Università degli studi di Modena e Reggio Emilia
Dipartimento di Scienze Fisiche, Informatiche e Matematiche

Corso di Laurea in Informatica

Strategie Innovative di Sicurezza Informatica: monitoraggio delle reti grazie a Darktrace e Tpot

Relatore:
Prof. Ferretti Luca

Candidato:
Matteo Violi

Anno Accademico 2023/2024

Indice

Capitolo 1

Introduzione

1.1 Contestualizzazione del tirocinio curricolare universitario

1.2 Scopo delle tesi

Capitolo 2

Fondamenti teorici su Honeypot e IDS

2.1 Introduzione agli honeypot

2.1.1 Definizione e scopo

Nel 1989, Clifford Stoll pubblica quello che poi diventerà uno dei classici della letteratura sulla sicurezza informatica: **The Cuckoo's Egg**. Nel romanzo, Stoll racconta di aver scoperto un tentativo di intrusione informatica nei sistemi del laboratorio del Lawrence Berkeley National Laboratory, dove lavorava come astrofisico.
Analizzando delle discrepanze sulle fatture di addebito per l'uso di risorse informatiche e cercando di capirne la causa, Stoll inizia a seguire le tracce digitali lasciate, le quali lo condurranno fino a un hacker. Quest'ultimo si rivelò essere Markuss Hess, hacker tedesco famoso per aver violato sistemi più di quattrocento sistemi dell'esercito americano per poi vendere tutte le informazioni ai servizi di intelligence sovietici.
Hess venne scoperto grazie a un'idea di Stoll: un finto portale vulnerabile del Lawrence Berkeley National Laboratory. Questo gli permise di stabilire una connessione e localizzare il criminale. Stoll definì questa sua creazione una *hoax*, una sorta di burla o truffa.
Uno dei primi documenti che trattava l'uso di trappole per attirare hacker malevoli fu redatto da William Cheswick, un pioniere della sicurezza informatica e l'ideatore di uno dei primi firewall. Cheswick creò quello che in quell'epoca chiamò "roach motel", una trappola progettata per intrappolare gli hacker, ispirandosi alla metafora di un motel per scarafaggi.
Nel corso degli anni, il termine *honeypot* ha guadagnato sempre più popolarità, in quanto associato alla tradizione folkloristica dei popoli germanici, slavi e celtici. Secondo questa tradizione, gli orsi tendono a rubare il miele dagli alveari, un parallelismo che riflette l'idea di attirare e intrappolare gli 'hacker' simili a predatori.
In generale, un honeypot è costituito da un sistema informatico che simula un sistema legittimo, rendendolo vulnerabile ai più comuni attacchi informatici. L'obiettivo è di deviare l'attaccante dalle macchine reali e critiche, consentendo nel contempo lo studio dei loro comportamenti e delle tecniche di attacco durante e dopo la fase di *exploitation*.

2.1.2 Tipologie di honeypot

Dal momento della loro concezione, possiamo categorizzare le diverse tipologie di honeypot in base alle risorse allocate o al contesto di utilizzo.
Per quanto riguarda le risorse, possiamo suddividerli in due categorie principali:

- **Honeypot Fisici**: Questi utilizzano macchine reali con indirizzi IP dedicati, simulando comportamenti modellati dal sistema. Tuttavia, questo modello è raramente adottato a causa dell'alto costo di acquisizione, manutenzione e delle specifiche esigenze hardware.

- **Honeypot Virtuali**: Questa tipologia consente l'installazione e la simulazione di un host sulla rete, assegnando un indirizzo IP alla macchina virtuale. Questo approccio è il più diffuso, offrendo un equilibrio tra efficacia e praticità.

Per quanto riguarda il contesto di utilizzo, possiamo distinguere:

- **Honeypot di Produzione**: Questi honeypot sono progettati per un utilizzo semplice, immagazzinano un numero limitato di informazioni e sono spesso implementati in contesti aziendali. Collocati all'interno della rete aziendale insieme agli altri server di produzione, raccolgono meno dati e operano a bassa intensità.

- **Honeypot di Ricerca**: Questi honeypot sono finalizzati alla raccolta di informazioni sulle metodologie di attacco degli aggressori. Non forniscono un valore specifico a un'organizzazione particolare, ma sono più complessi da installare e mantenere, raccogliendo un'ampia quantità di dati.

Recentemente, il mercato legato a questi servizi ha introdotto nuove tipologie di honeypot che estendono le funzionalità di base e incorporano tecniche di inganno, automatizzando la scalabilità su grandi reti. Le tipologie più diffuse includono:

- **Honeypot malware**: Questi honeypot simulano un sistema vulnerabile agli attacchi più comuni da parte di malware, consentendo uno studio approfondito del malware, delle sue origini e del suo comportamento.

- **Honeypot spam**: Questi honeypot simulano relay di posta aperti o proxy aperti, comunemente utilizzati dagli spammer. Ciò consente di rivelare l'indirizzo IP dello spammer e fornire una cattura in blocco dello spam.

- **Honeypot database**: Questi honeypot simulano database con possibili vulnerabilità, come ad esempio SQL Injection.

- **Honeypot ICS**: Questi honeypot simulano sistemi di controllo industriale come i PLC (controller logico programmabile).

2.1.3 Tpot: panoramica

2.1.4 Tpot: scopo e utilità in ambiente di tirocinio

2.2 Teoria sugli IDS

2.2.1 Evoluzione e storia degli IDS

Il primo concetto preliminare di sistema di rilevamento delle intrusioni (IDS) è stato descritto nel 1980 da James Anderson presso la National Security Agency e comprendeva un insieme di strumenti per gli amministratori per esaminare i registri di audit. Nel febbraio del 1987, Dorothy E. Denning, assistita da Peter G. Neumann presso IDS International, pubblicò un documento intitolato "An Intrusion Detection Model".
Questo modello presentava un sistema esperto basato su regole per rilevare pattern di intrusioni note e una componente di rilevazione statistica basata su profili di utenti, sistemi host e sistemi di destinazione, diventando noto come Intrusion Detection Expert System.
Nel 1993, Teresa F. Lunt, autrice di "IDES: An Intelligent System for Detecting Intruders", aggiunse l'ultimo componente al modello di Denning: una rete neurale artificiale capace di adattarsi agli eventi e modificarsi.
Un sistema di rilevamento delle intrusioni (IDS) è un dispositivo software o un'applicativo che monitora una rete o i dispositivi su cui è installato. Quando rileva un'anomalia, la segnala a un sistema di raccolta di eventi di sicurezza (SIEM), che utilizza tecniche di filtraggio degli allarmi per distinguere falsi positivi da attività dannose.
Gli IDS, come un firewall, vengono utilizzati per prevenire intrusioni nella rete, ma differiscono dalla risposta a tali intrusioni. I sistemi di rilevamento delle intrusioni possono anche avere scopi specifici integrandoli con strumenti personalizzati, come l'utilizzo di un honeypot per attirare e caratterizzare il traffico dannoso.
Recentemente, alcuni prodotti IDS hanno la capacità di rispondere alle intrusioni rilevate, denominati sistemi di rilevamento e prevenzione delle intrusioni (IDPS). Gli IDPS aggiungono la capacità di fermare un attacco rilevato, registrare gli eventi, avvisare gli amministratori, bloccare la minaccia e generare rapporti. A differenza degli IDS, gli IDPS devono essere posizionati "in linea", monitorando in tempo reale per bloccare intrusioni, inviare allarmi, rifiutare pacchetti dannosi e correggere errori di rete.

2.2.2 Tipologie di IDS

La classificazione tipica dei sistemi di intrusione si basa sulla loro posizione:

- **NIDS (Network IDS)**: Posizionati strategicamente nella rete, monitorano il traffico da e verso tutti i dispositivi, analizzando idealmente sia l'entrata che l'uscita. L'uso di reti neurali artificiali può migliorare i tassi di rilevamento grazie alla capacità di analizzare grandi volumi di dati in modo intelligente e apprendere dagli errori, sviluppando un sistema di avviso precoce.

- **HIDS (Host IDS)**: Operano su singoli host o dispositivi, monitorando solo i pacchetti in entrata e in uscita. Consentono l'analisi del traffico di rete criptato, una volta arrivato all'host.

Gli IDS possono essere classificati anche in base all'approccio di rilevamento:

- **Signature-based**: Ricerca pattern specifici, simile all'azione degli antivirus per individuare sequenze di byte o istruzioni malevole conosciute. Risponde velocemente a attacchi noti, ma può non riconoscere nuovi attacchi senza pattern noti.
- **Anomaly-based**: Utilizza l'apprendimento automatico per creare un modello di attività affidabile e confrontare il nuovo comportamento. Riesce a rilevare attacchi sconosciuti, ma potrebbe generare falsi positivi, identificando attività legittime come malevoli.

2.2.3 Darktrace: panoramica

2.2.4 Darktrace: funzionamento

Capitolo 3

Sperimentazione con Tpot e Darktrace

3.1 Implementazione di Tpot e analisi dei risultati

3.1.1 Configurazione di base

3.1.2 Simulazione di server in produzione

3.1.3 Dati raccolti

3.1.4 Esperienze pratiche durante il tirocinio

3.2 Monitoraggio delle reti con Darktrace

3.2.1 Studi di caso

3.2.2 Esempi di minacce rilevate

3.3 Integrare Darktrace e Tpot per una maggiore sicurezza

Capitolo 4

Conclusioni

4.1 Riassunto delle principali conclusioni

4.2 Riflessioni personali sull'esperienza di tirocinio

4.3 Suggerimenti per future ricerche o sviluppi in questo ambito

Capitolo 5

Bibliografia

Capitolo 6

Ringraziamenti