Cos'è una Honeypot in Cybersecurity?

Una honeypot è un sistema o dispositivo progettato per simulare una risorsa vulnerabile in una rete, attirando e monitorando i comportamenti di potenziali attaccanti.

Possono essere classificate in base a diversi criteri, come ***il livello di interazione*** con l'attaccante, ***l'obiettivo*** per cui sono state progettate e ***il contesto d'uso*** (aziendale o di ricerca).

1. Classificazione per Livello di Interazione

1. **Honeypots a Bassa Interazione**
    - **Descrizione:** Simulano solo una parte limitata di un sistema reale. Offrono funzionalità base per attirare gli attaccanti, come porte aperte o servizi basilari.
    - **Obiettivo:** Rilevare tentativi di attacco e registrare attività preliminari (scansioni di rete, exploit semplici).
    - **Esempi di utilizzo:** Simulare una porta SSH o un servizio HTTP con funzionalità limitate.
    - **Vantaggi:**
        - Facile da configurare.
        - Basso rischio, poiché l'attaccante non può interagire con un sistema reale.
    - **Svantaggi:**
        - Raccolgono dati limitati.
        - Gli attaccanti esperti possono riconoscerle facilmente.
    - **Esempio:** Kippo (simula un server SSH base).
    -
2. **Honeypots ad Alta Interazione**
    - **Descrizione:** Simulano un intero sistema reale, come un server completo o un'applicazione complessa, consentendo agli attaccanti di interagire con esso in modo più approfondito.
    - **Obiettivo:** Raccogliere dati dettagliati sul comportamento dell'attaccante, incluso il tipo di exploit utilizzato e i comandi eseguiti.
    - **Esempi di utilizzo:** Un server web vulnerabile configurato per attirare attacchi mirati.
    - **Vantaggi:**
        - Raccoglie molte informazioni, comprese le tecniche avanzate degli attaccanti.
        - Ideale per analisi dettagliate e ricerca.
    - **Svantaggi:**
        - Maggiore complessità di configurazione.
        - Può rappresentare un rischio per la rete aziendale se non adeguatamente isolata.
    - **Esempio:** Dionaea (honeypot per raccogliere malware ed exploit).
3. **Honeypots a Media Interazione**
    - **Descrizione:** Compromesso tra bassa e alta interazione. Simulano alcuni aspetti avanzati di un sistema reale senza esporre l'intera infrastruttura.

- **Obiettivo:** Aumentare la credibilità agli occhi dell'attaccante senza i rischi di un'alta interazione.
- **Esempi di utilizzo:** Simulare una parte di un database SQL vulnerabile o un servizio FTP.
- **Vantaggi:**
  - Più sicura rispetto alle honeypot ad alta interazione.
  - Raccolgono più dati rispetto a quelle a bassa interazione.
- **Svantaggi:**
  - Possono essere meno convincenti rispetto a honeypot di alta interazione.

---

2. Classificazione per Contesto di Utilizzo

1. **Honeypots di Produzione**
   - **Descrizione:** Utilizzate in ambienti operativi reali per proteggere reti aziendali. Spesso configurate per sembrare parte della rete e attirare attacchi.
   - **Obiettivo:** Distrarre gli attaccanti dalle risorse reali e individuare intrusioni.
   - **Caratteristiche:** Basso impatto sulle operazioni aziendali, configurate per minimizzare rischi.
   - **Esempio:** Simulare una stampante di rete o un server FTP vulnerabile.
2. **Honeypots di Ricerca**
   - **Descrizione:** Utilizzate per raccogliere informazioni sugli attaccanti e studiare nuovi exploit e tecniche.
   - **Obiettivo:** Comprendere le minacce emergenti e migliorare le difese.
   - **Caratteristiche:** Spesso ad alta interazione per raccogliere il maggior numero possibile di dati.
   - **Esempio:** Dionaea (per catturare malware).

---

3. Honeynets

- **Descrizione:** Una rete completa di honeypots interconnessi che simula un'infrastruttura complessa (ad esempio una rete aziendale con server, workstation, e dispositivi IoT).
- **Obiettivo:** Osservare attacchi complessi, come movimenti laterali, escalation di privilegi, e comportamenti post-sfruttamento.
- **Vantaggi:**
  - Perfette per simulare ambienti reali.
  - Offrono una visione dettagliata delle tattiche avanzate degli attaccanti.
- **Svantaggi:**
  - Complessità elevata di configurazione e manutenzione.
  - Richiedono un isolamento rigoroso per evitare che vengano usate come trampolini di lancio.
- **Esempio:** Honeynet Project (framework per creare honeynets).

---

4. Honeypots per Scopi Specifici

1. **Email Honeypots**
    - **Descrizione:** Progettate per attirare spammer o analizzare campagne di phishing.
    - **Funzionamento:** Creano indirizzi email fittizi per raccogliere spam e analizzarlo.
    - **Utilità:** Identificare campagne di spam e le tecniche di phishing.
2. **Database Honeypots**
    - **Descrizione:** Simulano database vulnerabili per attirare attacchi SQL Injection o tentativi di accesso non autorizzati.
    - **Esempio:** Mysqlpot.
3. **IoT Honeypots**
    - **Descrizione:** Simulano dispositivi IoT vulnerabili, come videocamere IP o router.
    - **Obiettivo:** Studiare attacchi che colpiscono dispositivi connessi.
    - **Esempio:** IoTPOT.

MIGLIORI HONEYPOTS NELLA CYBERSECURITY

Ecco una lista aggiornata di **honeypots migliori** e ampiamente utilizzate nel campo della cybersecurity, con una descrizione dettagliata e l'indicazione se sono **open-source** o **commerciali**:

---

1. T-Pot

- **Tipologia:** Honeypot all-in-one.
- **Open-source.**
- **Descrizione:** T-Pot è una piattaforma che integra diverse honeypots (Dionaea, Cowrie, conpot, ecc.) in un unico sistema. È altamente configurabile e fornisce un'interfaccia grafica per monitorare gli attacchi in tempo reale.
- **Perché usarla:** Ideale per raccogliere una varietà di dati da diverse tipologie di attacchi (es. malware, brute force, attacchi industriali).
- **Uso pratico:** Ottima per ambienti di test aziendali e di ricerca.

---

2. Cowrie

- **Tipologia:** Honeypot SSH e Telnet.
- **Open-source.**
- **Descrizione:** Successore di Kippo, Cowrie è un honeypot avanzato che simula un server SSH/Telnet. Può registrare i comandi eseguiti dagli attaccanti e catturare file.
- **Perché usarla:** Ideale per monitorare tentativi di brute force e raccolta di comandi utilizzati dagli attaccanti.
- **Uso pratico:** Perfetto per testare attacchi SSH/Telnet e migliorare le politiche di sicurezza.

---

3. Modern Honey Network (MHN)

- **Tipologia:** Sistema di gestione di honeypots.
- **Open-source.**
- **Descrizione:** MHN è una piattaforma per gestire e monitorare honeypots distribuite in rete. Supporta l'integrazione con strumenti come Dionaea, Cowrie e altri.
- **Perché usarla:** Centralizza il controllo e la raccolta di dati da più honeypots.
- **Uso pratico:** Adatto per reti aziendali complesse con più honeypots.

---

4. Cuckoo Sandbox

- **Tipologia:** Sandbox per analisi malware (honeypot indiretto).
- **Open-source.**
- **Descrizione:** Simula un ambiente reale per eseguire e analizzare malware. Anche se non è una honeypot classica, viene utilizzata per attirare e studiare file sospetti.
- **Perché usarla:** Utile per analisi forensi e malware testing.
- **Uso pratico:** Ideale per team di ricerca sulla sicurezza.

---

5. KFSensor

- **Tipologia:** Honeypot commerciale.
- **Commerciale.**
- **Descrizione:** KFSensor è una soluzione honeypot completa per ambienti Windows, progettata per rilevare e analizzare attacchi.
- **Perché usarla:** Offre un'interfaccia user-friendly e funzionalità avanzate di logging.
- **Uso pratico:** Perfetta per aziende che cercano soluzioni pronte all'uso.

---

6. Conpot

- **Tipologia:** Honeypot per SCADA e sistemi industriali.
- **Open-source.**
- **Descrizione:** Simula dispositivi industriali SCADA (Supervisory Control and Data Acquisition) per attirare attacchi a infrastrutture critiche.
- **Perché usarla:** Utile per studiare attacchi rivolti a sistemi ICS/SCADA.
- **Uso pratico:** Ideale per infrastrutture industriali e ricerca su attacchi critici.

---

7. Glastopf

- **Tipologia:** Honeypot per attacchi web.
- **Open-source.**
- **Descrizione:** Specializzato nell'attirare e registrare attacchi a livello di applicazioni web, come SQL Injection e XSS.
- **Perché usarla:** Eccellente per analizzare attacchi specifici su siti web.
- **Uso pratico:** Monitoraggio di siti web e analisi delle vulnerabilità applicative.

---

8. Canarytokens

- **Tipologia:** Honeypot leggero basato su token.
- **Commerciale (con versione gratuita).**
- **Descrizione:** Non è un honeypot tradizionale ma utilizza token inseriti in documenti, email o link per monitorare movimenti sospetti. Quando un token viene attivato, invia un avviso.
- **Perché usarla:** Perfetta per monitorare attacchi o movimenti laterali all'interno di una rete.
- **Uso pratico:** Semplice da implementare per proteggere dati sensibili.

Confronto tra questi strumenti

Nome	Tipologia	Licenza	Obiettivo principale
T-Pot	All-in-one	Open-source	Monitoraggio di attacchi multipli
Cowrie	SSH/Telnet honeypot	Open-source	Brute force e comandi eseguiti
MHN	Sistema di gestione	Open-source	Gestione centralizzata di honeypots
Cuckoo Sandbox	Sandbox	Open-source	Analisi di malware
KFSensor	Honeypot commerciale	Commerciale	Rilevazione di attacchi aziendali
Conpot	Honeypot per SCADA	Open-source	Sicurezza per infrastrutture critiche
Glastopf	Honeypot web	Open-source	Attacchi a siti web
Canarytokens	Token honeypot	Commerciale	Rilevamento di movimenti sospetti

Quale scegliere?

- **Per aziende:** KFSensor o Canarytokens.
- **Per ricerca:** T-Pot, Dionaea, Cowrie, Glastopf.
- **Per infrastrutture industriali:** Conpot.
- **Per analisi malware:** Cuckoo Sandbox.

VANTAGGI E RISCHI NELL'USO DI HONEYPOT

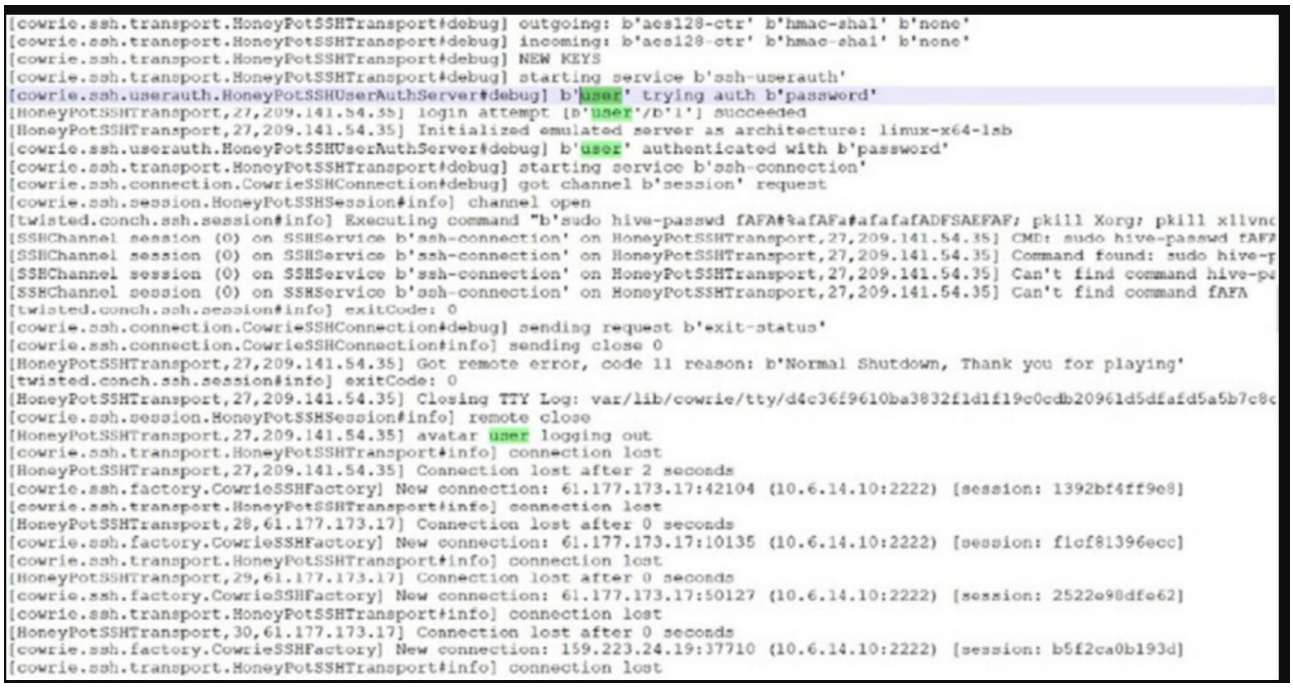
Vantaggi:

- **Monitoraggio degli attacchi:** Raccolgono dati sugli attaccanti, inclusi metodi e strumenti utilizzati.
- **Difesa proattiva:** Possono rallentare o distrarre gli attaccanti.
- **Supporto alla forensica:** Forniscono log utili per indagini future.
- **Costi contenuti:** Un singolo dispositivo può attirare e monitorare molti attaccanti.

Rischi o Limitazioni:

1. **Rilevazione:** Attaccanti esperti possono riconoscerle, riducendone l'efficacia.
2. **Uso malevolo:** Se mal configurate, possono essere sfruttate per attaccare altri sistemi.
3. **Dati limitati:** Raccolgono solo informazioni relative agli attacchi diretti alla honeypot.
4. **Risorse richieste:** Alcuni tipi di honeypot richiedono manutenzione e monitoraggio costanti.

ESEMPI DI LOG GENERATI DALLE HONEYPOT



Cowrie Honeypot Log

- **Autenticazione utente:**

  ```
  cowrie.ssh.userauth.HoneyPotSSHUserAuthServer] b'user' trying auth
  b'password'

  cowrie.ssh.userauth.HoneyPotSSHUserAuthServer] b'user' authenticated with
  b'password'
  ```

  - L'attaccante ha utilizzato il nome utente `user` e la password `password`.
  - Autenticazione avvenuta con successo, poiché la honeypot simula un server con credenziali predefinite.

- **Comando eseguito dall'attaccante:**

  ```
  SSHChannel session] CMD: sudo hive-passwd FAF#aFAFAfADFSAEFPAF; pkill
  Xorg; pkill x11vnc
  ```

  - L'attaccante ha tentato di:
    1. Eseguire un comando con `sudo` per cambiare una password (ipoteticamente tramite `hive-passwd`).
    2. Terminare processi come `Xorg` e `x11vnc` (potrebbero essere tentativi di sabotaggio o modifiche locali).

  Nota:

  - I comandi `hive-passwd` e `FAF#aFAFAfADFSAEFPAF` non sono stati riconosciuti dal sistema:

  ```
  Can't find command hive-passwd
  Can't find command FAF#aFAFAfADFSAEFPAF
  ```

- **Sessione chiusa:**

```
[twisted.conch.ssh.session] exitCode 0
[HoneyPotSSHTransport] remote close
[HoneyPotSSHTransport] Connection lost
```

    - L'attaccante ha chiuso la sessione senza errori apparenti.

- **Nuove connessioni perse:**

```
[HoneyPotSSHTransport] connection lost after 2 seconds
[HoneyPotSSHTransport] connection lost after 0 seconds
```

    - Diverse connessioni successive non sono state mantenute, suggerendo che l'attaccante (o un bot) potrebbe aver testato velocemente accessi multipli.

Analisi del Log

1. **Tentativi di attacco:**
    - L'attaccante ha cercato di utilizzare comandi malevoli per:
        - Cambiare password (`hive-passwd`).
        - Terminare servizi grafici o remoti (`Xorg`, `x11vnc`).
2. **Dati registrati utili per l'analisi forense:**
    - **IP dell'attaccante:** `27.209.141.54.35` (può essere utilizzato per identificare o tracciare l'origine dell'attacco).
    - **Comandi tentati:** Informazioni sui possibili obiettivi dell'attaccante.
    - **Tempi e durata:** Timestamp delle connessioni per analizzare pattern di comportamento.
3. **Conclusioni:**
    - Questo log mostra un comportamento tipico di attaccanti automatici o bot che tentano attacchi su server SSH vulnerabili.
    - È importante isolare e analizzare i pattern per migliorare le difese della rete reale.