# Gli Honeypot nella Cybersecurity

Gli Honeypot nella Cybersecurity: Uno Strumento tra Inganno e Difesa

Nel mondo digitale, dove le minacce informatiche sono in costante evoluzione, difendersi non significa
soltanto proteggersi, ma anche imparare dai propri avversari. È qui che entrano in gioco gli honeypot,
sistemi progettati come vere e proprie "trappole" per attirare gli hacker e raccogliere informazioni preziose.
Il concetto è affascinante e strategico: farsi attaccare per capire meglio come difendersi.

Cos'è un Honeypot?
Un honeypot è un sistema o risorsa informatica configurata per sembrare vulnerabile. Gli attaccanti,
credendo di poter sfruttare facilmente queste falle, interagiscono con il sistema, fornendo dati cruciali su
tecniche, strumenti e comportamenti. In realtà, ciò che viene simulato è un ambiente controllato, monitorato
costantemente per raccogliere informazioni utili. Ad esempio, immagina una porta SSH che invita tentativi
di accesso: ogni comando inviato e ogni password tentata sono registrati.

Tipologie di Honeypot
Gli honeypot si distinguono per complessità e scopo:

1. Bassa Interazione: Sistemi semplici che imitano un servizio specifico, come un server web o una

porta

aperta. Sono sicuri, ma raccolgono dati limitati.

2. Alta Interazione: Sistemi complessi che simulano intere infrastrutture IT. Un attaccante può "giocare"

nel sistema, permettendo ai difensori di osservare ogni dettaglio del suo approccio. Questi honeypot sono

più rischiosi, ma estremamente informativi.

3. Honeynets: Simulano intere reti di dispositivi con interazioni realistiche. Gli attacchi osservati possono

aiutare a sviluppare strategie di protezione per la rete reale.

Applicazioni Avanzate

Gli honeypot non sono solo strumenti passivi: possono essere utilizzati attivamente in contesti complessi

per raccogliere dati strategici. Ad esempio, per rilevare attacchi zero-day, monitorare botnet o studiare

il comportamento degli attaccanti.

Honeypot e Machine Learning

Gli honeypot possono integrare tecnologie di intelligenza artificiale per automatizzare l'analisi dei dati

raccolti. Questo consente di identificare pattern di attacco ricorrenti, correlare gli attacchi a specifiche

campagne criminali e riconoscere varianti di malware.

## Valore dei Log Generati

I log prodotti da un honeypot non sono semplici file di testo: rappresentano dati ricchi di informazioni per l'analisi forense e la sicurezza proattiva. Questi includono IP, timestamp, comandi eseguiti e movimenti nella rete.

## Esempi Reali di Utilizzo

Gli honeypot sono stati utilizzati in numerosi casi, come attacchi contro ospedali, rilevamento di malware bancario o protezione contro botnet come Mirai.

## Considerazioni Etiche

L'uso degli honeypot solleva anche questioni etiche e legali, come la responsabilità in caso di danni causati da un attaccante che utilizza l'honeypot come trampolino.

## Conclusione

Gli honeypot sono strumenti potenti per comprendere e contrastare le minacce informatiche. Se ben implementati, possono trasformare le vulnerabilità apparenti in una fonte di forza strategica per la cybersecurity.