**Relazione sull'Identificazione e Analisi degli Indicatori di Compromissione (IOC)**

**Introduzione**

Il presente documento descrive il processo di analisi di una cattura di rete effettuata con Wireshark, con l'obiettivo di identificare potenziali Indicatori di Compromissione (IOC), formulare ipotesi sui vettori di attacco utilizzati e proporre azioni per mitigare l'impatto attuale e prevenire futuri attacchi. L'analisi ha portato all'identificazione di diversi pattern sospetti nel traffico di rete che potrebbero essere riconducibili ad attività malevole.

**1. Preparazione dell'Ambiente**

L'analisi è stata condotta utilizzando **Wireshark**, uno strumento di analisi del traffico di rete. La cattura di pacchetti è stata aperta su un sistema basato su Kali Linux, un ambiente comunemente utilizzato per attività di penetration testing e analisi forense. Durante l'analisi, sono stati utilizzati diversi filtri per isolare il traffico pertinente, tra cui:

- **Traffico TCP**: `tcp`
- **Indirizzi IP sospetti**: `ip.addr == 192.168.200.150`

**2. Identificazione e Analisi degli Indicatori di Compromissione (IOC)**

A seguito dell'analisi, sono stati identificati i seguenti **Indicatori di Compromissione** (IOC):

- **Traffico TCP RST/ACK ricorrente**:

È stato osservato un elevato numero di pacchetti TCP con flag **RST/ACK**, un pattern comunemente associato a attività di **port scanning** o tentativi di riconoscimento dei servizi. Questo tipo di traffico potrebbe suggerire un tentativo da parte di un attaccante di determinare quali porte siano aperte su un host di destinazione.

- **Traffico da/verso 192.168.200.150**:

Il dispositivo con indirizzo IP **192.168.200.150** ha inviato traffico sospetto verso un altro dispositivo interno, **192.168.200.100**. Questa attività potrebbe essere indicativa di una **compromissione interna** o della presenza di **malware** sul dispositivo compromesso.

- **Pattern ripetitivi nel traffico**:

Sono stati rilevati pacchetti che si ripetono con intervalli temporali regolari. Questo potrebbe essere il risultato di tentativi di **attacchi brute force** o attività di **esfiltrazione di dati**.

**3. Ipotesi sui Potenziali Vettori di Attacco**

In base agli IOC identificati, sono stati formulati i seguenti vettori di attacco:

- **Port Scanning**:

L'analisi dei pacchetti RST/ACK suggerisce che un attaccante stia cercando di identificare porte vulnerabili per potenziali attacchi.

- **Command & Control (C2)**:

Il traffico ripetuto tra il dispositivo compromesso e un server remoto potrebbe essere un tentativo di **comunicazione C2**, dove un attaccante controlla il dispositivo compromesso tramite comandi remoti.

- **Compromissione Interna**:

L'IP **192.168.200.150** potrebbe essere stato compromesso e utilizzato come punto di partenza per un attacco laterale all'interno della rete.

**4. Azioni per Mitigare l'Impatto e Prevenire Futuri Attacchi**

**Impatto Attuale**

Per mitigare l'impatto dell'attacco attuale, si raccomandano le seguenti azioni immediate:

- **Isolamento dei Dispositivi Coinvolti**:

È necessario isolare i dispositivi **192.168.200.150** e **192.168.200.100** dalla rete per prevenire la diffusione di attività malevole.

- **Scansione dei Dispositivi Compromessi**:

Utilizzare strumenti di sicurezza, come **ClamAV** o **chkrootkit**, per rilevare e rimuovere eventuali malware dai dispositivi compromessi.

**Prevenzione Futura**

Per prevenire futuri attacchi, si suggeriscono le seguenti azioni:

- **Implementazione di un IDS/IPS**:

L'installazione di un sistema di rilevamento e prevenzione delle intrusioni (IDS/IPS) come **Snort** o **Suricata** permetterebbe di monitorare e bloccare in tempo reale le attività sospette.

- **Aggiornamenti Regolari dei Sistemi**:

È fondamentale applicare regolarmente patch e aggiornamenti di sicurezza per ridurre le vulnerabilità.

- **Monitoraggio Continuo**:

Integrare un sistema **SIEM** (Security Information and Event Management) per centralizzare l'analisi dei log di rete e rilevare pattern sospetti.

- **Educazione del Personale**:

È essenziale formare il personale aziendale sulla sicurezza informatica, in particolare sui rischi di **phishing** e **social engineering**.

- **Segmentazione della Rete**:

Implementare una **segmentazione della rete** tramite VLAN per limitare la comunicazione tra dispositivi sensibili e altre risorse della rete.

**Conclusioni**

L'analisi del traffico di rete effettuata con Wireshark ha permesso di individuare diversi Indicatori di Compromissione (IOC), tra cui tentativi di port scanning, sfruttamento di porte non standard e possibili comunicazioni verso un server di comando e controllo. Questi indicatori suggeriscono attività malevole all'interno della rete, potenzialmente condotte da un attaccante esterno o tramite un dispositivo interno compromesso.

Le azioni correttive proposte mirano a contenere l'impatto attuale, prevenendo ulteriori danni attraverso l'isolamento dei dispositivi compromessi, il blocco di IP e porte sospette e l'analisi approfondita dei sistemi coinvolti. Parallelamente, le raccomandazioni preventive forniscono una strategia completa per rafforzare la sicurezza della rete, migliorando il monitoraggio continuo, l'educazione del personale e l'implementazione di soluzioni tecnologiche avanzate come IDS/IPS e SIEM.

L'adozione tempestiva delle contromisure e delle misure preventive suggerite non solo mitigherà l'impatto dell'incidente attuale, ma contribuirà a costruire una rete più resiliente e sicura contro potenziali attacchi futuri.