Definizione delle Honeypot

Cos'è una honeypot in cybersecurity?

Una honeypot è un sistema o risorsa informatica deliberatamente vulnerabile progettata per attirare e monitorare attività malevole. Il suo scopo principale è ingannare attaccanti o malware, raccogliendo informazioni utili per la difesa delle reti. Non è parte integrante della rete operativa, ma un'esca che registra le azioni degli intrusi.

Tipi principali di honeypot:

1. **Bassa interazione:**
    a. Simula parzialmente i servizi o le applicazioni.
    b. Minimizza i rischi poiché non permette agli attaccanti di ottenere un accesso completo.
    c. Esempi: emulazioni di server FTP o SSH.
2. **Alta interazione:**
    a. Riproduce interamente un sistema operativo o servizio.
    b. Fornisce dati più ricchi sugli attacchi ma comporta rischi maggiori.
    c. Può essere compromesso e utilizzato contro la rete.
3. **Honeynets:**
    a. Una rete completa di honeypot con più sistemi simulati.
    b. Consente di analizzare attacchi complessi e movimenti laterali.

Vantaggi dell'uso delle honeypot:

- **Monitoraggio avanzato:** Permettono di catturare nuovi exploit e strategie degli attaccanti.
- **Riduzione dei falsi positivi:** Registrano solo attività intenzionali malevole, riducendo il "rumore".
- **Supporto all'analisi forense:** Offrono dati dettagliati per analisi post-attacco.
- **Protezione passiva:** Distraggono gli attaccanti da risorse critiche.

Rischi e limitazioni:

- **Rischio di compromissione:** Gli attaccanti possono usare una honeypot compromessa per attaccare la rete principale.
- **Limitato al traffico diretto:** Non rileva attacchi che non interagiscono direttamente con la honeypot.
- **Manutenzione e monitoraggio costosi:** Richiedono competenze per l'implementazione e analisi costanti.

Strumenti di honeypot:

1. **Cowrie**
    a. **Scopo e funzionalità principali:**

Un honeypot SSH e Telnet che emula un sistema vulnerabile. Registra credenziali, comandi eseguiti e tentativi di brute force.

    b. **Utilità:** Ottimo per monitorare attacchi al protocollo SSH.
    c. **Scenario reale:** Studi sui pattern di attacco di botnet.
2. **Dionaea**
    a. **Scopo e funzionalità principali:**

Progettato per catturare malware, offre emulazione di servizi vulnerabili come SMB, HTTP e FTP.

    b. **Utilità:** Permette di raccogliere campioni di malware per l'analisi.
    c. **Scenario reale:** Utile in reti aziendali per rilevare nuovi malware.
3. **Honeyd**
    a. **Scopo e funzionalità principali:**

Un honeypot configurabile che simula sistemi operativi e servizi multipli.

    b. **Utilità:** Aiuta a creare ambienti fittizi per confondere gli attaccanti.
    c. **Scenario reale:** Difesa contro scanner automatici o tentativi di footprinting.

Uso Pratico: Esempi di Log Generati

Dati registrati:

- **IP e timestamp:** Identificazione degli attaccanti e cronologia degli attacchi.
- **Comandi eseguiti:** Rivelano gli obiettivi e le intenzioni degli attaccanti.
- **Dettagli del payload:** Utili per analizzare exploit o malware utilizzati.

Valore per l'analisi forense:

- **Identificazione di pattern:** Permette di scoprire nuove tecniche di attacco.
- **Tracciabilità:** Offre prove concrete per collegare attività malevole a specifici attori.
- **Prevenzione futura:** Facilita l'aggiornamento di regole e difese basate sulle informazioni raccolte.