962 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
39 36 . 775861964 192.168.200.100	192.168.200.150	66 41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	TCP	66 41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
40 36 . 775975876 192.168.200.100	192.168.200.150	66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	TCP	66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
41 36 . 776095853 192.168.200.100	192.168.200.150	66 53962 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	TCP	66 53962 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810535439 Tscr=4294952466	
42 36 . 776179338 192.168.200.100	192.168.200.150	74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=128	TCP	74 50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=128	
43 36 . 776233886 192.168.200.100	192.168.200.150	74 54228 - 994 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=128	TCP	74 54228 - 994 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=128	
44 36 . 776338616 192.168.200.100	192.168.200.150	74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=128	TCP	74 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=810535439 WS=128	
45 36 . 776385694 192.168.200.100	192.168.200.150	74 33942 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tscr=810535440 WS=128	TCP	74 33942 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tscr=810535440 WS=128	
46 36 . 776402596 192.168.200.100	192.168.200.150	74 49814 - 250 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tscr=810535440 WS=128	TCP	74 49814 - 250 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tscr=810535440 WS=128	
47 36 . 776451284 192.168.200.150	192.168.200.100	69 199 - 56684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	TCP	69 199 - 56684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
48 36 . 776451357 192.168.200.150	192.168.200.100	68 995 - 54228 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	TCP	68 995 - 54228 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
49 36 . 776478208 192.168.200.150	192.168.200.100	74 40869 - 142 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tscr=810535440 WS=128	TCP	74 40869 - 142 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tscr=810535440 WS=128	
50 36 . 776513166 192.168.200.150	192.168.200.100	74 40906 - 142 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tscr=810535440 WS=128	TCP	74 40906 - 142 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535440 Tscr=810535440 WS=128	
Frame 26: Packet, 69 bytes on wire (480 bits), 69 bytes captured (480 bits) on interface eth1, id 0					
Ethernet II, Src: PCSystemTec_fd:87:1e (08:00:27:87:1e), 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: 6					

- 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**

Wireshark - Packet 1 - Cattura\_U3\_W1\_L5.pcapng

```

> NetBIOS Datagram Service
> SMB (Server Message Block Protocol), Trans Request (0x25)
> SMB Mailslot Protocol
- Microsoft Windows Browser Protocol
  Command: Host Announcement (0x01)
  Update Count: 1
  Update Periodicity: 2 minutes
  Host Name: METASPOITABLE
  Windows version:
  OS Major Version: 4
  OS Minor Version: 9
> Server Type: 0x00019a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser
  Browser Protocol Major Version: 15
  Browser Protocol Minor Version: 1
  Signature: 0xaas5
  Host Comment: metasploitable server (Samba 3.0.20-Debian)

0020 c8 ff 00 8a 00 8a 00 fc 4b 01 11 0a 75 b4 c0 a8 .....K...u...
0030 c8 96 00 8a 00 e6 00 00 20 45 4e 45 46 46 45 45 .....ENEFFEE
0040 42 46 44 46 41 45 4d 45 50 45 4a 46 45 45 42 45 BFDFAEAE PEJFEEBE
0050 43 45 4d 45 46 43 41 41 41 00 20 46 48 45 50 46 CEMEFCAA A..FHEPF
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43 CELEHFCE PFFFACAC
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 4d 42 ACACACAC ABN..SMB
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 %.....
0090 00 00 00 00 00 00 00 00 00 00 00 11 00 00 4c .....L...
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....[...]
00b0 00 00 4c 00 56 00 03 00 01 00 01 00 02 00 5d ..L V.....]
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53 \MAILSL OT\BROWS
00d0 45 00 01 01 c0 d4 01 00 4d 45 54 41 53 50 4c 4f E.....METASPL0
00e0 49 54 41 42 4c 45 00 00 04 09 03 9a 01 00 0f 01 ITABLE:.....
00f0 55 aa 6d 65 74 61 73 78 6c 6f 69 74 61 62 6c 65 U:metasploit
0100 20 73 65 72 76 95 72 28 28 53 61 6d 62 61 20 33 server (Samba 3
0110 2e 30 2e 32 30 2d 44 65 62 69 61 6e 29 00 ,0.20-De bian);
```

Server Comment (browser.comment), 44 bytes

Show packet bytes Layout: Vertical (Stacked)

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

0020	c8 ff 00 8a 00 8a 00 fc	4b 01 11 0a 75 b4 c0 a8	.....K...u...
0030	c8 96 00 8a 00 e6 00 00	20 45 4e 45 46 46 45 45	.....ENEFFEE
0040	42 46 44 46 41 45 4d 45	50 45 4a 46 45 45 42 45	BFDFAEAE PEJFEEBE
0050	43 45 4d 45 46 43 41 41	41 00 20 46 48 45 50 46	CEMEFCAA A..FHEPF
0060	43 45 4c 45 48 46 43 45	50 46 46 46 41 43 41 43	CELEHFCE PFFFACAC
0070	41 43 41 43 41 43 41 43	41 42 4e 00 ff 53 4d 42	ACACACAC ABN..SMB
0080	25 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	%.....

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.

## 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