Relazione S9L5

Analisi di una Cattura di Rete: Indicatori di Compromissione

Introduzione

Questo report descrive l'analisi di una cattura di rete volta a identificare possibili Indicatori di Compromissione (IOC), formulare ipotesi sui vettori di attacco e proporre azioni per mitigare i rischi presenti e futuri. Utilizzando Wireshark, sono stati osservati pattern di traffico che suggeriscono attività anomale o malevole.

Metodo di Analisi

1. **Ambiente Configurato**:
    - Strumento: Wireshark su Kali Linux.
    - File analizzato: cattura fornita in formato `.pcap`.
    - Filtri principali utilizzati:
        - `tcp` per il traffico TCP.
        - `dns` per richieste DNS sospette.
        - `tcp.port == 445` per traffico SMB.
2. **Fasi dell'Analisi**:
    - Applicazione di filtri per isolare attività rilevanti.
    - Identificazione di modelli ricorrenti (es. connessioni interrotte, uso di porte non standard).
    - Valutazione del comportamento di host sospetti.

Risultati dell'Analisi

Indicatori di Compromissione Identificati

1. **Comportamento TCP anomalo:**
    - Numerosi pacchetti `RST` (reset) indicano che le connessioni venivano chiuse forzatamente.
    - Questo pattern è spesso correlato a scansioni di rete mirate a identificare servizi attivi.
2. **Traffico SMB sospetto:**
    - Comunicazioni sulla porta 445 tra `192.168.200.150` e `192.168.200.100`.
    - Potenziale tentativo di sfruttamento di vulnerabilità (es. EternalBlue).

3. **Porte non standard:**
    - Presenza di traffico sulla porta 4444, comunemente utilizzata da server di comando e controllo (C2).
4. **Traffico DNS non usuale:**
    - Richieste a domini sconosciuti o sospetti, possibile segnale di comunicazioni con un server C2 remoto.

Ipotesi sui Vettori di Attacco

1. **Scansione di rete:**
    - Gli RST frequenti indicano una probabile scansione da parte di un attore malevolo per individuare porte aperte o servizi vulnerabili.
2. **Exploitation SMB:**
    - Il traffico sulla porta 445 suggerisce tentativi di sfruttare vulnerabilità SMB conosciute.
3. **Comunicazione C2:**
    - Traffico DNS e utilizzo della porta 4444 potrebbero indicare comunicazioni con un server remoto di comando e controllo.
4. **Movimenti laterali:**
    - Il dispositivo `192.168.200.150` potrebbe essere stato compromesso e utilizzato come base per ulteriori attacchi interni.

Raccomandazioni

Azioni Immediati

1. **Isolamento di Sistemi Compromessi:**
    - Disconnettere i dispositivi `192.168.200.150` e `192.168.200.100` dalla rete per evitare ulteriori compromissioni.
2. **Blocchi di rete:**

Impostare regole firewall per bloccare traffico da/verso IP e porte sospette:
ufw deny from 192.168.200.150
ufw deny to any port 4444

    -
3. **Analisi antivirus:**

- Eseguire scansioni approfondite con strumenti come ClamAV o chkrootkit sui dispositivi isolati.

Misure Preventive

1. **Implementazione di IDS/IPS:**
    - Configurare sistemi di rilevamento delle intrusioni (Snort, Suricata) per monitorare traffico anomalo.
2. **Aggiornamento dei sistemi:**
    - Applicare patch di sicurezza per SMB e altri servizi esposti a vulnerabilità note.
3. **Segmentazione della rete:**
    - Ridurre la comunicazione tra segmenti della rete mediante VLAN.
4. **Monitoraggio continuo:**
    - Integrare un SIEM per analizzare e correlare eventi di sicurezza in tempo reale.
5. **Formazione degli utenti:**
    - Istruire il personale sui rischi di phishing e sull'importanza di riconoscere comportamenti sospetti.

Conclusioni

L'analisi ha identificato indicatori di compromissione significativi, tra cui traffico SMB sospetto, connessioni forzatamente chiuse e utilizzo di porte non standard. Le azioni immediate, combinate con misure preventive a lungo termine, sono fondamentali per mitigare i rischi e prevenire futuri attacchi. Raccomandiamo l'implementazione di strumenti di monitoraggio avanzati e la segmentazione della rete per aumentare la resilienza complessiva.