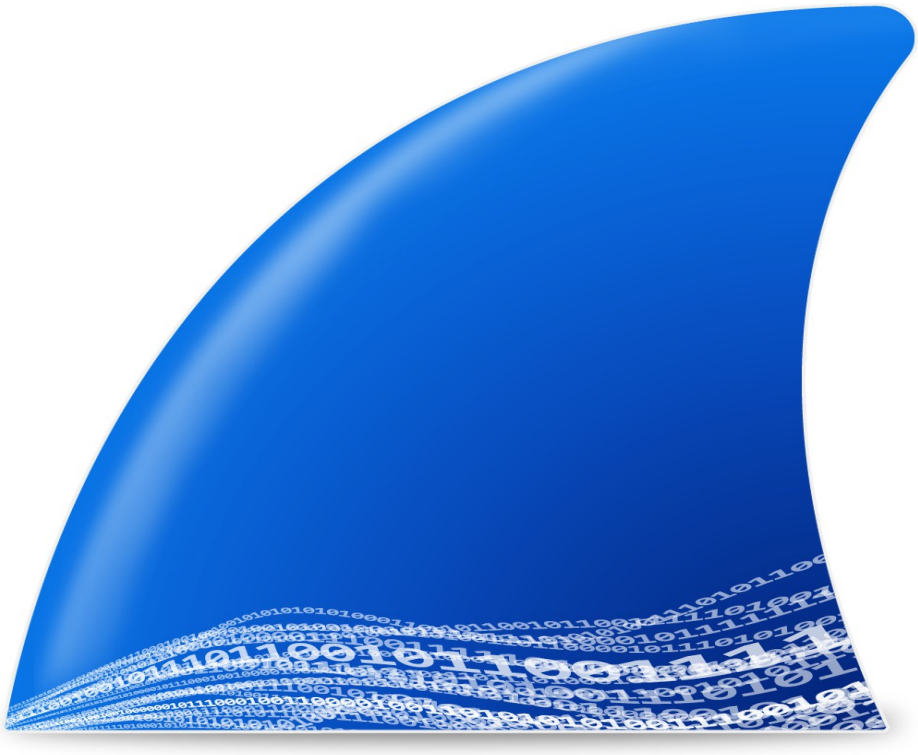
THREAT INTELLIGENCE E IOC (INDICATOR OF COMPROMISE) CON WIRESHARK



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, 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

INDICATORI DI COMPROMISSIONE (IOC)

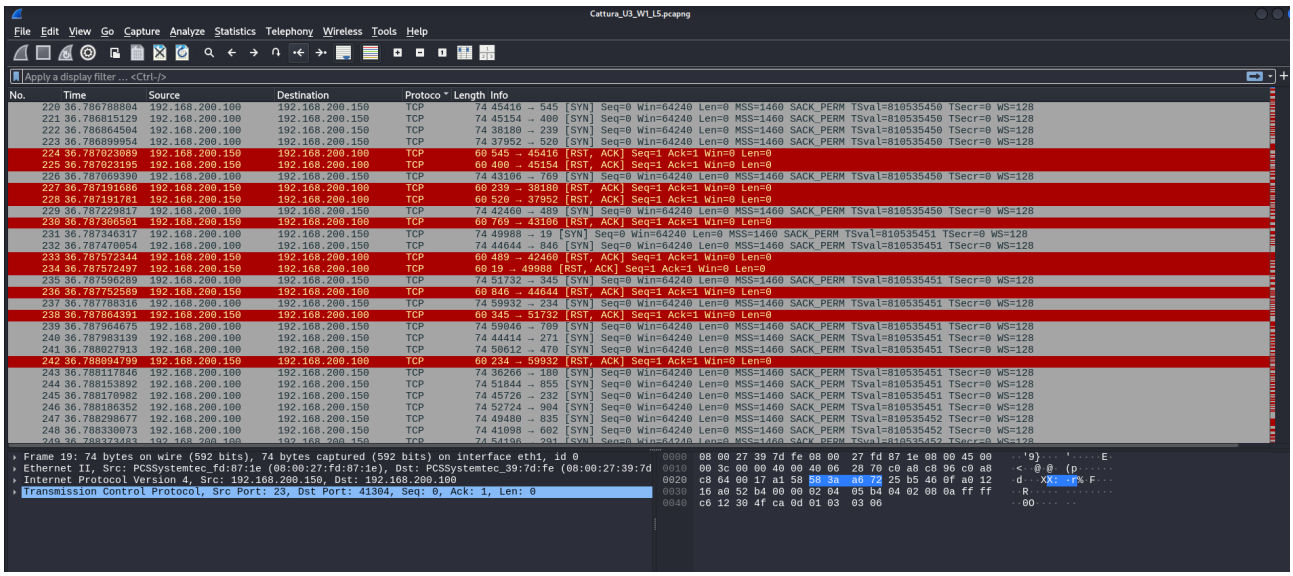
Gli Indicatori di Compromissione (IOC) sono evidenze che indicano la presenza di un'intrusione o di un'attività dannosa all'interno di un sistema informatico o di una rete. In altre parole, sono tracce lasciate da un attacco informatico, come malware, accessi non autorizzati o esfiltrazione di dati.

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.



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.