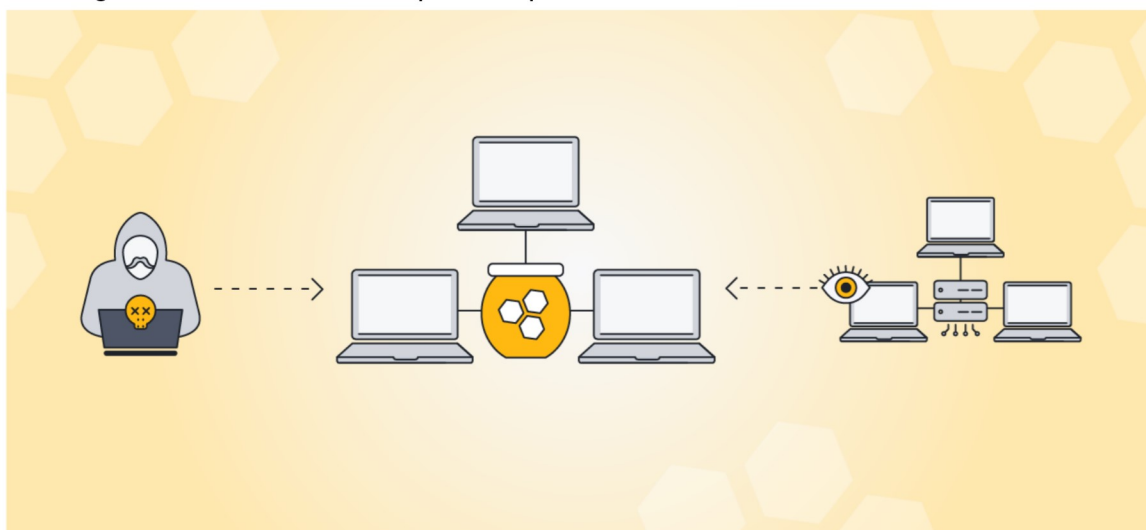


# Ricerca sulle Honeypot per il Corso di Cybersecurity

## Introduzione alle Honeypot

Le honeypot sono trappole digitali create per attirare, rilevare e studiare le attività malevoli di attaccanti informatici. Questi sistemi, che appaiono come vulnerabili o contenenti dati sensibili, in realtà sono progettati come strumenti di difesa usati per raccogliere informazioni sugli attaccanti, analizzare il loro comportamento e sviluppare contromisure contro minacce future. Sebbene le honeypot siano oggi parte integrante delle strategie di cybersecurity, la loro origine risale agli anni '80, con una delle prime implementazioni attribuita a Clifford Stoll.



## La Prima Honeypot: Clifford Stoll e il Caso di Markus Hess (1986)

Nel 1986, Clifford Stoll, un amministratore di sistemi al Lawrence Berkeley National Laboratory in California, si imbatté in una piccola discrepanza finanziaria di 75 centesimi nei registri del sistema di fatturazione. Questa apparente incongruenza si rivelò essere il primo segnale di un accesso illegale ai sistemi del laboratorio. L'intruso sfruttava una vulnerabilità per accedere a informazioni sensibili su progetti governativi e militari.

Dopo aver notato che l'hacker si connetteva ai sistemi del laboratorio durante la notte, Stoll decise di creare una trappola. Progettò un sistema vulnerabile che sembrava contenere dati riservati, ma che in realtà non aveva alcun valore. Questa prima honeypot era un sistema fisico che attivava un allarme quando l'hacker si collegava. Grazie a questa trappola, Stoll fu in grado di tracciare e monitorare l'attività dell'intruso per diverso tempo.

Alla fine, l'hacker fu identificato come Markus Hess, un cittadino tedesco che vendeva informazioni all'Unione Sovietica. Questo caso non solo portò all'arresto di Hess, ma evidenziò

per la prima volta l'importanza degli strumenti di monitoraggio per la sicurezza informatica, ponendo le basi per le honeypot moderne.

## Evoluzione delle Honeypot

### Anni '90: L'Inizio dell'Automazione

Con l'avvento di internet negli anni '90, le honeypot si sono evolute da strumenti rudimentali a sistemi più sofisticati. Durante questo periodo, furono create le prime versioni automatizzate delle honeypot, progettate per ridurre l'intervento umano e monitorare gli attaccanti su larga scala. Un esempio importante di questa evoluzione fu il **Honeynet Project**, avviato nel 1999, che introdusse il concetto di "honeynet", una rete di honeypot collegati che consentono di monitorare attacchi complessi e simultanei su più sistemi.

In questo periodo, le honeypot cominciarono a essere classificate in due categorie principali:

- **Honeypot ad alta interazione:** Simulano completamente sistemi reali, permettendo agli attaccanti di interagire liberamente con il sistema. Queste honeypot offrono la possibilità di raccogliere un'enorme quantità di informazioni sul comportamento degli attaccanti, ma comportano anche rischi elevati poiché l'attaccante potrebbe sfruttare il sistema per sferrare attacchi ad altre infrastrutture.
- **Honeypot a bassa interazione:** Limitano le interazioni consentite agli attaccanti, monitorando solo alcune attività come tentativi di connessione e scansione delle porte. Questi sistemi sono più sicuri rispetto alle honeypot ad alta interazione, ma forniscono meno informazioni dettagliate.

### Anni 2000: Espansione e Diversificazione

Con la crescente diffusione di internet e la proliferazione delle minacce informatiche, le honeypot divennero parte integrante delle strategie di difesa informatica durante gli anni 2000. Oltre a rilevare attacchi, vennero utilizzate per studiare e prevenire minacce emergenti, come botnet e worm.

- **Code Red Worm (2001):** Questo worm infettò migliaia di server web Microsoft IIS. Le honeypot furono cruciali per lo studio del comportamento del worm e per lo sviluppo di contromisure in grado di mitigare i danni causati dall'infezione. La diffusione del worm dimostrò l'importanza di avere honeypot in grado di monitorare gli attacchi su scala globale.
- **ICS Honeypot:** Durante questo periodo, le honeypot furono impiegate anche per proteggere infrastrutture critiche come impianti industriali e centrali elettriche. Queste "honeypot industriali" (ICS Honeypot) furono create per monitorare e studiare attacchi rivolti ai sistemi di controllo industriale (ICS), che controllano operazioni come la produzione di energia.

Un altro sviluppo chiave in questo periodo fu la diversificazione delle honeypot in base al tipo di attacco e alla piattaforma utilizzata. Le honeypot divennero fondamentali per monitorare non solo le reti aziendali ma anche infrastrutture critiche, dispositivi IoT e sistemi basati su cloud.

TERMS	Types of Honeypots	Services Supported	Log File Support	Platform Support	Notification Capability
TOOLS					
Netbait	Production honeypots and Research honeypots	TCP or UDP	Yes, it logs all the activities of the attackers.	Macintosh, Linux and window operating system	It uses logging as well as alerting mechanism
Mantrap	High interaction honeypots	It uses the cage services that are used for creating mirror copies of master OS	Yes	Run on virtual system	It provides stealth monitoring with outstanding notification capability
Specter	Medium interaction honeypots	FTP, SMTP, POP3, HTTP, and TELNET	Yes	Window XP	Outstanding notification capability
KFsensor	Low interaction honeypots	Testing for open proxy servers, Dameware, myDoom and blaster worm detection.	Yes	Window based operating system	It uses logging as well as alerting mechanism
BackOfficer friendly	Low interaction honeypots	It supports http, ftp, telnet or mail in total 7 services.	No, it does not log the methods used by the attackers rather it response instantly.	Run on any windows including windows 95 and windows 98	No remote logging, alerting or configuring personality
Bait n Switch	Production honeypots	It monitors network activities.	Yes	Run on Linux operating system	It uses logging as well as alerting mechanism
Labrea Tarpit	Low interaction honeypots	Stop the automated attack by scanning the network for unused IP addresses, capturing them and marked them as spam.	Yes	Run on Ubuntu operating system	It uses logging as well as alerting mechanism
Honeyd	Low interaction honeypots	Immunization from worm and spam	Yes	Window and Linux operating system	No built in mechanism for alerting
Deception toolkit	High interaction honeypots	DTK uses TCP wrapper service in order to block unusual traffic on active ports.	Yes	Executes on Linux and Window based operating system	It uses logging as well as alerting mechanism

## Honeypot Moderne

Con l'avvento del cloud computing e la continua evoluzione delle tecnologie informatiche, le honeypot moderne sono diventate più sofisticate e sono utilizzate in una vasta gamma di scenari. Esse si adattano a nuove minacce come il ransomware, il furto di dati, e gli attacchi distribuiti (DDoS), rappresentando una linea di difesa attiva e proattiva per le infrastrutture.

- **Honeypot di rete:** Simulano intere reti di computer, creando un ambiente realistico per attrarre gli attaccanti e monitorare comportamenti dannosi. Queste honeypot vengono utilizzate, ad esempio, per studiare attacchi di tipo ransomware o DDoS (Distributed Denial of Service).
- **Honeyfiles e Honeytokens:** Questi file o frammenti di dati falsi sono progettati per attrarre attacchi mirati. Quando un attaccante tenta di accedere o manipolare questi file, il sistema rileva l'intrusione e raccoglie informazioni preziose sull'attacco.
- **Honeypot nel cloud:** Con la crescita delle infrastrutture cloud, le honeypot sono state adattate per monitorare e studiare attacchi rivolti a servizi cloud. Questi sistemi permettono di proteggere ambienti virtuali e distribuiti in rete, che oggi rappresentano una grande fetta dell'infrastruttura informatica globale.
- **Honeypot virtuali:** Simulano macchine virtuali, rappresentando un sistema apparentemente reale per attirare e analizzare attacchi in ambienti virtualizzati.



- **Honeypot client (o honeyclient):** Simulano sistemi client vulnerabili, come browser o email clients, e vanno attivamente alla ricerca di server malevoli, a differenza delle honeypot tradizionali che agiscono come server in attesa di attacchi.




## Casi Interessanti di Honeypot

Alcuni esempi significativi di attacchi studiati grazie all'utilizzo di honeypot includono:

- **Worm Code Red (2001):** Come menzionato in precedenza, le honeypot giocarono un ruolo essenziale nel monitorare e mitigare l'effetto di questo worm su server web a livello mondiale.
- **Progetto Ghostnet (2009):** Ghostnet era una rete globale di sorveglianza che sfruttava malware per infiltrarsi in computer situati in più di 100 paesi. Le honeypot furono fondamentali per raccogliere prove e monitorare gli attacchi ai sistemi compromessi.
- **Stuxnet (2010):** Sebbene scoperto attraverso altre tecniche, le honeypot industriali furono utilizzate per comprendere meglio la minaccia di Stuxnet e il suo impatto sui sistemi di controllo industriale (ICS). Questo caso rappresenta un esempio cruciale di come le honeypot possano essere impiegate per proteggere infrastrutture critiche.
- **Mirai Botnet (2016):** Una delle più grandi botnet mai create, Mirai sfruttò dispositivi IoT vulnerabili per condurre attacchi DDoS di ampia scala. Grazie a honeypot distribuite, i ricercatori furono in grado di catturare dispositivi compromessi e studiare come disabilitarli.

## Altri Esempi di Honeypot

-  **Email honeypot (o spam traps):** Sono finti indirizzi email creati appositamente per attirare attaccanti e ricevere spam. Il falso indirizzo email viene solitamente collocato in una posizione "nascosta" dove solo un raccoglitore automatico di indirizzi email (o harvester) può individuarlo. Questo significa che nessun utente legittimo può individuare quell'indirizzo email, il che evita l'incidenza di falsi positivi negli alert. Aiutano a evitare che lo spam o email malevole vengano inviate a indirizzi email legittimi, poiché tutti i messaggi aventi lo stesso contenuto di quelli inviati alla honeypot verranno automaticamente bloccati e l'IP del mittente aggiunto a una blacklist. Sono utili per lo studio di campagne di spam, tentativi di phishing e allegati dannosi.
-  **Database honeypot:** Contengono dataset fittizi e vulnerabili disegnati per attirare attaccanti che riescano a bucare i firewall. Vengono utilizzate per monitorare i tipi e le occorrenze di attacchi ai danni dei database. Ad esempio, possono raccogliere informazioni riguardo le SQL injections, vulnerabilità dei software, privilege abuse e altri metodi utilizzati per ottenere l'accesso ai database, oltre a essere utilizzati per analizzare come i dati rubati nell'attacco vengano utilizzati nelle fasi successive.
-

-  **Malware honeypot:** Imitano le app software e le API per attrarre attacchi malware. Sono utili nell'individuazione di vulnerabilità delle API e ai fini dell'implementazione di software anti-malware.
- 
-  **Spider honeypot:** Creano delle pagine web e dei link cui solo i web crawler (o spiders) o i bot possono accedere, dando agli analisti la possibilità di studiare la maniera in cui bot malevoli e ad-network crawler operano, nonché i potenziali rischi e minacce per l'organizzazione.
- 
-  **HoneyBot:** Sviluppato da un gruppo di ricercatori della Georgia Tech's School of Electrical and Computer Engineering, l'HoneyBot è un robot connesso alla rete che può essere hackerato in pochi secondi e risponde ai comandi di un attaccante, inviando una risposta simulata senza però completare l'azione. Allo stesso tempo, il dispositivo avverte immediatamente di un attacco hacker in corso, permettendo al team di cyber security di rispondere all'attacco.

## Benefici e Rischi nell'Utilizzo delle Honeypot

### Benefici:

- **Rilevamento delle vulnerabilità:** Identificano le debolezze in servizi e applicazioni.
- **Riduzione dei falsi positivi:** Monitorano solo attacchi malevoli, limitando gli alert non necessari.
- **Costi contenuti:** Possono essere implementate con risorse hardware minime e software open source.
- **Strumento di formazione:** Offrono un ambiente sicuro per simulare e studiare attacchi.
- **Difesa proattiva:** Identificano vulnerabilità sconosciute e dirottano attacchi lontano dai veri obiettivi.
- **Rilevamento di minacce interne:** Monitorano anche azioni dannose da parte di dipendenti.

### Rischi:

- **Riconoscimento da parte degli attaccanti:** Hacker esperti potrebbero accorgersi di essere di fronte a una honeypot.
- **Rischio di compromissione:** Una honeypot mal configurata potrebbe fornire un accesso agli attaccanti ai sistemi reali.
- **Manutenzione continua:** Le honeypot devono essere aggiornate costantemente per rimanere efficaci.
- **Limitazioni nei dati raccolti:** Possono fornire informazioni solo su attacchi mirati alle honeypot stesse.

## **L'Avvento della Deception Technology e l'Intelligenza Artificiale**

Oltre alle tradizionali honeypot, nuove tecnologie come l'intelligenza artificiale stanno ridefinendo il panorama della cybersecurity. Un esempio è il sistema **DeepDig (DEcEption DIGging)**, sviluppato dall'University of Texas, che sfrutta il Deep Learning per studiare attacchi e "insegnare" agli IDS (Intrusion Detection Systems) come prevenirli.

## **Conclusione**

Le honeypot sono diventate uno strumento essenziale nella cybersecurity moderna. Offrono alle organizzazioni un modo efficace per rilevare attacchi, studiare le tecniche degli attaccanti e migliorare le difese. Mentre le tecnologie si evolvono, le honeypot continueranno a svolgere un ruolo cruciale nella protezione delle infrastrutture informatiche, contribuendo a creare un ambiente digitale più sicuro.