Definizione delle Honeypot

Cos'è una honeypot

Una **honeypot** è un sistema o una risorsa progettata per attrarre e ingannare gli attaccanti, simulando vulnerabilità per studiare le loro tecniche e comportamenti. Le honeypot possono essere utilizzate per raccogliere informazioni sugli attacchi e migliorare le difese di sicurezza.

Tipi di honeypot

1. **Bassa interazione**:
    a. Simulano solo alcuni servizi e non forniscono un ambiente completo. Sono più facili da implementare e meno rischiosi.
    b. Esempi: trappole per malware, trappole per spam.
2. **Alta interazione**:
    a. Offrono un ambiente completo e interattivo, permettendo agli attaccanti di interagire con il sistema come se fosse reale. Queste honeypot sono più complesse e rischiose, ma forniscono dati più dettagliati.
    b. Esempi: server virtuali che emulano sistemi operativi reali.
3. **Honeynets**:
    a. Reti di honeypot che lavorano insieme per attrarre attaccanti e raccogliere dati su attacchi distribuiti. Offrono una visione più ampia delle tecniche di attacco.

Vantaggi nell’uso per una rete aziendale

- **Raccolta di dati**: Le honeypot forniscono informazioni preziose sugli attaccanti, le loro tecniche e i loro obiettivi.
- **Miglioramento della sicurezza**: Analizzando gli attacchi, le aziende possono rafforzare le loro difese e prevenire futuri attacchi.
- **Distrazione degli attaccanti**: Le honeypot possono deviare gli attaccanti dai sistemi reali, riducendo il rischio di compromissione.

Rischi o limitazioni legati all'uso

- **Rischio di compromissione**: Se non configurate correttamente, le honeypot possono diventare un punto di accesso per gli attaccanti.
- **Falsi positivi**: Potrebbero generare allarmi non necessari, complicando la gestione della sicurezza.

- **Costi di gestione**: Richiedono risorse per la configurazione, la manutenzione e l'analisi dei dati raccolti.

Strumenti di honeypot open-source / commerciali

1. Honeyd

- **Descrizione**: Honeyd è un software open-source progettato per simulare una rete di sistemi operativi e servizi. Permette di creare honeypot virtuali che possono ingannare gli attaccanti facendogli credere di interagire con sistemi reali.
- **Funzionalità principali**:
  - Simulazione di vari sistemi operativi e servizi di rete.
  - Creazione di una rete virtuale di honeypot per raccogliere dati sugli attacchi.
  - Monitoraggio delle interazioni degli attaccanti con i sistemi simulati.
- **Utilità in uno scenario reale**: Honeyd è utile per le aziende che desiderano testare le proprie difese e raccogliere informazioni sulle tecniche di attacco, migliorando così la sicurezza della rete.

2. Dionaea

- **Descrizione**: Dionaea è un honeypot progettato specificamente per catturare malware e attacchi a servizi vulnerabili. È in grado di raccogliere campioni di malware per l'analisi.
- **Funzionalità principali**:
  - Cattura di exploit e malware attraverso la simulazione di servizi vulnerabili.
  - Raccolta di informazioni dettagliate sugli attacchi, inclusi i file di malware.
  - Analisi dei dati raccolti per migliorare le difese contro attacchi specifici.
- **Utilità in uno scenario reale**: Dionaea è particolarmente utile per le aziende che vogliono analizzare il malware e comprendere le tecniche utilizzate dagli attaccanti, contribuendo a rafforzare le loro misure di sicurezza.

3. Cowrie

- **Descrizione**: Cowrie è un honeypot che simula un sistema vulnerabile per raccogliere informazioni sugli attacchi, in particolare quelli che mirano a servizi SSH e Telnet.
- **Funzionalità principali**:

    - Simulazione di un ambiente SSH e Telnet per attrarre attaccanti.
    - Registrazione delle interazioni degli attaccanti, inclusi i comandi eseguiti.
    - Raccolta di dati per analisi forensi e miglioramento della sicurezza.
- **Utilità in uno scenario reale**: Cowrie è utile per monitorare tentativi di accesso non autorizzato e raccogliere informazioni sulle tecniche di attacco, consentendo alle aziende di migliorare le loro difese contro accessi non autorizzati.

Esempi di log generati dalle honeypot

Certo! Ecco alcuni esempi di log generati dai tre honeypot: **Honeyd**, **Dionaea** e **Cowrie**. Questi log forniscono informazioni preziose sugli attacchi e sulle interazioni degli attaccanti.

1. Honeyd

I log di Honeyd possono includere informazioni come:

- **Timestamp**: Data e ora dell'interazione.
- **Indirizzo IP**: Indirizzo IP dell'attaccante.
- **Tipo di attacco**: Descrizione del tipo di attacco tentato (es. scansione delle porte).
- **Servizi simulati**: Elenco dei servizi che sono stati simulati e a cui l'attaccante ha tentato di accedere.

Esempio di log:

```
[2024-12-06 14:32:10] ATTACCO: Scansione delle porte da 192.168.1.10
Servizi simulati: HTTP, FTP
```

2. Dionaea

Dionaea è progettato per catturare malware e attacchi a servizi vulnerabili. I log possono includere:

- **Timestamp**: Data e ora dell'attacco.
- **Indirizzo IP**: Indirizzo IP dell'attaccante.
- **Tipo di malware**: Nome e tipo di malware catturato.
- **Comandi eseguiti**: Comandi che l'attaccante ha tentato di eseguire.

Esempio di log:

```
[2024-12-06 15:45:22] MALWARE CATTURATO: Trojan.Win32.Generic
Indirizzo IP: 203.0.113.5
Comandi eseguiti: download malware.exe
```

3. Cowrie

Cowrie registra le interazioni degli attaccanti su SSH e Telnet. I log possono includere:

- **Timestamp**: Data e ora dell'accesso.
- **Indirizzo IP**: Indirizzo IP dell'attaccante.
- **Comandi eseguiti**: Comandi che l'attaccante ha tentato di eseguire.
- **Risultato**: Esito dell'interazione (es. accesso riuscito o fallito).

Esempio di log:

```
[2024-12-06 16:00:05] ACCESSO: Tentativo di accesso SSH da
198.51.100.20
Comandi eseguiti: ls -la
Risultato: Accesso fallito
```