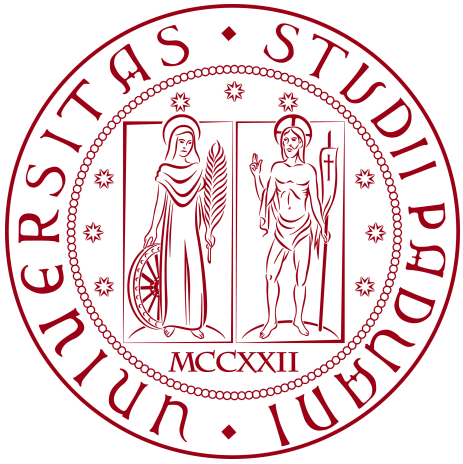
Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea in Informatica



Un sistema Honeypot per l'analisi di attacchi informatici in ambiente controllato

Tesi di Laurea

Relatore

Prof. Vardanega Tullio

Laureando

Marko Peric

Matricola 2011067

Anno Accademico 2024-2025

Ringraziamenti

Padova, Agosto 2025 *Marko Peric*

Sommario

Il presente elaborato descrive il lavoro svolto durante il periodo di stage, della durata di circa 320 ore, dal laureando Marko Peric presso l'azienda Eurosystem S.p.A. dal 18/06/2024 al 13/08/2025. L'elaborato illustra i processi, le metodologie e gli strumenti impiegati nella progettazione e nello sviluppo di un sistema *honeypot* finalizzato al monitoraggio e alla rilevazione di attività malevole in rete. Il sistema si basa sull'installazione di servizi volutamente vulnerabili su un server Linux Debian, con lo scopo di attirare potenziali attaccanti e analizzarne i comportamenti. I *log* generati dai servizi vengono successivamente raccolti, elaborati e trasferiti in InfluxDB per la loro conservazione, e resi disponibili tramite Grafana per consentire un'analisi e una visualizzazione efficace delle informazioni tramite *dashboard*.

Struttura dell'elaborato

In questa sezione viene presentata la struttura dell'elaborato, illustrando brevemente il contenuto di ciascun capitolo:

Il primo capitolo approfondisce il contesto aziendale in cui si è svolto lo *stage*, fornendo una panoramica completa dell'azienda, dei suoi prodotti e servizi nel settore della cybersecurity, degli strumenti tecnologici utilizzati e dell'organizzazione del team di sicurezza informatica, analizzando inoltre l'approccio dell'azienda verso l'innovazione tecnologica;

Il secondo capitolo identifica e analizza il problema alla base del progetto, definendo gli obiettivi specifici dello sviluppo del sistema *honeypot*, i vincoli operativi e tecnici che hanno influenzato il lavoro, le prospettive di

sviluppo futuro e le motivazioni personali che hanno guidato la scelta di questo percorso di stage;

Il terzo capitolo documenta l'intero processo di sviluppo del sistema honeypot, dall'analisi dei requisiti e dei casi d'uso alla progettazione dell'architettura, dalla fase di codifica alle attività di verifica e validazione, presentando il prodotto finale e valutando il grado di conformità rispetto ai requisiti iniziali;

Il quarto capitolo presenta una valutazione retrospettiva dell'esperienza formativa, analizzando il raggiungimento degli obiettivi prefissati, le conoscenze tecniche acquisite nel campo della sicurezza informatica e le competenze professionali sviluppate durante il periodo di tirocinio presso l'azienda.

Criteri tipografici adottati

Riguardo la stesura del testo, relativamente al elaborato sono state adottate le seguenti convenzioni tipografiche:

- gli acronimi e le abbreviazioni sono raccolti in un'apposita sezione dedicata, denominata Elenco degli acronimi e sono segnati con la seguente nomenclatura *Esempio di acronimo (ES)*$_G$;
- i termini ambigui o di uso non comune, invece, sono definiti all'interno del Glossario e sono segnati con la seguente nomenclatura *esempio di termine*$_G$;
- i termini in lingua straniera o facenti parti del gergo tecnico sono evidenziati con il carattere *corsivo*.

Indice

Elenco delle figure

Elenco delle tabelle

Elenco dei codici sorgenti

Capitolo 1

Contesto lavorativo

Il primo capitolo fornisce una panoramica sull'azienda ospitante Eurosystem S.p.A., evidenziando le principali aree operative dell'azienda.

1.1 L'azienda

Eurosystem S.p.A. è un'impresa informatica con sede principale a Villorba (TV), attiva nel settore della consulenza, dei prodotti e dei servizi IT. L'azienda è presente sul territorio nazionale con otto sedi operative, distribuite principalmente nel Nord Italia. Tra queste, la sede di Tavagnacco (UD) riveste un ruolo centrale in quanto ospita il reparto dedicato alle attività di *cybersecurity*, ambito in cui è stato svolto il tirocinio curricolare in modalità da remoto. Fondata con l'obiettivo di fornire soluzioni tecnologiche a supporto delle imprese, Eurosystem S.p.A. si rivolge prevalentemente al settore delle piccole e medie imprese, accompagnandole nei processi di digitalizzazione e nella gestione dei rischi informatici. L'azienda si caratterizza per un approccio che combina l'adozione di tecnologie consolidate con l'attenzione verso l'innovazione e la sicurezza delle infrastrutture digitali. Il reparto di *cybersecurity* si distingue per la sua funzione trasversale, in quanto collabora sia con i clienti sia con gli altri reparti aziendali, integrando misure di protezione all'interno delle soluzioni tecnologiche fornite. L'attenzione di Eurosystem S.p.A. non è rivolta unicamente alla fornitura di servizi, ma anche al mantenimento e all'aggiornamento costante delle competenze del personale. La formazione continua rappresenta un elemento fondamentale:

nei periodi di minore operatività, i team dedicano tempo allo studio di nuove tematiche, all'analisi di strumenti emergenti e alla sperimentazione di metodologie utili a fronteggiare l'evoluzione costante delle minacce informatiche.

1.2 Prodotti e servizi offerti

Eurosystem S.p.A. offre una gamma di prodotti e servizi informatici pensati per garantire la protezione delle infrastrutture IT aziendali. In particolare, il reparto di *cybersecurity* si occupa delle seguenti attività principali:

- **Monitoraggio e risposta agli incidenti**: tramite il *Security Operation Center* (SOC) e i servizi di *Managed Detection and Response* (MDR), viene assicurato un monitoraggio continuo delle reti aziendali, con l'obiettivo di rilevare anomalie e possibili minacce in tempo reale. Ogni incidente viene analizzato in profondità attraverso:
  - raccolta e analisi dei log e dei dati di rete per ricostruire l'accaduto;
  - identificazione dei vettori di attacco e delle vulnerabilità sfruttate;
  - isolamento delle minacce e ripristino dei sistemi tramite soluzioni di *backup* e *disaster recovery*;
  - produzione di report dettagliati con analisi, azioni intraprese e raccomandazioni di miglioramento.
- **Verifiche di sicurezza**: comprendono attività di *Cyber Analysis Assessment*, tra cui:
  - *Vulnerability Management* e *Penetration Test* per identificare e valutare i punti deboli delle infrastrutture IT;
  - *Phishing Assessment* per testare la resilienza degli utenti contro campagne fraudolente;
  - *Threat Intelligence* per raccogliere e analizzare informazioni utili a prevenire attacchi futuri.

- **Analisi delle reti**: i servizi di analisi delle reti hanno l'obiettivo di garantire la sicurezza e l'integrità delle infrastrutture di rete. Le attività principali includono:
  - monitoraggio del traffico e rilevamento di anomalie;
  - prevenzione e gestione delle intrusioni;
  - protezione delle reti industriali per assicurare continuità operativa.
- **Gestione degli *endpoint***: riguarda la protezione dei dispositivi aziendali, sia interni che remoti, attraverso:
  - monitoraggio costante dello stato di sicurezza;
  - gestione degli aggiornamenti correttivi e politiche di sicurezza;
  - controllo delle identità e degli accessi;
  - rilevamento e risposta rapida alle minacce;
  - redazione di *report* e *audit*$_G$ di conformità.
- **Gestione dei dati**: supporto alle aziende nella protezione, nell'organizzazione e nella conformità dei dati, in linea con le normative vigenti.
- **Gestione degli utenti e sensibilizzazione**: attività di istruzione dei clienti finalizzata a diffondere buone pratiche di sicurezza informatica, con particolare attenzione agli accessi, ai privilegi e ai comportamenti sicuri. Queste attività contribuiscono a ridurre i rischi legati al fattore umano.
- **Supporto in caso di criticità**: assistenza diretta e tempestiva ai clienti nella gestione di incidenti o sospette violazioni, con l'obiettivo di ridurre al minimo l'impatto sull'operatività aziendale.

Questo insieme di attività consente di identificare in modo proattivo le vulnerabilità dei sistemi informativi, predisporre adeguate misure di protezione e garantire un aggiornamento costante delle competenze necessarie ad affrontare l'evoluzione delle minacce informatiche.

1.3 Strumenti *hardware*

In caso di svolgimento delle attività lavorative da remoto, l'azienda fornisce i seguenti strumenti:

- Computer portatile HP impostato con l'account e la mail aziendale;
- Mouse.

1.4 Strumenti *software*

Le tecnologie e gli strumenti utilizzati a supporto delle attività lavorative sono molteplici e si possono suddividere in due categorie principali: strumenti organizzativi e strumenti produttivi.

1.4.1 Strumenti organizzativi

- **Microsoft Teams**: principale strumento di comunicazione interna, utilizzato per coordinare le attività, condividere documenti e partecipare a riunioni o chiamate quando necessario;
- **Microsoft Outlook**: utilizzato per la gestione della posta elettronica e dell'agenda. Oltre a pianificare incontri e mantenere un flusso di comunicazione costante con i colleghi, viene impiegato anche per lo scambio di comunicazioni con i clienti e per la ricezione di notifiche relative a incidenti di sicurezza provenienti dalle aziende, consentendo così di garantire una comunicazione diretta e tempestiva in caso di necessità;
- **GitHub**: utilizzato come piattaforma di controllo versione per la gestione del codice sorgente, il monitoraggio delle modifiche e la collaborazione su progetti software.

1.4.2 Strumenti produttivi

- **LaTeX**: impiegato per la redazione della documentazione, grazie alle sue avanzate capacità di formattazione e gestione di contenuti tecnici e scien-

tifici. Consente di realizzare documenti professionali, con ottima resa tipografica di formule, grafici, bibliografie e glossari. La separazione tra contenuto e presentazione rende il codice sorgente riutilizzabile e adatto a collaborazioni in ambito accademico e lavorativo;

- **Python**: linguaggio di programmazione ampiamente utilizzato in ambito aziendale per attività di *cybersecurity*, in particolare nell'automazione di processi, nell'analisi di log e nella creazione di strumenti di monitoraggio e rilevamento delle minacce. Grazie alle numerose librerie dedicate, consente di sviluppare rapidamente script per il testing della sicurezza, l'interazione con *Application Programming Interface (API)*$_G$ e la gestione di sistemi complessi;

- **Visual Studio Code (VSCode)**: ambiente di sviluppo leggero, modulare e altamente personalizzabile, adottato principalmente per la scrittura, il debugging e la manutenzione di script e progetti. Supporta numerosi linguaggi e strumenti tramite estensioni dedicate. Pur rappresentando l'IDE più diffuso tra i dipendenti, non è imposto: ciascun utente può scegliere soluzioni alternative in base alle proprie esigenze operative e preferenze personali;

- **Docker**: tecnologia di virtualizzazione basata su *container*$_G$, adottata per garantire ambienti isolati, scalabili e facilmente replicabili. Permette di standardizzare le applicazioni, includendo tutte le dipendenze necessarie per l'esecuzione. Grazie alla leggerezza e portabilità, semplifica lo sviluppo, il testing e la distribuzione, riducendo i problemi di compatibilità tra sistemi.

1.5 Organizzazione del team

1.5.1 *Chief Information Security Officer* (CISO)

Il *Chief Information Security Officer (CISO)*$_G$ è la figura responsabile della strategia di sicurezza informatica all'interno dell'azienda. Supervisiona le atti-

vità del reparto di *cybersecurity* e assicura che siano coerenti con gli obiettivi aziendali e le normative vigenti. Durante il tirocinio, questa figura ha svolto il ruolo di tutor aziendale. Le principali attività comprendono:

- definizione delle politiche e delle strategie di sicurezza informatica;
- supervisione delle attività operative del team di *cybersecurity*;
- coordinamento tra i diversi ruoli del reparto;
- verifica della conformità alle normative e agli standard di settore;
- supporto e formazione interna sulle tematiche di sicurezza.

1.5.2 *Penetration tester*

Il *penetration tester* ha l'obiettivo di individuare le vulnerabilità nei sistemi informatici, simulando attacchi controllati per verificarne la resilienza. Le principali attività comprendono:

- pianificazione ed esecuzione di *penetration test*;
- simulazione di scenari di attacco realistici;
- identificazione e analisi delle vulnerabilità riscontrate;
- redazione di report tecnici con indicazioni sulle criticità rilevate;
- proposta di contromisure per mitigare i rischi individuati.

1.5.3 *Security analyst*

Il *security analyst* si occupa del monitoraggio continuo e della gestione operativa degli eventi di sicurezza, con l'obiettivo di rilevare e rispondere a potenziali incidenti. Le principali attività comprendono:

- monitoraggio dei sistemi e delle infrastrutture tramite strumenti di analisi;
- rilevamento e classificazione degli avvisi di sicurezza;

- analisi dei log e delle anomalie di rete;
- supporto nella gestione e risposta agli incidenti informatici;
- elaborazione di linee guida e buone pratiche di sicurezza per clienti e colleghi.

1.6 Predisposizione all'innovazione

L'ambito della *cybersecurity* è caratterizzato da un'evoluzione continua: nuove vulnerabilità, strumenti di attacco e metodologie di compromissione emergono con frequenza sempre maggiore. Per questo motivo, l'innovazione e l'aggiornamento costante costituiscono elementi fondamentali per ogni azienda che operi in questo settore. Eurosystem S.p.A. ha sviluppato un approccio che integra formazione, ricerca e sperimentazione, con l'obiettivo di anticipare i rischi e fornire soluzioni di difesa sempre più efficaci ai propri clienti. Un aspetto centrale è la formazione continua: nei momenti di minore operatività i team si dedicano allo studio di nuove tematiche, alla valutazione di strumenti emergenti e all'adozione di metodologie innovative. In questo modo rimangono aggiornati sull'evoluzione delle minacce informatiche e rafforzano le proprie competenze tecniche. In parallelo, viene dato ampio spazio alla sperimentazione pratica di strumenti e tecniche di attacco. L'azienda valuta regolarmente soluzioni utilizzate dai *penetration tester* durante le verifiche di sicurezza sui sistemi dei clienti. Tra questi strumenti rientrano dispositivi come:

- **USB Rubber Ducky**, che permette di eseguire comandi automatici sui dispositivi a cui viene collegata, simulando un attacco tramite periferica USB. Viene impiegata per facilitare le attività di *penetration testing* in loco presso le aziende clienti, consentendo di valutare la sicurezza delle postazioni di lavoro rispetto a questo tipo di minacce;

Figura 1.1: Dispositivo USB Rubber Ducky.
Fonte: https://shop.hak5.org

- **LAN Turtle**, un adattatore di rete che consente di instaurare accessi remoti nascosti e di analizzare il traffico direttamente dall'interno della rete aziendale. Viene utilizzato durante le attività di *penetration testing* per verificare l'esposizione delle infrastrutture a minacce derivanti dall'inserimento fisico di dispositivi malevoli;

Figura 1.2: Dispositivo LAN Turtle.
Fonte: https://shop.hak5.org

L'adozione di tali strumenti non ha un fine puramente dimostrativo, ma rappresenta un'attività concreta di valutazione del livello di sicurezza dei clienti, in quanto permette di evidenziare vulnerabilità legate al fattore umano e alla protezione fisica delle postazioni di lavoro. Oltre agli strumenti hardware, vengono analizzate e adottate nuove piattaforme e metodologie orientate sia all'offensiva sia alla difensiva. Tra queste si possono citare:

- l'impiego di tecniche avanzate di *Threat Intelligence*, volte a raccogliere e analizzare informazioni relative a campagne malevole, infrastrutture di attacco e nuove vulnerabilità sfruttate in scenari reali;
- l'aggiornamento continuo dei framework di *penetration testing* e *vulnerability management*, che consente di disporre di strumenti più precisi ed efficaci per identificare punti deboli e priorità di intervento;

- la sperimentazione di approcci innovativi al *red teaming*, in cui vengono simulate operazioni complesse di attacco, con l'obiettivo di valutare non soltanto le difese tecnologiche ma anche le capacità organizzative e di risposta dei clienti.

In conclusione, la predisposizione all'innovazione non è intesa come un'attività separata, ma come parte integrante delle operazioni quotidiane. L'integrazione di formazione, sperimentazione e ricerca applicata consente al reparto di *cybersecurity* di affrontare in maniera proattiva le sfide poste dalle minacce informatiche, mantenendo un equilibrio tra lo sviluppo delle competenze interne e l'offerta di servizi sempre più efficaci e aggiornati per i clienti.

Capitolo 2

Scopo del progetto

2.1 Il ruolo degli *stage* nell'azienda

La sezione analizza il ruolo degli *stage* nell'azienda ospitante, mostrando come essi favoriscano l'innovazione e supportino l'azienda nella sperimentazione di nuovi processi e metodologie operative.

2.2 Analisi del problema

Viene presentato il problema specifico che lo *stage* si propone di affrontare, analizzando le criticità esistenti nell'ambito della sicurezza informatica e la necessità del progetto per l'azienda.

2.3 Obiettivi

Questa sezione definisce gli obiettivi specifici dello *stage* accordati con il tutor aziendale, stabilendo risultati misurabili e traguardi concreti da raggiungere durante il periodo di tirocinio.

2.4 Vincoli

Questa sezione identifica i vincoli tecnici, temporali e organizzativi che hanno influenzato lo sviluppo del progetto, spiegando come questi sono stati gestiti

durante lo *stage*.

2.5 Sviluppi successivi allo *stage*

Si descrivono le possibili evoluzioni future del progetto sviluppato durante lo *stage* e come questo potrà essere integrato e sviluppato ulteriormente dall'azienda.

2.6 Motivazioni personali

Descrive le motivazioni personali che hanno spinto alla scelta di questo stage, gli interessi specifici nel campo della *cybersecurity* e le aspettative di crescita professionale.

Capitolo 3

Sviluppo del progetto

3.1 Analisi dei requisiti

3.1.1 Casi d'uso

Vengono identificati e descritti i principali casi d'uso del sistema sviluppato, illustrando gli scenari operativi in cui il prodotto sarà utilizzato e le interazioni tra utenti e sistema.

3.1.2 Requisiti

Si presenta l'analisi completa dei requisiti funzionali e non funzionali del sistema, definendo le specifiche tecniche che la soluzione deve soddisfare per rispondere alle esigenze aziendali.

3.2 Progettazione

3.2.1 Architettura del sistema

Viene descritta l'architettura complessiva del sistema sviluppato, illustrando la struttura dei componenti, le loro interazioni e le scelte architetturali tramite diagrammi delle classi e diagrammi di flusso.

3.2.2 Scelta dei servizi del sistema

Questa sezione illustra le motivazioni alla base della selezione dei servizi vulnerabili inclusi nel progetto, evidenziando come ciascuno di essi contribuisca al sistema.

3.3 Codifica

3.3.1 Struttura del progetto

Viene presentata l'organizzazione del codice e dei file del progetto, descrivendo la struttura delle cartelle, i pattern di sviluppo utilizzati e le convenzioni adottate per garantire manutenibilità e leggibilità.

3.3.2 Difficoltà incontrate

La sezione analizza gli ostacoli incontrati durante lo sviluppo del progetto, sia di natura tecnica sia organizzativa. Viene descritto come ciascuna difficoltà sia stata gestita e superata, evidenziando le soluzioni adottate.

3.4 Verifica

3.4.1 Test

La sezione illustra il metodo seguito per condurre le attività di testing, descrivendo i diversi tipi di test implementati e gli strumenti utilizzati per garantire la qualità del software.

3.5 Validazione

In questa sezione si illustra il processo di validazione del progetto sviluppato, includendo i test con strumenti di controllo e la verifica del rispetto dei requisiti.

3.6 Risultati del progetto

3.6.1 Prodotto finale

Questa sezione descrive il prodotto ottenuto dallo stage e come questo funziona, nei suoi vari aspetti e funzionalità.

3.6.2 Conformità ai requisiti

In questa sezione viene analizzato il grado di soddisfacimento dei requisiti inizialmente identificati, evidenziando quali requisiti sono stati raggiunti completamente e quali potrebbero richiedere sviluppi futuri.

Capitolo 4

Valutazione retrospettiva

4.1 Obiettivi raggiunti

La sezione ha l'obiettivo di fornire una valutazione dettagliata dei risultati ottenuti durante lo *stage*, evidenziando quali e quanti degli obiettivi precedentemente definiti siano stati effettivamente raggiunti.

4.2 Conoscenze acquisite

Questa sezione elenca e descrive le nuove conoscenze acquisite durante lo stage, particolare riferimento alle tecnologie, metodologie e tecniche nel campo della cybersecurity e dello sviluppo *software*.

4.3 Competenze professionali acquisite

In questa sezione si descrivono le competenze pratiche e professionali sviluppate durante l'esperienza di *stage*, incluse competenze tecniche specifiche, capacità di *problem solving* e abilità di lavoro in team in ambiente professionale.

Bibliografia

Sitografia

Acronimi e abbreviazioni

API *Application Programming Interface*. 5

CISO *Chief Information Security Officer*. 5

ES Esempio di acronimo. v

Glossario

Audit Un processo sistematico di esame e valutazione delle attività, dei controlli e delle procedure di un'organizzazione, al fine di garantire la conformità alle normative e l'efficacia delle misure di sicurezza. 3

Container Un'unità standardizzata di software che include tutto il necessario per eseguire un'applicazione, garantendo coerenza tra gli ambienti di sviluppo, test e produzione. 5

Esempio di nome Esempio di descrizione. v