Wendy Rosettini

Abitazione : Via Luigi Sturzo, 67100, L'Aquila, Italia

E-mail: wendy.rosettini@gmail.com **Telefono:** (+39) 3279994218

Sito web: https://wendyrosettini.github.io/github-portfolio/

LinkedIn: https://www.linkedin.com/in/wendy-rosettini-9130a3289/

Sesso: Femminile **Data di nascita:** 10/09/2000 **Nazionalità:** Italiana

PRESENTAZIONE

Laureata in Ingegneria Informatica presso l'Università degli Studi dell'Aquila, con una tesi dal titolo: *"Sicurezza in ambito veicolare: studio, sviluppo e sperimentazione di schemi crittografici basati su HSM"*.
Attualmente iscritta al corso di Laurea Magistrale in *Cybersecurity* presso l'Università La Sapienza di Roma.

Ho appena terminato un tirocinio di 6 mesi presso **Leonardo S.p.A.**, focalizzato su un progetto di tesi che mira ad **automatizzare il penetration testing mediante l'utilizzo di tecniche di Intelligenza Artificiale**, in particolare con l'impiego di **Large Language Models (LLM)** per l'analisi, la pianificazione e l'esecuzione di attacchi simulati in scenari di sicurezza multidominio (reti, applicazioni web, dispositivi IoT).

ISTRUZIONE E FORMAZIONE

[2020 – 2023] **Ingegneria dell'informazione**

Università degli studi dell'Aquila

Città: L'Aquila | **Paese:** Italia |

[Attuale] **Cybersecurity**

Università La Sapienza

Città: Roma | **Paese:** Italia |

Certificazione C1 Cambridge English

Cambridge English

COMPETENZE LINGUISTICHE

Lingua madre: Italiano

Altre lingue:

inglese

ASCOLTO C1 **LETTURA** C1 **SCRITTURA** C1

PRODUZIONE ORALE C1 **INTERAZIONE ORALE** C1

tedesco

ASCOLTO B1 **LETTURA** B1 **SCRITTURA** B1

PRODUZIONE ORALE B1 **INTERAZIONE ORALE** B1

francese

ASCOLTO B1 **LETTURA** B1 **SCRITTURA** B1

PRODUZIONE ORALE B1 **INTERAZIONE ORALE** B1

Livelli: A1 e A2: Livello elementare B1 e B2: Livello intermedio C1 e C2: Livello avanzato

COMPETENZE

Penetration Testing Tools (Wireshark, Nmap, Burpsuite, Metasploit)) | Ethical Hacking | Malware Analysis | Risk-management | Object Oriented Program (OOP) | ■ Buona conoscenza linguaggi di programmazione

PATENTE DI GUIDA

Automobile: B

ESPERIENZA LAVORATIVA

[10/03/2025 – 12/09/2025] **Tirocinante Red team– Leonardo S.p.A.**

- Osservazione diretta delle attività di penetration testing, principalmente WAPT, con approfondimento di approcci DAST e SAST.
- Collaborazione con il team nella definizione e gestione di use case, con redazione di report tecnici e presentazioni interne sui risultati.
- Supporto alla realizzazione di dashboard e strumenti di visualizzazione per facilitare l'interpretazione dei dati e la comunicazione dei risultati ai diversi stakeholder.
- Partecipazione a CTF (Global Hack The Box, Red Hot Cyber) e validazione delle tecniche su macchine reali (HTB/VulnHub).
- Sviluppo della tesi: framework AI-driven per penetration testing con architettura multi-agente e implementazione del Model Context Protocol (MCP).
- Realizzazione di moduli di privilege escalation automatizzata, gestione di shell persistenti via WebSocket e sviluppo dell'interfaccia di controllo.
- Testing e benchmarking delle performance AI e implementazione di tecniche RAG per supporto decisionale avanzato.

PROGETTI

[10/03/2025 – 12/09/2025] **Development of an AI-Driven Framework for Automated Penetration Testing**

Progettazione e realizzazione di un sistema modulare che automatizza le fasi del penetration testing tramite agenti LLM e l'uso del Model Context Protocol (MCP). Il framework integra strumenti principali di Kali Linux come Nmap, Gobuster, Nikto, SQLMap, theHarvester, SearchSploit, con orchestrazione intelligente, post-exploitation e controllo human-in-the-loop.

Link: https://github.com/WendyRosettini/masters-thesis-multiagent-pentest | https://github.com/WendyRosettini/Pentest-Runner

[2023 – 2023] **Sicurezza in ambito veicolare: studio, sviluppo e sperimentazione di schemi crittografici basati su HSM**

La tesi tratta della sicurezza in ambito veicolare, con un focus sull'utilizzo di moduli di sicurezza hardware (HSM) e TPM per proteggere i veicoli da attacchi informatici. Analizza le vulnerabilità dei moderni sistemi automobilistici e sperimenta protocolli crittografici come l'AES e l'ECTAKS basato su curve ellittiche. Attraverso sperimentazioni pratiche su microcontrollori ESP32, la tesi valuta l'efficacia di questi sistemi di cifratura nel migliorare la sicurezza dei dati e delle comunicazioni tra i veicoli.

Link: https://drive.google.com/file/d/1oZJRywM75ihs5xgnwREWP5k1kdHpqao6/view?usp=sharing

[2021 – 2022] **Sviluppo di siti web**

Ho collaborato con due colleghi alla realizzazione di un sito web, occupandomi del design e della programmazione frontend/backend. Questo progetto mi ha permesso di acquisire competenze pratiche nell'utilizzo di tecnologie web come HTML, CSS, JavaScript, e PHP.

Link: https://foodrescue.altervista.org/foodrescue/

[2024 – 2024] **Creazione di una Macchina Virtuale per Penetration Testing**

Ho creato, insieme a una mia collega, una macchina virtuale dedicata al penetration testing, strutturata con tre livelli di privilege escalation (facile, medio, difficile) e tre livelli per ottenere accesso locale alla macchina (facile, medio, difficile), attraverso tecniche come SQL injection, il furto di cookie e le vulnerabilità di upload di file. Durante lo sviluppo, ho utilizzato diversi strumenti di penetration testing, simulando scenari realistici di vulnerabilità

Link: https://drive.google.com/file/d/1IUo7KfHntAANG9wObcx0sIHjdGM0Lb32/view?usp=sharing | https://drive.google.com/file/d/1T5A-cu5uWGLb_VUzgbMPETPmF-R5ZNY9/view?usp=sharing

[2024 – 2024] **Impostazione di Regole di Firewall e Meccanismi di Sicurezza in Rete**

Ho configurato regole di firewall su OPNsense in un ambiente Proxmox, implementando un sistema di sicurezza robusto per la rete. Ho anche impostato strumenti di Security Information and Event Management (SIEM) e Intrusion Detection System (IDS), insieme ad altri meccanismi di difesa, per monitorare e proteggere attivamente la rete da minacce e vulnerabilità.

Link: https://drive.google.com/file/d/1Z9u5VkLngfSm38Ffp-lXbxRp-n9ZnfJe/view?usp=sharing | https://drive.google.com/file/d/1Yvj6wgt0y2-RcKlszrbEM7G5Yn-iNNjN/view?usp=sharing | https://drive.google.com/file/d/1XvDNJWwzoerfgTzYYsTdWBln7WZE1nU2/view?usp=sharing

CONFERENZE E SEMINARI

[09/10/2024] **Cybertech Europe 2024** Roma

HOBBY E INTERESSI

Pianoforte, Chitarra, Sci alpino, ballo

CERTIFICAZIONI E COMPETIZIONI

Red Hot Cyber Conference – CTF XTF 2025

Partecipazione alla CTF della Red Hot Cyber Conference 2025 con il team *CarbonHackers*, classificati al 2° posto ex aequo con i vincitori. Abbiamo affrontato sfide avanzate in ambito **web exploitation**, **reverse engineering**, **decodifica ransomware**, **social engineering simulato con AI**, **hacking hardware IoT** e **compromissione di infrastrutture 4G realistiche**.