Cowrie

Scopo e funzionalità principali:

- Cowrie è un honeypot interattivo per servizi SSH e Telnet.
- Simula un ambiente di shell Unix per attirare attaccanti e monitorarne le attività.
- È in grado di registrare i comandi inseriti dall'attaccante, i tentativi di download di file malevoli e le tecniche di movimento laterale.

Perché potrebbe essere utile in uno scenario reale:

- Fornisce insight su nuovi strumenti o malware che gli aggressori tentano di scaricare.
- Contribuisce a migliorare le difese reali basandosi su informazioni raccolte direttamente dagli attacchi.

Uso pratico:

- Installato su un server appositamente dedicato, Cowrie viene lasciato visibile a potenziali attaccanti.
- L'amministratore analizza in seguito i log per identificare pattern di attacco ricorrenti e aggiornare i sistemi di protezione (firewall, IDS, password policy).

Dionaea

Scopo e funzionalità principali:

- Dionaea è un honeypot specializzato nel catturare malware.
- Simula diversi servizi vulnerabili (SMB, HTTP, FTP, MSSQL, ecc.) per attirare exploit e payload malevoli.
- Quando un attaccante sfrutta una vulnerabilità simulata, Dionaea tenta di “ingannare” il malware, inducendolo a infettare il sistema honeypot, permettendone la cattura per l’analisi.

Perché potrebbe essere utile in uno scenario reale:

- Aiuta a raccogliere campioni di malware senza mettere a rischio sistemi reali.
- Consente di ottenere dettagli su come gli attacchi sfruttano specifiche vulnerabilità.
- Facilita l’aggiornamento delle firme di antivirus, IDS/IPS e la definizione di policy di sicurezza più efficaci.

Uso pratico:

- Collocare Dionaea in una DMZ o su un server dedicato.
- Analizzare periodicamente i malware raccolti per identificare nuove minacce ed elaborare contromisure.

T-Pot (Distribuzione Honeypot Integrata)

Scopo e funzionalità principali:

- T-Pot è una soluzione all-in-one che integra diversi honeypot (come Cowrie, Dionaea, Elastichoney, Honeytrap, etc.) in una sola piattaforma.
- Fornisce un ambiente di monitoraggio con dashboard preconfigurate.
- Copre un ampio spettro di servizi, analizzando una vasta gamma di attacchi.

Perché potrebbe essere utile in uno scenario reale:

- Riduce la complessità di installazione e gestione di diversi honeypot separati.
- Offre una panoramica centralizzata degli attacchi, facilitando il rilevamento di pattern.
- È particolarmente utile per team di sicurezza che vogliono un'unica soluzione scalabile e facilmente gestibile.

Uso pratico:

- Distribuire T-Pot su una macchina virtuale o un server dedicato.
- Utilizzare la dashboard integrata per osservare in tempo reale gli attacchi e raccogliere dati da molteplici fonti con un unico strumento.

Log generati dalle honeypot: Dati Raccolti e Valore Forense

Tipi di dati registrati:

- **IP dell'attaccante:** Permette di identificare la presunta provenienza dell'attacco (anche se potrebbe essere un proxy o una botnet).
- **Timestamp delle azioni:** Consente di ricostruire la cronologia degli eventi, importante per stabilire una timeline accurata di un attacco.
- **Comandi eseguiti:** In honeypot come Cowrie, ogni comando inserito dall'attaccante viene salvato, fornendo informazioni sulle tecniche e sugli obiettivi (furto di dati, movimenti interni, installazione di malware, ecc.).
- **Payload e file scaricati:** Honeypot come Dionaea registrano i file malevoli scaricati, permettendo di analizzarne il contenuto.
- **Informazioni sul protocollo e sul servizio attaccato:** Mostra quali vulnerabilità sono state prese di mira, quali credenziali tentate, quali servizi attirano maggiormente gli attaccanti.

Valore di questi log per l’analisi forense:

- **Identificazione delle Tecniche di Attacco:** I log consentono di comprendere la catena di azioni compiute dagli aggressori, aiutando ad anticipare mosse simili contro i sistemi reali.
- **Miglioramento delle Difese:** I dati raccolti possono aiutare a raffinare i sistemi di rilevamento delle intrusioni, filtrare IP dannosi a livello di firewall, aggiornare blacklist e migliorare le regole di sicurezza.
- **Analisi Storica e Trend:** Confrontando i log nel tempo, si possono individuare trend, nuove tipologie di attacco, varianti di malware e tattiche emergenti, supportando una strategia di sicurezza proattiva.

In sintesi, i log degli honeypot sono una miniera di informazioni che, correttamente analizzate, consentono di comprendere meglio il panorama delle minacce, ridurre i rischi per l’infrastruttura aziendale e supportare indagini forensi più efficaci.