Honeypot

Docente: Marzia De Maina

Contenuti

I - Introduzione

Ci troviamo in un mondo digitale sempre più esposto a **minacce esterne**.

Esploriamo uno **strumento di difesa**, usato per ingannare gli attaccanti e studiare il loro comportamento: gli **honeypot.**

Big 💡 Idea

La sicurezza non è uno stato
ma un processo.

II - Cos’è un honeypot?

Si tratta di un sistema informatico progettato per **attirare potenziali attaccanti** e **registrare il loro comportamento** a fini di analisi e difesa. Due o più honeypot formano un **Honeynet**.

🔍 Curiosità

Honeypot significa letteralmente **barattolo di miele**: attrae l’attaccante come il miele attrae l’orso, offrendo un'esca dolce ma insidiosa.

Big 💡 Idea

Osservare senza intervenire permette di raccogliere dati preziosi.

III - Funzioni principali

A cosa serve un honeypot?

- **rileva gli attacchi**;
- **raccoglie informazioni** sugli attaccanti e sulle modalità di attacco;
- **allonta gli attaccanti** dalla rete reale;
- **studia gli argomenti** di interesse degli attaccanti;
- aiuta gli amministratori di sistema a **migliorare le strategie di sicurezza** della rete reale;
- **aiuta a studiare eventuali minacce** già presenti nella rete;
- **individua la provenienza delle minacce**.

IV - Tipologie per interazione

ALTA INTERAZIONE

Simula il più possibile un sistema completo

L’attaccante ha massima libertà di azione

MEDIA INTERAZIONE

Simula servizi più complessi (es. database)

Registra ogni input dell’attaccante

Tra i comandi possibili: login, query, comandi fittizi

BASSA INTERAZIONE

Simula solo pochi servizi di rete (es. finta pagina web)

È una semplice esca: serve solo a verificare che qualcuno stia abboccando

---

È sicuro ma raccoglie poche informazioni

Sintesi delle tipologie per interazione

Tipologia	Complessità di implementazione	Quantità di dati raccolti	Livello di sicurezza	Uso ideale
Alta Interazione	ALTA	ALTA	*MOLTO RISCHIOSA	Ricerca avanzata
Media Interazione	MEDIA	MEDIA	MEDIA	Studio generico
Bassa Interazione	BASSA	BASSA	ALTA	Esche

***deve essere ben isolato dal sistema reale**

V - Tipologie per utilizzo

HONEYPOT DI RICERCA

raccoglie informazioni (bassa o media interazione)

identifica le compromissioni nella rete interna e inganna l'attaccante (alta interazione)

HONEYPOT DI PRODUZIONE

VI - Logging

Come viene registrata l’attività degli honeypot?

Ogni interazione viene **tracciata e custodita** nei file di log:

- **registrano tutti gli accessi** con timestamp, IP sorgente e comando inviato;
- **ricostruiscono la catena dell’attacco**;
- permettono di **riconoscere i pattern ricorrenti** e di **analizzare gli strumenti** e **il percorso** utilizzati dall’attaccante.

Big 💡 Idea

Ogni azione in rete lascia tracce: ogni comportamento é tracciabile e analizzabile attraverso un logging continuo

Esempio di file di log

```
[2025-06-06 10:23:18] Incoming connection from 192.167.215.12 on port 22 (SSH)
[2025-06-06 10:23:19] Attempted login with username: root
[2025-06-06 10:23:20] Failed password for root from 192.167.215.12
[2025-06-06 10:23:23] Attempted login with username: admin
[2025-06-06 10:23:24] Failed password for admin from 192.167.215.12

[2025-06-06 10:24:15] Incoming connection from 192.167.215.12 on port 80 (HTTP)
[2025-06-06 10:24:16] GET /admin/login.php HTTP/1.1
[2025-06-06 10:24:17] Response: 403 Forbidden
```

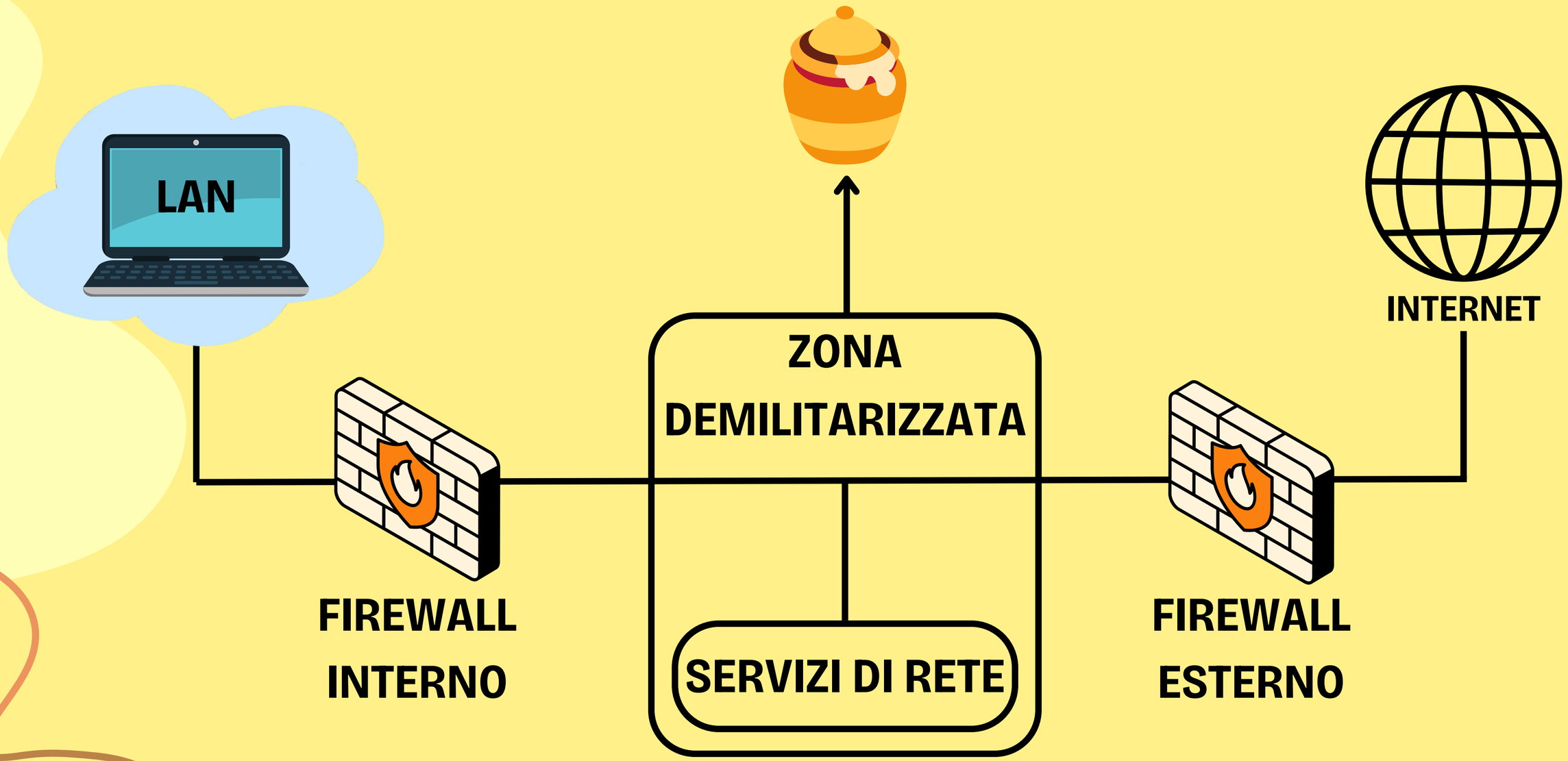
Big 💡 Idea

La comunicazione in un sistema digitale avviene per mezzo di protocolli.

VII - Esempi

- **HONEYPOT DI POSTA ELETTRONICA** → indirizzi fittizi
- **HONEYPOT DI DATI** → database, cartelle di file
- **HONEYPOT PER I MALWARE** → applicazioni, API
- **SPIDER HONEYPOT** → pagine web, link
- **CLIENT HONEYPOT** → dispositivi lato client che attirano i server dannosi

VIII - Posizionamento in una rete



IX - Pro vs Contro

PRO	CONTRO
Basso tasso di falsi positivi	Trampolino per altri attacchi se mal configurato
Migliore strumento per il continuo monitoraggio degli attacchi	Se è troppo semplice, è facilmente riconoscibile dagli attaccanti esperti
Individua le vulnerabilità del proprio sistema di sicurezza	Non è uno strumento di attacco

Bibliografia

📚 **William Stallings e Lawrie Brown (2015)**
***Computer security: principles and practice*, Pearson**

📚 **Keith W. Ross e James F Kurose (2012)**
***Computer networking*, Pearson Education**

📚 **Abhishek Mairh et al. (2011)**
“*Honeypot in network security: a survey*” in: *Proceedings of the 2011 international conference on communication, computing & security*

💻 **Francesco La Trofa**
Cos’è e come viene utilizzato un Honeypot
url: https://universeit.blog/honeypot/
visitato il 30/06/2025