Consegna S9-L5

Consegna: Threat Intelligence e IOC

⚜️ **Tag:** #threat_intelligence #ioc #wireshark #compromissione

Traccia

Durante la lezione teorica, abbiamo visto la **Threat Intelligence** e gli **Indicatori di Compromissione (IOC)**. Gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Obiettivo

Per l'esercizio pratico, analizzare la cattura di rete allegata, effettuata con **Wireshark** (file: `Cattura_U3_W1_L3.pcapng`), e rispondere ai seguenti quesiti:

1. **Identificare e analizzare eventuali IOC**, ovvero evidenze di attacchi in corso.
2. **Ipotesi sui potenziali vettori di attacco:**
   - Quali metodi o strumenti potrebbero essere stati utilizzati dagli attaccanti?
3. **Proposte di mitigazione:**
   - Consigliare azioni per ridurre gli impatti dell'attacco attuale.
   - Proporre strategie per prevenire futuri attacchi simili.

Strumenti Utilizzati

1. **Wireshark:**
   - Analizzare il traffico di rete per identificare anomalie e segnali di compromissione.

2. **Threat Intelligence Platforms:**
    - Consultare database di indicatori noti per verificare corrispondenze con il traffico sospetto.
3. **Logs di Sistema:**
    - Collegare gli eventi di rete a potenziali attività su host interni.

Output Attesi

1. **Report di Analisi:**
    - Elenco degli IOC identificati (es. IP sospetti, nomi di dominio, firme malware).
    - Descrizione del flusso di attacco, se identificato.
2. **Mitigazioni Proposte:**
    - Configurazioni di firewall e IDS/IPS.
    - Strategie di aggiornamento e patching.
    - Misure di formazione per il personale IT.

Conclusione

L’esercizio consente di approfondire l'uso di Wireshark e la gestione di IOC nel contesto della **Threat Intelligence**. Queste competenze sono fondamentali per rilevare e mitigare gli attacchi in tempo reale, garantendo una migliore protezione dell'infrastruttura.

🔑 **Chiavi:**
[threat_intelligence, ioc, wireshark, compromissione]