# RELAZIONE HONEYPOT

L'honeypot, letteralmente "vaso di miele", è un sistema esca (PC o server) progettato per attirare e ingannare gli attaccanti, deviandoli da obiettivi reali e fornendo informazioni preziose sulle loro tattiche e strumenti. Sebbene il concetto di honeypot risalga agli anni '80, il suo utilizzo si è evoluto con il panorama delle minacce informatiche, diventando uno strumento essenziale per la difesa proattiva.

## Posizionamento Strategico dell'Honeypot nella Rete

La posizione dell'honeypot all'interno della rete è cruciale per la sua efficacia. Esistono due principali approcci:

- **Honeypot di produzione:** Installato all'interno della rete di produzione, simulando un sistema reale e attraente per gli attaccanti. Questa configurazione offre una visione diretta delle tattiche degli attaccanti in un ambiente reale, ma comporta un rischio maggiore in caso di compromissione.
- **Honeypot di ricerca:** Isolato dalla rete di produzione, spesso in una DMZ o in un ambiente cloud dedicato. Questa configurazione riduce i rischi, ma potrebbe non riflettere accuratamente gli attacchi reali.

La scelta dipende dagli obiettivi specifici:

- **Rilevamento e analisi delle minacce:** Un honeypot di produzione può fornire informazioni dettagliate sulle tattiche degli attaccanti in tempo reale.
- **Distrazione e ritardo:** Un honeypot, indipendentemente dalla posizione, può deviare gli attaccanti da obiettivi critici, guadagnando tempo per la risposta agli incidenti.
- **Ricerca e sviluppo:** Un honeypot di ricerca può essere utilizzato per studiare nuovi malware e tecniche di attacco in un ambiente controllato.

## Implementazione nella Nostra Topologia di Rete

Nella nostra topologia di rete, per evitare eccessivi rischi, la proposta è di installare l’honeypot nella nostra DMZ, collegato al firewall che impedisca qualunque tipo di traffico proveniente dal server esca. Gli “zero day” e gli attacchi rilevati possono essere utilizzati per aggiornare il database del nostro NIPS.

## Scelta dell'Honeypot: Canary

La nostra scelta è ricaduta su Canary, sviluppato da Thinkst Applied Research, un honeypot ad alta interazione noto per la sua capacità di rilevare attacchi sofisticati e fornire informazioni dettagliate sull’attività degli attaccanti.