Definizione delle Honeypot

Una honeypot è un sistema o una risorsa digitale configurata per apparire come un obiettivo vulnerabile, progettata per attirare e ingannare potenziali attaccanti informatici. Le honeypot sono utilizzate per monitorare, rilevare e studiare comportamenti malevoli, con l'obiettivo di raccogliere informazioni utili per rafforzare la sicurezza di una rete.

Principali tipi di Honeypot

1. Honeypot a bassa interazione:
   Simulano solo alcuni servizi o funzioni di un sistema reale. Sono più semplici da implementare e a basso rischio, ma offrono informazioni limitate sugli attacchi.
   - Esempio: Emulare un server FTP o un database vulnerabile.
2. Honeypot ad alta interazione:
   Replicano completamente un sistema operativo o un'applicazione reale, consentendo agli attaccanti di interagire in modo approfondito. Offrono dati dettagliati, ma comportano maggiori rischi e richiedono più risorse per la gestione.
3. Honeynets:
   Una rete di honeypot progettata per simulare una complessa infrastruttura IT. Sono ideali per rilevare attacchi avanzati e studiare tattiche, tecniche e procedure (TTP) utilizzate dagli attaccanti.

Vantaggi delle Honeypot

- Rilevazione degli attacchi: Identificano comportamenti malevoli che potrebbero passare inosservati con i sistemi tradizionali di rilevazione.
- Raccolta di informazioni: Forniscono dettagli sugli attacchi, come indirizzi IP, exploit utilizzati e modalità operative.
- Analisi delle minacce: Permettono di studiare le tecniche degli attaccanti, migliorando le strategie di difesa.
- Riduzione dei falsi positivi: A differenza di altri strumenti, le honeypot rilevano solo attività malevole dirette, minimizzando i falsi allarmi.

Rischi e Limitazioni

1. Possibile compromissione: Un honeypot compromesso potrebbe essere usato dagli attaccanti per lanciare attacchi contro altre reti.
2. Limitazioni di rilevamento: Rilevano solo attacchi diretti contro di loro e non quelli contro l’intera rete.
3. Manutenzione complessa: Le honeypot ad alta interazione richiedono risorse significative per essere gestite e aggiornate.
4. Esposizione legale: Se un attaccante utilizza l’honeypot per scopi malevoli, potrebbero sorgere implicazioni legali.

Strumenti di Honeypot

1. Cowrie
    - Scopo e funzionalità: Honeypot SSH/Telnet che simula un ambiente reale per catturare credenziali e comandi eseguiti dagli attaccanti.
    - Utilità: Ottimo per monitorare attacchi brute force e studiare script di automazione.
    - Scenario reale: Può aiutare a identificare tecniche di movimento laterale in reti aziendali.
2. Kippo (erede di Cowrie):
    - Scopo e funzionalità: Honeypot SSH per emulare un sistema Linux vulnerabile.
    - Utilità: Fornisce log dettagliati delle interazioni e delle credenziali compromesse.
    - Scenario reale: Utile per analizzare tentativi di accesso remoto da parte di botnet.
3. Honeyd
    - Scopo e funzionalità: Crea reti virtuali per simulare infrastrutture complesse.
    - Utilità: Ideale per attirare attacchi di tipo network scan e studiare tecniche di ricognizione.
    - Scenario reale: Permette di simulare più dispositivi per analizzare attacchi distribuiti.

Log Generati dalle Honeypot

Dati registrati:

1. Indirizzi IP: Identificano gli attaccanti e la loro origine geografica.
2. Timestamp: Registrano l'orario preciso di ogni interazione.
3. Credenziali utilizzate: Rilevano username e password provati dagli attaccanti.
4. Comandi eseguiti: Mostrano le intenzioni e le tecniche dell'attaccante.
5. Payloads scaricati: Consentono l'analisi di malware o script dannosi utilizzati negli attacchi.

Valore per l'analisi forense:

1. Individuazione delle TTP: Identificare i modelli di comportamento degli attaccanti.
2. Correlazione di eventi: Collegare tentativi di attacco a campagne di minacce più ampie.
3. Identificazione di botnet: Analizzare script automatizzati e IP di comando e controllo (C&C).
4. Studio dei malware: Permette di isolare ed esaminare i payload dannosi utilizzati.

Le honeypot non sono solo trappole per gli attaccanti, ma strumenti cruciali per comprendere e prevenire le minacce avanzate.