Scheda 1

# **BONUS 3**

# **🔒 Report Tecnico: Isolamento di un Host Compromesso Utilizzando il Metodo 5-Tuple**

## **📌 Indice**

1. 🔹 **Introduzione**
2. 🎯 **Obiettivi del Laboratorio**
3. 🔍 **Panoramica del Metodo 5-Tuple**
4. 🛠 **Requisiti**
5. 📑 **Procedura**
   * 🛡 **Parte 1: Revisione degli Alert in Sguil**
   * 🕵️ **Parte 2: Analisi del Traffico con Wireshark**
   * 📊 **Parte 3: Investigazione con Kibana**
   * 🚧 **Parte 4: Mitigazione e Prevenzione**
6. ✅ **Conclusioni e Raccomandazioni**
7. 📖 **Glossario**
8. 🔗 **Risorse Aggiuntive**

## **🔹 1. Introduzione**

In un ambiente di rete complesso, il rilevamento tempestivo di attività sospette è fondamentale per prevenire compromissioni di dati sensibili. Questo report illustra il processo per identificare e isolare un host compromesso in una rete utilizzando il metodo 5-Tuple. L'analisi sarà condotta attraverso strumenti di sicurezza come **Security Onion**, **Sguil**, **Wireshark** e **Kibana**.

🎯 **Obiettivo principale:** Dimostrare come, attraverso la correlazione degli eventi di rete e l'analisi dei log, sia possibile identificare una minaccia, comprenderne il modus operandi e attuare misure di prevenzione efficaci.

## **🎯 2. Obiettivi del Laboratorio**

✔ Comprendere il funzionamento e l'importanza del metodo 5-Tuple nell'analisi forense di rete. ✔ Identificare un host compromesso tramite l'analisi dettagliata dei log di sicurezza. ✔ Correlare gli eventi di sicurezza utilizzando diversi strumenti di analisi. ✔ Isolare l'host compromesso per ridurre il rischio di compromissione estesa. ✔ Applicare misure preventive per evitare attacchi futuri.

## **🔍 3. Panoramica del Metodo 5-Tuple**

Il metodo **5-Tuple** è uno degli strumenti più utilizzati dagli analisti di sicurezza per identificare e tracciare il traffico di rete sospetto. Questo metodo si basa sull'analisi di cinque parametri fondamentali:

* 📌 **Indirizzo IP sorgente** 🏠
* 📌 **Porta sorgente** 🔢
* 📌 **Indirizzo IP destinazione** 🎯
* 📌 **Porta destinazione** 🔢
* 📌 **Protocollo di trasporto (TCP/UDP)** 🔄

🔎 **Obiettivo:** Individuare con precisione il traffico sospetto e adottare misure necessarie per mitigarne gli effetti.

## **🛠 4. Requisiti**

✅ **Security Onion VM** ✅ **Accesso agli strumenti Sguil, Wireshark e Kibana** ✅ **Credenziali di accesso (utente: analyst, password: cyberops)** ✅ **Connessione alla rete per analizzare i log remoti** ✅ **Autorizzazioni di amministratore per applicare misure di isolamento**

## **📑 5. Procedura**

### **🛡 Parte 1: Revisione degli Alert in Sguil**

1. Avviare **Security Onion** e accedere con le credenziali fornite.
2. Aprire **Sguil**, selezionare tutte le interfacce e avviare il servizio.
3. Analizzare la colonna "Event Message" per identificare alert sospetti.
4. Individuare l'alert **GPL ATTACK\_RESPONSE id check returned root**.
5. Selezionare **Show Packet Data** e **Show Rule** per visualizzare i dettagli dell'alert.
6. Fare clic con il tasto destro sull'**Alert ID 5.1** e selezionare **Transcript** per esaminare la transazione tra l'attaccante e il target.

### **🕵️ Parte 2: Analisi del Traffico con Wireshark**

1. Dalla vista di Sguil, fare clic con il tasto destro sull'alert ID 5.1 e selezionare **Wireshark**.
2. Visualizzare i pacchetti catturati e seguire il **TCP Stream** per analizzare la conversazione tra attaccante e vittima.
3. Identificare i comandi eseguiti dall'attaccante, come whoami, per confermare i privilegi di root.
4. Esaminare i file trasferiti tra le macchine coinvolte.

### **📊 Parte 3: Investigazione con Kibana**

1. Tornare su **Sguil**, fare clic con il tasto destro sull'IP sospetto e selezionare **Kibana IP Lookup**.
2. Modificare il **time range** per includere il periodo dell'attacco.
3. Filtrare per il protocollo FTP per verificare se è stato usato per trasferire file sospetti.
4. Analizzare il file confidential.txt per confermare il furto di dati.
5. Verificare le credenziali usate per l'accesso al server FTP (analyst / cyberops).
6. Estrarre i dettagli sul file trasferito, tra cui il tipo MIME e il timestamp dell'operazione.

### **🚧 Parte 4: Mitigazione e Prevenzione**

🚀 **Isolare immediatamente l'host compromesso** 🔑 **Cambiare tutte le credenziali di accesso** sui dispositivi vulnerabili 🛑 **Aggiornare le regole firewall** per bloccare il traffico sospetto 🔄 **Applicare patch di sicurezza** per correggere vulnerabilità sfruttate 📡 **Monitorare costantemente i log di rete** per individuare comportamenti anomali

## **✅ 6. Conclusioni e Raccomandazioni**

🔬 Questo laboratorio ha dimostrato come l'analisi approfondita di log e traffico di rete possa aiutare a identificare e neutralizzare minacce informatiche.

💡 **Per evitare compromissioni future, è essenziale adottare una strategia di sicurezza proattiva che includa monitoraggio continuo, aggiornamenti regolari e policy di accesso rigorose.**

## **📖 8. Glossario**

* **5-Tuple**: Metodo di identificazione del traffico di rete.
* **Sguil**: Strumento per la gestione degli eventi di sicurezza.
* **Wireshark**: Analizzatore di traffico di rete.
* **Kibana**: Piattaforma di visualizzazione e analisi dei dati.

## **🔗 9. Risorse Aggiuntive**

* 🔗 [Security Onion](https://securityonion.net/)
* 🔗 [Guida Wireshark](https://www.wireshark.org/)