

# THREAT INTELLIGENCE E IOC (INDICATOR OF COMPROMISE) CON WIRESHARK



## OBIETTIVO

L'esercizio pratico prevede un'analisi di una cattura di rete effettuata con Wireshark. In particolare si deve analizzare la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliare un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

## INDICATORI DI COMPROMISSIONE (IOC)

Gli Indicatori di Compromissione (IOC) sono evidenze che indicano la presenza di un'intrusione o di un'attività dannosa all'interno di un sistema informatico o di una rete. In altre parole, sono tracce lasciate da un attacco informatico, come malware, accessi non autorizzati o esfiltrazione di dati.

Gli IOC possono assumere diverse forme, tra cui:

- **File:** Hash di file dannosi, nomi di file sospetti, modifiche non autorizzate ai file di sistema.
- **Indirizzi IP:** Indirizzi IP di server di comando e controllo (C2), indirizzi IP associati ad attività di scansione o attacchi.
- **Nomi di dominio:** Nomi di dominio utilizzati per il phishing o per ospitare malware.
- **Chiavi di registro:** Modifiche non autorizzate al registro di sistema.
- **Anomalie di rete:** Traffico di rete anomalo, come picchi di utilizzo della banda o connessioni a indirizzi IP sconosciuti.
- **Comportamenti anomali:** attività inusuali registrate all'interno dei log di sistema.

L'analisi degli IOC è fondamentale per:

- **Rilevare intrusioni:** Identificare la presenza di un attacco in corso o già avvenuto.
- **Indagare incidenti:** Comprendere la portata e la natura di un attacco.
- **Prevenire futuri attacchi:** Utilizzare le informazioni sugli IOC per rafforzare le difese di sicurezza.

No.	Time	Source	Destination	Protocol	Length	Info
220	36.786788804	192.168.200.100	192.168.200.150	TCP	74	45154 → 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
221	36.786815129	192.168.200.100	192.168.200.150	TCP	74	45154 → 460 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
222	36.786845584	192.168.200.100	192.168.200.150	TCP	74	38180 → 239 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
223	36.786899554	192.168.200.100	192.168.200.150	TCP	74	37952 → 520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
224	36.787023989	192.168.200.150	192.168.200.100	TCP	60	545 → 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
225	36.787023195	192.168.200.150	192.168.200.100	TCP	60	480 → 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
226	36.787039359	192.168.200.100	192.168.200.150	TCP	74	43100 → 760 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
227	36.787191086	192.168.200.150	192.168.200.100	TCP	60	239 → 38180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
228	36.787191761	192.168.200.150	192.168.200.100	TCP	60	520 → 37952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
229	36.787229617	192.168.200.100	192.168.200.150	TCP	74	42460 → 480 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
230	36.787260591	192.168.200.150	192.168.200.100	TCP	60	760 → 43100 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
231	36.787346317	192.168.200.100	192.168.200.150	TCP	74	49988 → 19 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
232	36.787479654	192.168.200.100	192.168.200.150	TCP	74	44644 → 846 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
233	36.787572244	192.168.200.150	192.168.200.100	TCP	60	439 → 42460 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
234	36.787572497	192.168.200.100	192.168.200.150	TCP	60	19 → 49988 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
235	36.787596289	192.168.200.100	192.168.200.150	TCP	74	51732 → 345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
236	36.787752589	192.168.200.150	192.168.200.100	TCP	60	846 → 44644 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
237	36.787770816	192.168.200.100	192.168.200.150	TCP	74	52032 → 231 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
238	36.787864391	192.168.200.150	192.168.200.100	TCP	60	345 → 51732 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
239	36.787964675	192.168.200.100	192.168.200.150	TCP	74	59046 → 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
240	36.787983139	192.168.200.100	192.168.200.150	TCP	74	44414 → 271 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
241	36.788027913	192.168.200.100	192.168.200.150	TCP	74	59612 → 470 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
242	36.788094799	192.168.200.150	192.168.200.100	TCP	60	234 → 59932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
243	36.788117846	192.168.200.100	192.168.200.150	TCP	74	36206 → 180 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
244	36.788153092	192.168.200.100	192.168.200.150	TCP	74	51844 → 955 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
245	36.788176982	192.168.200.100	192.168.200.150	TCP	74	52724 → 232 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
246	36.788186352	192.168.200.100	192.168.200.150	TCP	74	52724 → 904 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535451 TSecr=0 WS=128
247	36.788298677	192.168.200.100	192.168.200.150	TCP	74	49480 → 835 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
248	36.788339073	192.168.200.100	192.168.200.150	TCP	74	41090 → 602 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128
249	36.788373483	192.168.200.100	192.168.200.150	TCP	74	54166 → 201 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535452 TSecr=0 WS=128

## RICERCA ED ANALISI DEGLI IOC

Dall'analisi effettuata sulla cattura abbiamo notato questi indicatori di compromissione

- **Elevato numero di pacchetti TCP con flag SYN e RST/ACK:**
  - E' un chiaro indicatore di una scansione di porte. L'attaccante sta sondando attivamente le porte del server di destinazione.
  - La combinazione di SYN e RST/ACK suggerisce una scansione di tipo "TCP connect scan" (-sT in Nmap), che completa il three-way handshake per le porte aperte, ma riceve un RST per quelle chiuse.
- **Connessioni incomplete con flag SYN:**
  - Questo potrebbe anche indicare un tentativo di "SYN flood", un attacco DoS che mira a sovraccaricare il server con richieste di connessione incomplete.
  - Tuttavia, il fatto che ci siano anche molti RST/ACK suggerisce che la scansione di porte è l'attività principale.
- **Indirizzi IP sulla stessa rete (192.168.200.xxx):**
  - Questo è un dettaglio cruciale. Implica che l'attacco potrebbe provenire da un dispositivo compromesso all'interno della rete locale, il che aumenta il rischio e richiede un'indagine interna.
  - Potrebbe trattarsi di un dipendente malintenzionato o di un altro dispositivo compromesso
- **Variazione continua delle porte di destinazione:**
  - La scansione di tutte le 65535 porte indica un tentativo di mappare l'intera gamma di servizi del server.
  - Questo è un comportamento aggressivo che mira a identificare qualsiasi potenziale vulnerabilità.
- **Chiusura rapida delle connessioni con RST:**
  - Il fatto che l'attaccante non acceda a servizi aperti conferma che l'obiettivo principale è la scansione e il rilevamento, non l'accesso diretto.

## VETTORI DI ATTACCO

- **Attacco interno:**
  - La provenienza dell'attacco dalla stessa rete solleva la preoccupazione di un attacco interno.
  - Questo potrebbe essere un dipendente malintenzionato o un dispositivo compromesso.
- **Probabile scansione di porte (Nmap -sT):**
  - La scansione TCP connect è un metodo standard per mappare i servizi in esecuzione su un server.
  - L'attaccante potrebbe essere alla ricerca di porte aperte con servizi vulnerabili.

## AZIONI DI MITIGAZIONE CONSIGLIATE

- **Modifica delle regole del firewall:**
  - Implementare regole di limitazione della delle richieste TCP
- **Isolamento Logico (Segmentazione della Rete):**
  - Inserire il dispositivo sospetto in una VLAN dedicata con regole più restrittive e permettendo l'accesso solo ai servizi necessari.
- **Installazione di Sistemi di Rilevamento delle Intrusioni (IDS/IPS):**
  - Implementare un IDS/IPS per rilevare e bloccare le scansioni di porte e altri attacchi.
  - Configurare l'IDS/IPS per generare avvisi in caso di attività sospette.
- **Verifica dei dispositivi interni:**
  - Eseguire scansioni antivirus e antimalware su tutti i dispositivi della rete locale.
  - Verificare la configurazione di sicurezza di tutti i dispositivi, inclusi i dispositivi IoT.
  - Effettuare controlli sulle credenziali degli utilizzatori, e verificare che non vi siano account compromessi.