Scheda Tecnica

Servizio HoneyPot

SOC Cyber Defense SA, Via Cantonale 23c, CH 6928 Manno
T +41 91 611 70 00, info@soccd.swiss - www.soccd.swiss

1. *Descrizione generale*

Un servizio honeypot è una strategia di sicurezza informatica progettata per attrarre e monitorare attacchi informatici, fungendo da esca per i cybercriminali. Questo sistema può essere implementato sia come hardware che come software, ed è caratterizzato da vulnerabilità deliberate che lo rendono un obiettivo interessante per gli attaccanti.

Il funzionamento di un honeypot si basa sulla creazione di un ambiente isolato che simula risorse o sistemi reali, ma senza contenere dati sensibili. Quando un attaccante tenta di sfruttare le vulnerabilità dell'honeypot, le sue azioni vengono registrate e analizzate, fornendo agli esperti di sicurezza informazioni preziose sui metodi e le tecniche utilizzate dagli aggressori.

2. *Descrizione prodotti e funzionalità*

Le caratteristiche principali di un HoneyPot sono:

- Attrattività

  Un honeypot è progettato per sembrare un obiettivo interessante per gli attaccanti. Può simulare un sistema o una risorsa autentica per attirare attenzione e interazioni malevole.

- Isolamento

  L'honeypot è implementato in un ambiente isolato logicamente per evitare che un attacco su di esso si estenda al resto dell'infrastruttura.

- Monitoraggio

  Registra attentamente tutte le attività che avvengono al suo interno. Questo include tentativi di accesso, interazioni con il sistema e comportamenti anomali che potrebbero indicare un attacco.

- Flessibilità

  Gli honeypot possono essere configurati per emulare diversi tipi di sistemi e servizi, consentendo agli amministratori di scegliere il livello di complessità e la specificità desiderati.

I vantaggi di un honeypot possono essere:

- Rilevamento precoce

  Essendo progettato per attirare attenzione, un honeypot può rivelare gli attacchi in una fase molto precoce. Ciò consente agli amministratori di sistema di intervenire prima che l'attacco raggiunga la rete principale.

- Raccolta di informazioni

  Gli honeypot forniscono preziose informazioni sulle tattiche, tecniche e procedure (TTP) degli attaccanti. Questi dati possono essere utilizzati per migliorare le difese e rafforzare la sicurezza complessiva.

- Studio del comportamento degli attaccanti

  Analizzando le interazioni con l'honeypot, gli analisti del SOC ottengono una comprensione più approfondita del comportamento degli attaccanti, consentendo una migliore preparazione contro minacce simili in futuro e estendendo la conoscenza a tutti i clienti.

- Attività di trappola

  Gli honeypot possono servire come una sorta di "trappola" per gli attaccanti. Attaccare un honeypot può distrarre gli aggressori da obiettivi più critici nell'infrastruttura.

- Sviluppo e test di nuove difese

  Gli honeypot offrono un ambiente controllato per testare nuove tecniche di difesa e misure di sicurezza senza rischi per la rete principale.