

ELVIS HAVERIKU

+32 497 73 37 62
elvishaveriku@gmail.com
Brussels, Belgium

IT & CYBERSECURITY

PROFILE

Motivated IT professional with a growing passion for cybersecurity. I have hands-on experience working with Windows, Linux, and network monitoring tools, and I enjoy digging into logs, spotting unusual activity, and understanding how systems behave. I've worked with SIEM tools like Splunk and have used Python and Bash to automate small tasks. I'm always learning, experimenting, and improving my skills. Looking for an opportunity to grow in an IT or cybersecurity role where I can contribute, learn, and build real-world experience.

SKILLS

- Cybersecurity & Monitoring: Splunk, Snort, Wireshark, Burp Suite, Metasploit, Nmap
 - Scripting & Development: Python, Bash, PowerShell, Flask, MySQL, HTML/CSS/JS
 - Systems & Administration: Windows Server, Active Directory, Linux (Ubuntu/Kali), Nginx, hardware configuration
 - Problem-Solving & Mindset: Critical thinking, solution-oriented approach, curiosity, continuous learning
 - Collaboration & Work Style: Teamwork, communication, time management, dedication, adaptability
-

PROFESSIONAL EXPERIENCE

Bookkeeper – "Haveriku-97" (Kavaja, Albania)

June 2016 – October 2023

- Recorded daily financial transactions (sales, purchases, receipts, payments)
- Calculated and submitted payroll taxes and social contributions.
- Assisted in the preparation of financial statements (balance sheet, P&L, cash flow).

Data Entry Specialist – "WeAreFiber" (Tirana, Albania)

August 2021 – January 2023

- Managed data entry and validation using Excel ensuring accuracy.

Intern – "Intesa SanPaolo Bank Albania" (Tirana, Albania)

September 2017 – December 2017

- Assisted in the everyday operations in the bank branch.
-

EDUCATION

Cybersecurity Training

BeCode Brussels

October 2024 – April 2025

- System Administration: Managed Windows/Linux servers, user access, security hardening, and basic automation.
- Networking: Practiced TCP/IP, OSI model, routing, switching, and analysis of network protocols.
- Programming & Scripting: Built small tools and automations with Python, Bash, PowerShell, SQL, and Flask.
- Security Monitoring: Analyzed logs and network traffic using Snort, Suricata, Zeek, Wireshark and Splunk
- Penetration Testing: Performed enumeration, exploitation, post-exploitation, and vulnerability assessment using Nmap, Burp Suite, and Metasploit.

Complete Python Developer Course

Zero to Mastery Academy

July 2023 – October 2023

Professional Master in Finance and Accounting

European University of Tirana

September 2012 – April 2014

Bachelor in Finance and Banking

European University of Tirana

September 2009 – July 2012

CERTIFICATIONS

- Microsoft SC-900: Security, Compliance, and Identity Fundamentals
 - Microsoft AZ-900: Azure Fundamentals
 - TryHackMe: SOC Level 1 Certificate
-

LANGUAGES

- Albanian (Native) – English C1 – French A2 – Italian B2

CYBERSECURITY & IT PROJECTS

C2 SERVER CREATION AND TRAFFIC DETECTION

- Created an isolated virtual lab with Kali Linux (attacker), Windows 10 (victim), and Ubuntu (Splunk SIEM) using VirtualBox and internal networking.
- Simulated adversary command and control (C2) traffic using MITRE Caldera and deployed beaconing agents on the victim endpoint.
- Configured Splunk with Sysmon log ingestion for real-time detection and analysis of malicious network and host activity.

AUTOMATED WEB SECURITY RECONNAISSANCE

- Utilized Subfinder for discovering subdomains and Nuclei for vulnerability scanning.
- Developed a Python script to detect missing security headers on multiple domains.
- Implemented logging and low-noise scanning to enhance efficiency and reduce detection

FLASK SERVER CONTACT FORM

- Developed a web-based contact form using the Flask framework in Python.
- Applied validation and sanitization to ensure secure and accurate user input.

PHISHING WEBSITE SERVER

- Created a Flask-based malicious web application designed to capture user login credentials through a login form.
- Deployed the website online using Ngrok to simulate a phishing attack environment.

WINDOWS SERVER 2022 ACTIVE DIRECTORY

- Deployed and configured a secure Windows Server 2022 environment with Active Directory (AD) and key server roles including DNS, DHCP, and IIS.
- Integrated users with role-based access and applied granular permissions using Group Policy Objects (GPOs).

LINUX SERVER CONFIGURATION

- Configured a Linux server infrastructure with DHCP, DNS, and Nginx.
- Automated backups and remote management using cron jobs and SSH.
- Implemented partitioned storage and enhanced data integrity with rsync.

NETWORK ARCHITECTURE WITH CISCO PACKET TRACER

- Designed a secure network architecture with VLANs and Access Control Lists (ACLs).
- Configured DNS, DHCP, and iSCSI servers for optimized functionality and efficiency.