HONEYPOT

Gli honeypot sono sistemi di sicurezza informatica progettati per attirare e ingannare potenziali attaccanti, simulando vulnerabilità reali o falsi obiettivi all'interno di una rete. Il loro scopo principale è quello di monitorare, rilevare e studiare i comportamenti degli attaccanti, raccogliendo informazioni su metodi, strumenti e tecniche utilizzati, senza compromettere i sistemi reali. In sostanza, gli honeypot funzionano come trappole digitali, inducendo gli aggressori a rivelare i loro tentativi di intrusione.

Gli honeypot si suddividono in due categorie principali:

- di produzione: sono utilizzati come difesa attiva dalle grandi aziende per ingannare gli hacker e tenerli alla larga dalla rete principale. Le aziende utilizzano i dati raccolti durante questa violazione “controllata” per eliminare eventuali punti deboli presenti nei loro sistemi di difesa e proteggere meglio la rete reale dai tentativi di hacking.
- di ricerca: sono trappole complesse utilizzate solitamente dai governi o dalle grandi società di sicurezza informatica per monitorare lo sviluppo delle minacce persistenti avanzate e rimanere al passo con l’evoluzione delle tecniche di hacking.

Tipi di honeypot:

- a bassa interazione. Emula soltanto alcune parti del sistema che vuole proteggere, solitamente le più ambite. Per questo motivo, richiede un impiego di risorse ridotto rispetto agli honeypot ad alta interazione, ed è anche più semplice da gestire. Tuttavia, è più facilmente riconoscibile da parte degli hacker, quindi potrebbe non essere in grado di ottenere molte informazioni sulla loro identità. Generalmente si tratta di una buona soluzione per individuare attacchi automatici e di basso livello, come quelli eseguiti da bot e worm, ma meno efficace contro attacchi più sofisticati.
- ad alta interazione. Imita in tutto e per tutto il sistema che vuole proteggere e può contenere alcuni dati e informazioni reali per essere più convincente. Richiede molte risorse per essere gestito e, per questo, solitamente viene implementato su macchine virtuali, che permettono di isolare meglio gli honeypot dal sistema reale. Questo tipo di honeypot è più difficile da riconoscere, quindi è molto efficace anche contro attacchi da parte di hacker più abili, ma è anche quello che presenta più rischi. Se non adeguatamente isolato, infatti, un honeypot ad alta interazione potrebbe fare da gateway per l’accesso all’effettivo sistema che si vuole proteggere.

Come funzionano:

1. Creazione dell'illusione di vulnerabilità: l'honeypot simula vulnerabilità, come un server mal configurato, una porta aperta o un servizio vulnerabile. Questi segnali attirano gli attaccanti.
2. Intercettazione dell'attacco: Quando un hacker interagisce con l'honeypot, tutte le sue azioni vengono monitorate e registrate. L'attaccante crede di essere entrato in un sistema reale, ma in realtà sta operando su una piattaforma controllata.
3. Raccolta di dati: Ogni attività dell'attaccante, comprese tecniche di intrusione, exploit utilizzati e altre azioni, viene registrata. Questo aiuta gli esperti di sicurezza a comprendere le tattiche degli attaccanti e a migliorare le difese.
4. Prevenzione e difesa: Anche se gli honeypot non sono progettati per bloccare direttamente gli attacchi (come fanno i firewall o gli antivirus), aiutano le organizzazioni a migliorare le loro difese rilevando nuove minacce e vulnerabilità.

Gli honeypot hanno un basso tasso di falsi positivi. Questo è in netto contrasto con i tradizionali sistemi di rilevamento delle intrusioni (IDS), che presentano invece un alto livello di falsi allarmi. Ancora una volta, questo aiuta ad assegnare le giuste priorità e mantiene la richiesta di risorse dall'honeypot a un basso livello. Aggiungiamo che sfruttando i dati raccolti dagli honeypot e correlandoli con altri registri di sistema e del firewall, gli IDS possono venire configurati con allerte più rilevanti, per produrre un minor numero di falsi positivi. In questo modo, gli honeypot possono aiutare a rifinire e migliorare gli altri sistemi di sicurezza informatica.

Sebbene la cybersecurity dell'honeypot aiuterà a delineare l'ambiente della minaccia, l'unico attacco che potrà vedere è quello rivolto contro se stessa. Solo perché una minaccia non è stata rivolta contro l'honeypot, questo non significa che non esista. È comunque importante restare al passo con le novità nel campo della sicurezza informatica e del cybercrimine.