Simão Andrade

Date of birth: 2002 | **Nationality:** Portuguese | **Email address:** simaoaugusto11@hotmail.com | **Website:** nimouh.netlify.app | **LinkedIn:** linkedin.com/in/simaoafandrade/ | **Github:** github.com/NiMouh | **Address:** Portugal (Home)

ABOUT ME

I developed an enthusiasm for cybersecurity and technology at the age of 13 and this passion continued to grow throughout my degree. Not only that, but I'm a very ambitious and adaptable person who is constantly looking for new challenges to conquer.

WORK EXPERIENCE

APPLICATION SECURITY ENGINEER – KÖRBER – 06/03/2026 – Current – PORTO, PORTUGAL

Business or Sector: Information and communication | **Department:** Cybersecurity | **Website:** www.koerber.com

In this job, my main activities are:

- Implement security measures in accordance with Körber Group's application security guidelines and policies.
- Conduct security assessments and code reviews to identify and mitigate vulnerabilities.
- Collaborate with software architects and developers to integrate security practices into the development lifecycle.
- Develop and maintain secure coding standards and guidelines.
- Perform threat modeling and risk assessments for new and existing applications.
- Implement and manage security tools for static and dynamic analysis, and vulnerability scanning.
- Enhance the secure software development lifecycle (SDLC) by integrating security into CI/CD pipelines and DevSecOps practices.
- Perform regular reviews our software development lifecycle and products.
- Conduct regular security audits and penetration testing on applications.
- Provide training and support to software engineers on application security best practices.

NETWORK SECURITY ENGINEER – CLOUDFLARE – 02/03/2025 – 02/03/2026 – PORTUGAL

Business or Sector: Information and communication | **Department:** Cybersecurity | **Website:** www.cloudflare.com

In this job, my main activities are:

- Protecting network infrastructure by analyzing and mitigating malicious traffic.
- Communicating with clients to support incident response efforts.
- Troubleshoot network performance, availability, and configuration issues. Use of tools like MTR, traceroute, dig and netcat to determine open ports, DNS propagation, return path and routing problems.
- Analyzing various data points like IP addresses, cookies, HTTP headers, and JavaScript to differentiate between legitimate and malicious traffic. Use of tools like cURL for inspecting HTTP headers and bash scripts for automating log analysis.
- Mitigating DDoS attacks across OSI model layers 3, 4, and 7. This involves leveraging Cloudflare's security tools, including Magic Transit, Spectrum, WAF (Web Application Firewall), reputation lists, packet inspection, blocklisting, allowlisting, and rate limiting. Use of tools such as cURL, openssl and custom tools for analyzing SSL/TLS traffic during incident response.
- Creation, testing and monitoring of WAF custom and managed rulesets in order to prevent unwanted traffic.

CYBERSECURITY CONSULTANT – PRIO ENERGY SA – 01/09/2024 – 28/02/2025 – AVEIRO, PORTUGAL

Business or Sector: Information and communication | **Department:** Cybersecurity and Information Security | **Website:** www.prio.pt

During my thesis, I was assigned to guide the current cybersecurity team on technical and non-technical subjects with the following objectives:

- Carrying out internal audits and assessing compliance with nationally and internationally recognized information security standards (PCI DSS, SMD, ISO 27001).
- Identifying and classifying information assets, such as hardware, software, and data.
- Conduction and creation of cyber awareness campaigns.

CYBERSECURITY ANALYST – ALTICE LABS – 01/07/2024 – 13/09/2024 – AVEIRO, PORTUGAL

Business or Sector: Information and communication | **Department:** Cybersecurity | **Website:** www.alticelabs.com

During this internship, I was assigned to a project to improve the current threat modeling process at Altice Labs, by incorporating threats and mitigations specific to modern software architectures.

My main activities were:

- Research state-of-the-art best practices concerning modern cloud architectures (e.g. AWS, GCP).
- Develop Microsoft TMT templates with the researched threats and mitigations for modern software architectures.
- Test the developed templates in the context of an Altice Labs application.

24/7 FRONT-OFFICE – CELFINET – 19/06/2023 – 19/09/2023 – COVILHÃ, PORTUGAL

Business or Sector: Information and communication | **Department:** Telecommunications | **Website:** https://celfinet.com/

During this internship, I was ensuring the availability and performance of telecom services offered by telecoms companies.
My main activities were:

- Monitoring to identify telecommunication incidents and/or service failures.
- Assessing the severity of incidents by maintaining control over response and resolution times.
- Graphical representation of the network element causing the alarm according to severity and SLA using Python and PowerBI.

WEB DEVELOPER – CELEUMA – 15/12/2019 – 15/06/2020 – VISEU, PORTUGAL

Business or Sector: Information and communication | **Department:** Web Development | **Website:** www.celeuma.pt

During this internship, I was a member of a team developing a dynamic website in a creative agency, actively contributing to all stages from conceptualization (design and architecture) to production deployment.

My main activities were:

- Writing clean, efficient, and responsive code for website functionality (Javascript).
- Integrating backend services and databases as required (PHP and MySQL).
- Participating in team meetings and discussions to brainstorm solutions and address project challenges.

EDUCATION AND TRAINING

15/09/2023 – CURRENT Aveiro, Portugal

MASTER OF CYBERSECURITY University of Aveiro

As of now, this degree made me capable of:

- Explore methodologies and techniques for identifying and exploiting vulnerabilities and protecting services and systems (OWASP ZAP, Burp Suite, NMAP, Wireshark);
- Being able to develop and operate applications with security requirements (OWASP, SDLC).
- Have knowledge of international standards and what they are used for (e.g. ISO 27001, NIST);
- Acquire understanding of the European regulation (applied in the Portuguese National Transposition) on cybersecurity and information security (GDPR, NIS1);
- Acquire the ability to implement security mechanisms in communication networks (Firewall, IDS).
- Understand and develop architectures and methodologies for: network and services monitoring (e.g. SIEM, SNMP, Netflow and Sysinternals Suite), detection of attacks and functional anomalies, and deploy counter-measures and/or functional corrections.

Website https://www.ua.pt/en/curso/462 | **Final grade** 17 mark (currently) | **Level in EQF** EQF level 7 |

National classification 7 | **Type of credits** ECTS | **Number of credits** 120

15/09/2020 – 15/06/2023 Covilhã, Portugal

BACHELOR OF COMPUTER SCIENCE AND ENGINEERING University of Beira Interior

During my degree, I got capable to perform these roles:

- Design and develop software (Scrum Framework);
- Programming applications (C Language, Java, PHP, Python, Ocaml);
- Programming Frameworks (Spring Boot Framework, ReactJS);
- Automation for management of informatics systems (Bash Scripting);

- Installing, configuring and maintaining of computer networks (Switches, Routers, Servers, Network Segmentation);
- Know the workings of the underlying protocols of IP networks (BGP, HTTP, DNS, DHCP, SMTP);
- Properly utilize encryption algorithms, cryptography tools, authentication mechanisms and digital signatures (OpenSSL, GnuPGP);

Website https://www.ubi.pt/en/course/42 | **Final grade** 16 mark | **Level in EQF** EQF level 6 | **National classification** 6 |

Type of credits ECTS | **Number of credits** 180

15/09/2017 – 15/06/2020 Castro Daire, Viseu, Portugal

TECHNICAL COURSE OF COMPUTER NETWORK INSTALLATION AND MANAGEMENT Highschool of Castro Daire

700+ hours worth of internships in the web development and system administration fields.

Final grade 17 mark | **Level in EQF** EQF level 4 | **National classification** 4

LANGUAGE SKILLS

Mother tongue(s): **PORTUGUESE**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	C1	C1	B2	B2	C1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

SKILLS

Programming Languages

C language | Java | PHP | Python | JavaScript | SQL | Bash Scripting

Tools

Visual Studio Code | Git | Atlassian stack (Jira, Confluence, ...) | Kibana | Grafana | WAF

Operating Systems

Linux OS (Ubuntu, Parrot and Kali) | Windows

Markup Languages

Markdown | HTML | LaTeX

Design & Styling

Figma | CSS

Network Tools

Wireshark / GNS3 | Cisco Packet tracer | Virtual Machines | Burp Suite | Postman | Kleopatra

PROJECTS

01/11/2024

Tryhackme Path

Currently doing the TryHackMe Junior Pentester Path, focusing both in web and network exploitation, while also improving skills for custom tooling solutions.

Link https://tryhackme.com/p/simaoandrade

Network Anomaly Detection, in order to define SIEM Rules

The detection of anomalous behaviours in communication networks is crucial for maintaining cybersecurity, allowing organizations to identify and respond to potential threats effectively. This project involved the **creation of SIEM rules to detect malicious activities and identify potentially compromised devices** within the network. The work spanned from analysing normal network behaviours to defining and testing rules tailored for detecting sophisticated threats.

The following concepts were explored in depth:

- **Analysis of normal network behaviours** to establish baselines for internal and external traffic flows;
- **Identification of internal servers and services** to map critical infrastructure;
- **Definition of SIEM rules targeting:**
    - Internal BotNet activities;
    - Data exfiltration through HTTPS and DNS;
    - External users exhibiting anomalous usage of public company services;
- **Testing of SIEM rules to validate their effectiveness** in detecting anomalies;
- **Identification of compromised devices based** on rule triggers and behavioural patterns;
- Documentation of findings in a detailed report, providing insights and recommendations.

Link https://github.com/NiMouh/AD_SR

Discord Data Exfiltration Detection Using Machine Learning

This project focuses on detecting data exfiltration through Discord by developing a machine learning (ML) solution. A Discord bot simulates data exfiltration scenarios, and network traffic features are extracted from packets and flows to train the ML model.

Key Components:

- **Data Exfiltration Simulation:** Developed a Discord bot using webhooks to emulate data exfiltration activities along with normal behaviour.
- **Feature Extraction:** Using Pyshark, analysed network traffic to extract features from packets and flows for ML model training.
- **ML Model Development:** Trained and validated an ML model to help identify patterns indicative of data exfiltration via Discord.
- **Anomaly Detection:** Implemented the ML model to monitor network traffic and detect suspicious activities associated with data exfiltration.

Challenges Addressed:

- **Encrypted Communications:** Discord uses HTTPS, encrypting data in transit and hindering traditional inspection methods. This project overcomes this by focusing on metadata and TCP/UDP traffic patterns rather than content inspection.
- **Legitimate vs. Malicious Traffic:** Differentiated between normal Discord usage and potential exfiltration attempts by analysing behavioural patterns and anomalies in network traffic.

Link https://github.com/NiMouh/discord_exfiltration

IDS (Intrusion Detection System) using ML (Machine Learning)

This project implements an IDS leveraging ML techniques to classify network traffic as benign or anomalous and to identify specific types of attacks. The system employs both binary and multi-class classification models to detect families of **Botnets** (Mirai and Gafgyt).

Key Components:

- **Binary Classification:** Applied Grid-Search with Decision Trees to distinguish between normal and anomalous network traffic.
- **Multi-Class Classification:** Utilized Classification Decision Trees to identify specific attack types within the network traffic.
- **Feature Analysis:** Examined 27 attributes from the dataset, including Mutual Information metrics and statistical features, to inform model training.

Model Validation:

- **McNemar's Statistic:** Applied to compare the performance of different classification models and assess their statistical significance.
- **Performance Metrics:** Evaluated models using accuracy, precision, recall, and F1-score to measure their effectiveness in detecting botnet intrusions.

Link https://github.com/NiMouh/IDS

IdP (Identity Provider) for a CRM application

Authentication and authorization are extremely important topics in terms of cybersecurity, allowing access to be granted to the right entity. Using the **Flask Framework**, an IdP was developed that supports services, in this case access to information and information and functionalities of a CRM, with varying degrees of criticality and applies **multi-factor authentication** methods dynamically according to the **risk profile**.

The following concepts were explored in depth:

- Architectural projection of the project;
- Creation of user profiles;
- **Risk-based authentication** approach;
- Implementation of the **OAuth 2.0** authorization protocol;
- Security at web development level;
- Integration of a single authentication method for three different services.

Link https://github.com/NiMouh/IdP_CRM

IoT Vulnerability Monitoring

An analysis was conducted for the conceptual design of an IoT monitoring application using the **Secure Development Lifecycle (SDL)** methodology. While the application itself was not developed, the project focused on applying SDL principles to explore the security requirements and risks associated with IoT environments.

The following concepts were explored in depth:

- **Fuzz Testing:** Analysis of how this technique can uncover vulnerabilities by simulating unexpected or malformed inputs, identifying potential weak points in IoT communication protocols using of Burp suite custom payloads.
- **Hazard Analysis:** A structured evaluation of risks, focusing on IoT-specific threats such as insecure device communication, weak authentication, and potential data breaches.
- **Functional Security Requirements:** Secure communication protocols to protect data transmission, robust authentication mechanisms for access control and real-time monitoring capabilities for identifying vulnerabilities.
- **Non-Functional Security Requirements:** Scalability to accommodate large IoT networks, reliability to ensure continuous monitoring even under adverse conditions.

Tamper Proof Data Vault (TPDV)

This project focused on leveraging **Intel SGX enclaves** to implement a secure and tamper-proof digital vault.

Through this implementation, the following key concepts were explored and learned:

- **Intel SGX Enclaves:** Understanding how hardware-based isolation ensures secure execution of code and data integrity, even in potentially compromised systems.
- **Data Integrity:** Utilizing cryptographic hashing to detect any unauthorized modifications to files.
- **Secure Key Management:** Ensuring passwords and sensitive operations remain isolated within the enclave.
- **Secure Cloning:** Safely transferring cryptographic data between enclaves to replicate the vault without compromising its integrity.
- **Designing Secure Systems:** Building a user-friendly interface for interacting with tamper-proof systems while maintaining strict security controls.

Link https://github.com/NiMouh/TPDV

COMMUNICATION AND INTERPERSONAL SKILLS

Representative of the Year

Throughout all my Bachelor's degree and the last year of my Master's, I dedicated myself to representing my colleagues as their elected representative, advocating for their interests. In this role, I organized supplementary classes, taught by both myself and fellow students, aimed at supporting those who struggled with course material, thereby contributing to the development of future computer engineers.