Threat Intelligence & IOC Report

Analisi di una cattura di rete e identificazione di Indicatori di Compromissione (IOC)

Ardelean Pop Catalin
Master in Cyber Security Specialist – Epicode

6 febbraio 2026

Indice

1 Traccia dell'esercizio

Durante la lezione teorica sono stati introdotti i concetti di **Threat Intelligence** e di **Indicatori di Compromissione (IOC)**. Gli IOC rappresentano evidenze osservabili di un attacco in corso o già avvenuto.

Lo studente ha ricevuto una cattura di traffico di rete (file `.pcap`) da analizzare con Wireshark con i seguenti obiettivi:

- Identificare e analizzare eventuali IOC.
- Formulare ipotesi sui possibili vettori di attacco.
- Proporre azioni di mitigazione per ridurre l'impatto dell'attacco attuale e prevenire attacchi simili in futuro.

2 Scenario di laboratorio

La cattura analizzata riguarda una rete locale privata in cui sono presenti due host principali:

- **192.168.200.100** – macchina attaccante/scanner.
- **192.168.200.150** – macchina vittima, identificata come **Metasploitable**.

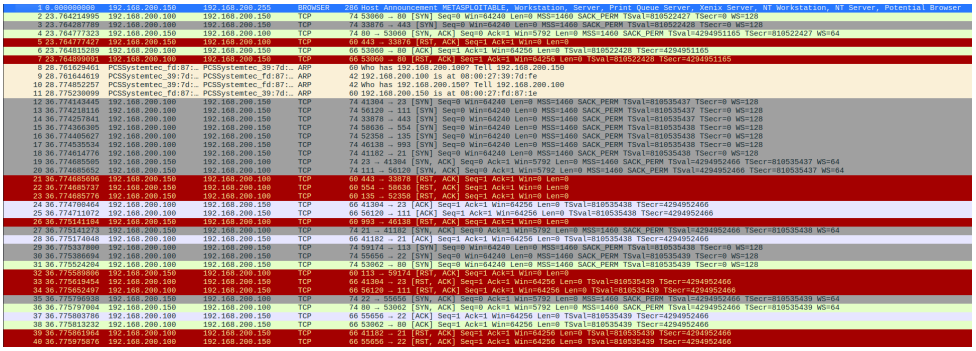

Figura 1: Frame iniziale della cattura Wireshark

Dal primo frame della cattura emerge infatti un messaggio di broadcast di tipo:

`BROWSER Host Announcement METASPLOITABLE`

Questo indica chiaramente che l'host bersaglio è una macchina vulnerabile.

3 Analisi generale del traffico

L'analisi della cattura è stata effettuata tramite Wireshark, osservando in particolare i pattern TCP tra i due host.

Sono state riscontrate le seguenti caratteristiche principali:

- Traffico fortemente unidirezionale: quasi tutti i pacchetti partono da **192.168.200.100**.
- Risposte sistematiche da parte di **192.168.200.150**.
- Assenza di traffico applicativo (HTTP, DNS, FTP, ecc.) significativo.
- Presenza massiva di pacchetti TCP SYN seguiti da RST o SYN/ACK.

Questi elementi indicano in modo inequivocabile un'attività di **ricognizione attiva tramite port scanning**.

4 Identificazione di attaccante e vittima

4.1 Attaccante

IP: 192.168.200.100

Evidenze:

- Invia sistematicamente pacchetti TCP SYN verso molte porte diverse.
- Utilizza porte sorgente effimere casuali (ad esempio 53060, 33876, 41304, 56120, ecc.).
- Non stabilisce mai sessioni TCP complete.

Ruolo assegnato: **Scanner / Prober**.

4.2 Vittima

IP: 192.168.200.150 (Metasploitable)

Evidenze:

- Riceve tutti i tentativi di connessione.
- Risponde con:
  - **SYN/ACK** su porte aperte.
  - **RST,ACK** su porte chiuse o filtrate.

Ruolo assegnato: **Target della scansione**.

5 Tipo di scansione rilevata

L'analisi dei pattern TCP mostra che si tratta di una:

TCP SYN Scan (Stealth Scan)

Il comportamento osservato è:

```
Attaccante -> Vittima  [SYN]
Vittima -> Attaccante  [SYN,ACK]   (porta aperta)
Attaccante -> Vittima  [RST,ACK]   (chiusura immediata)
```

Oppure:

```
Attaccante -> Vittima  [SYN]
Vittima -> Attaccante  [RST,ACK]   (porta chiusa)
```

Questo comportamento è compatibile con l'uso di strumenti come:

```
nmap -sS -p- 192.168.200.150
```

ovvero una scansione completa di tutte le porte TCP.

6 Porte scansionate

Dalla cattura emerge che l'attaccante ha testato centinaia di porte TCP, tra cui:

80, 21, 22, 23, 25, 53, 111, 139, 445, 512, 514, e molte altre porte.

Questo indica una **full port scan**, non una scansione mirata a pochi servizi.

7 Porte aperte su Metasploitable

Dall'analisi delle risposte SYN/ACK, risultano **aperte** le seguenti porte chiave:

Porta	Servizio tipico	Stato
21	FTP	Aperta
22	SSH	Aperta
23	Telnet	Aperta (critica)
25	SMTP	Aperta
53	DNS	Aperta
80	HTTP	Aperta
111	RPCbind	Aperta
139	NetBIOS	Aperta
445	SMB	Aperta
512	Rexec/Rlogin	Aperta
514	Syslog	Aperta

Queste porte sono tipiche di Metasploitable e rappresentano superfici di attacco intenzionalmente esposte.

8 IOC (Indicator of Compromise)

Gli Indicatori di Compromissione (IOC) rappresentano evidenze osservabili nel traffico di rete che suggeriscono attività potenzialmente malevole o non autorizzata. Nel caso in esame, gli IOC sono stati ricavati direttamente dall'analisi della cattura Wireshark, osservando i pattern TCP, il comportamento temporale dei pacchetti e la relazione tra l'host sorgente e quello di destinazione.

Gli IOC individuati sono suddivisi in due categorie principali:

- IOC di rete (basati su indirizzi, protocolli e pattern di comunicazione);
- IOC comportamentali (basati sul modo in cui il traffico si manifesta nel tempo).

8.1 IOC di rete

La tabella seguente riassume gli IOC di rete più rilevanti estratti dalla cattura:

Tipo IOC	**Descrizione tecnica osservata**
Attaccante	192.168.200.100. Questo host genera in modo sistematico pacchetti TCP SYN verso un ampio intervallo di porte sul target. Utilizza porte sorgente effimere casuali e non stabilisce mai sessioni TCP complete, comportamento tipico di un tool di scanning automatizzato.
Vittima	192.168.200.150, identificata nei primi frame come *METASPLOITABLE*. L'host riceve tutti i tentativi di connessione e risponde coerentemente con SYN/ACK sulle porte aperte e RST/ACK sulle porte chiuse o filtrate, fornendo feedback chiaro allo scanner.
Tecnica	TCP SYN Scan massivo (stealth scan). Questa tecnica consente all'attaccante di mappare lo stato delle porte senza completare il three-way handshake, riducendo la probabilità di essere rilevato da log applicativi tradizionali.
Pattern di comunicazione	SYN → SYN/ACK → RST sulle porte aperte; SYN → RST/ACK sulle porte chiuse. Questo pattern è fortemente indicativo di scanning attivo e non compatibile con traffico applicativo legittimo.
Ritmo del traffico	Altamente regolare e meccanico, con intervalli temporali quasi costanti tra i pacchetti. L'assenza di variazioni temporali casuali suggerisce l'uso di un tool automatizzato (ad esempio Nmap o Masscan).
Obiettivo dell'attività	Enumerazione sistematica dei servizi esposti su 192.168.200.150, con l'intento di identificare superfici di attacco sfruttabili in una fase successiva.

8.1.1 Interpretazione operativa degli IOC di rete

Dalla combinazione degli IOC di rete emerge chiaramente che:

- L'attività non è casuale né accidentale, ma pianificata e intenzionale.
- Non si tratta di errore di configurazione o traffico malformato, bensì di ricognizione attiva.

- Il comportamento è coerente con la fase di **Reconnaissance** della Cyber Kill Chain.
- L'attaccante sta costruendo una mappa dei servizi disponibili prima di tentare eventuali exploit.

8.2 IOC comportamentali

Oltre agli IOC strettamente tecnici, sono stati identificati indicatori basati sul comportamento del traffico nel tempo:

- **Connessioni brevissime e ripetute**: Ogni tentativo di connessione dura pochi millisecondi e viene immediatamente chiuso dall'attaccante con RST, caratteristica tipica di scanning stealth.
- **Assenza di traffico applicativo reale**: Non si osservano richieste HTTP, scambi DNS, trasferimenti FTP o altre interazioni applicative. Questo conferma che lo scopo non è comunicare con i servizi, ma solo verificarne lo stato.
- **Pattern meccanico e sistematico**: Le porte vengono testate in sequenza o secondo schemi regolari, incompatibili con traffico umano o applicativo legittimo.
- **Alta velocità di scansione**: Il numero di pacchetti al secondo è elevato e costante, indicando l'uso di un tool automatizzato e non di interazione manuale.
- **Copertura estesa delle porte**: Lo scanner non si limita a porte comuni (80/443), ma testa un ampio intervallo di porte TCP, suggerendo un intento di mappatura completa del target.
- **Feedback immediato dal target**: La macchina vittima risponde in modo coerente, permettendo allo scanner di costruire rapidamente una lista di porte aperte e chiuse.

9 Ipotesi sul vettore di attacco

Sulla base degli IOC, si formula la seguente ipotesi:

9.1 Ricognizione pre-attacco

L'attaccante sta effettuando la fase di **Reconnaissance** della Cyber Kill Chain, con l'obiettivo di:

- Identificare porte aperte.
- Enumerare servizi vulnerabili.
- Preparare exploit mirati in una fase successiva.

10 Rischi evidenziati

L'analisi della scansione e dello stato dei servizi esposti su **192.168.200.150 (Metasploitable)** evidenzia una superficie d'attacco ampia e critica, coerente con un sistema scarsamente hardenizzato e fortemente esposto in rete. Questa configurazione rende l'host particolarmente vulnerabile a tentativi di intrusione, movimento laterale e compromissione completa del sistema.

10.1 Rischi legati ai servizi esposti

- **HTTP (80/TCP) esposto**: La presenza di un server web accessibile rappresenta un rischio significativo perché:
  - può ospitare applicazioni vulnerabili o configurate in modo insicuro;
  - espone potenzialmente vulnerabilità applicative comuni come:
    - SQL Injection,
    - Cross-Site Scripting (XSS),
    - File Inclusion,
    - Directory Traversal,
    - errori di configurazione del web server.
  - costituisce un punto di ingresso per:
    - enumerazione di servizi interni,
    - upload di file malevoli,
    - esecuzione di codice remoto tramite exploit applicativi.

  Un servizio HTTP esposto senza adeguate protezioni è tipicamente uno dei primi vettori di attacco sfruttati durante una compromissione.

- **Telnet (23) esposto**: Telnet trasmette le credenziali in chiaro e non fornisce alcuna cifratura. Ciò consente a un attaccante di:
  - intercettare password tramite sniffing di rete,
  - effettuare brute force automatizzati,
  - ottenere controllo remoto del sistema con credenziali deboli.

- **FTP (21) aperto**: FTP rappresenta un rischio elevato perché:
  - non cifra il traffico;
  - potrebbe consentire accesso anonimo;
  - potrebbe essere sfruttato per caricare malware;

  - potrebbe permettere esfiltrazione di file sensibili.

- **SMB (445) e NetBIOS (139) esposti**: Questi servizi sono associati a vulnerabilità critiche sfruttate in attacchi reali (es. EternalBlue). La loro esposizione aumenta il rischio di:
  - ransomware,
  - movimento laterale all'interno della rete,
  - enumerazione di utenti e share.
- **RPCbind (111) esposto**: RPC può essere utilizzato per mappare servizi remoti attivi, facilitando attacchi mirati.
- **Servizi legacy (512/514)**: La presenza di servizi obsoleti indica una configurazione debole e assenza di hardening, aumentando la probabilità di compromissione.

10.2 Rischio complessivo

Considerando:

- la scansione TCP SYN massiva,
- l'esposizione di HTTP (80),
- la presenza di Telnet, FTP e SMB,

il livello di rischio complessivo è classificato come:

Rischio ALTO

Motivazione:

- La scansione indica una fase di ricognizione preparatoria a un possibile attacco.
- L'insieme dei servizi esposti offre molteplici punti di ingresso.
- La configurazione del sistema non è conforme alle best practice di sicurezza.

11 Azioni di mitigazione consigliate

11.1 Risposta immediata (Incident Response)

In caso di rilevazione di una scansione simile a quella osservata, il SOC dovrebbe:

- **Bloccare l'IP 192.168.200.100 sul firewall**.

- **Isolare 192.168.200.150 in VLAN separata**.
- **Attivare IDS/IPS (Snort o Suricata)** con regole per:
  - scansioni SYN massicce,
  - pattern SYN → SYN/ACK → RST,
  - tentativi ripetuti su più porte.
- **Monitorare il traffico HTTP (porta 80)** per rilevare:
  - tentativi di exploit web,
  - directory brute force,
  - file upload sospetti.

11.2 Prevenzione futura

- **Chiudere porte non necessarie**.
- **Disabilitare Telnet e usare solo SSH (22)**.
- **Proteggere HTTP (80) con:**
  - Web Application Firewall (WAF),
  - HTTPS (443) al posto di HTTP,
  - patching del server web.
- **Limitare SMB e RPC tramite firewall**.
- **Implementare rate limiting sui pacchetti SYN**.
- **Usare VPN per accesso remoto ai servizi interni**.

12 Conclusioni

La cattura analizzata mostra chiaramente una **scansione TCP SYN massiva** da:

192.168.200.100 → 192.168.200.150 (Metasploitable).

L'attività rappresenta una fase di ricognizione pre-attacco. L'esposizione della porta **80/HTTP**, insieme agli altri servizi insicuri, amplifica il rischio complessivo poiché offre un ulteriore vettore applicativo oltre ai servizi di sistema.

L'analisi sottolinea l'importanza di:

- Monitoraggio continuo del traffico di rete,

- Rilevazione precoce degli indicatori di compromissione (IOC),
- Segmentazione della rete,
- Hardening dei servizi esposti,
- Protezione dei servizi applicativi e di rete.