

## EXPERIENCE

---

### • **Hacktive Security**

Offensive Security Analyst

Full Remote

Mar. 2024 - Present

- Conducted penetration tests for many famous firms, identified high-severity vulnerabilities in web applications, network infrastructures, and APIs.
- Delivered detailed, high-quality reports outlining vulnerabilities, potential impacts, and actionable remediation steps, enhancing clients' security posture.
- Executed on-site internal network penetration tests thorough security assessments compliant with industry standards.
- Performed advanced Research initiatives and contributed to the development of security tools and techniques.

### • **Sapienza University**

Security Researcher

Full Remote

June 2023 - Feb. 2024

Received a research grant at DIET Department to continue the studies on security in programmable networks.

- Designed, implemented and tested an innovative framework for anomalies and attacks detection in network environments through log analysis using Python and Bash.
- Discovered vulnerabilities (CVEs) and new attack methodologies through testing, static and dynamic analysis in network applications written in Java.

### • **Consortium for the Research in Automation and Telecommunication (CRAT)**

Network Security Researcher

Full Remote

Sep. 2023 - Feb. 2024

For a project commissioned by the European Space Agency (ESA):

- Studied and defined system scenarios, technical requirements and specifications for a new communication protocol for satellite networks.
- Reviewed designs and implementations of various state-of-the-art network protocols for compatibility and security standards

### • **Bugcrowd**

Security Researcher

Full Remote

Nov. 2021 - Nov. 2023

- **bugcrowd.com/edoardottt**: Successfully identified and reported 300+ security vulnerabilities in high-profile companies and U.S. Government offices, with a specialization in web and network applications.
- **CISA Competition**: Recognized for outstanding work by reaching second place at the Cybersecurity and Infrastructure Security Agency (CISA) 2021 Competition.

### • **SeismoCloud**

Software Developer

Rome, Italy

Mar. 2020 - Oct. 2020

- **SeismoCloud EUD system**: Designed, implemented and secured an user-friendly End User Development system (Docker, NodeJS) to enable non-technical users to configure and control networks of IoT devices and online services (e.g. automate actions such as sending Telegram/Email messages and posting tweets through IoT devices data).
- **API development**: Resolved issues in the SeismoCloud REST API system (Golang) providing information on Sensors signalings, devices and users' data, as well as associated statistics.

## TECHNICAL SKILLS

---

Application and Network Security, Software Development and Security Code Review. Extensive knowledge of networks and networking protocols (TCP/IP, Routing, HTTP, DNS, DHCP, IPS, IDS, WAF, Firewall, Proxy).

- **Languages**: Python, Go, Bash, Java, C, Javascript, SQL, HTML and other C-family languages.
- **Technologies**: Linux (Local, VM and on Cloud), Windows, Git, GitHub Actions, BurpSuite, SAST and DAST, Metasploit, Nessus, Nuclei and other vulnerability scanners, Docker, Relational Databases, VSCode, Wireshark, Postman.

## EDUCATION

---

- **Sapienza University**  
Master's Degree in Cybersecurity; 109/110  
Dissertation: "Proposal and Investigation of a framework for Cross App Poisoning attacks detection in Software Defined Networks."  
Rome, Italy  
*Oct. 2020 – May 2023*
- **Sapienza University**  
Bachelor's Degree in Computer Science; 103/110  
Dissertation: "Design and development of the End User Development system in SeismoCloud".  
Rome, Italy  
*Sept. 2016 – Oct. 2020*
- **Fabio Besta Scientific High School**  
Scientific High School Diploma; 71/100  
Orte, Italy  
*Sept. 2011 – July 2016*

## AWARDS - CERTIFICATIONS - LICENSES

---

- **Security+ by CompTIA**  
Certified CompTIA Security+ ([Sec+ Certificate link](#))  
Feb. 2024
- **ICCA by INE**  
Certified Cloud Associate ([ICCA Certificate link](#))  
July 2023
- **eWPT by eLearnSecurity (INE)**  
Certified Web Application Penetration Tester ([eWPT Certificate link](#))  
June 2023
- **eJPT by eLearnSecurity (INE)**  
Certified Junior Penetration Tester ([eJPT Certificate link](#))  
Sept. 2022

## OPEN SOURCE PROJECTS

---

Open-sourcing since 2018, reached 11k+ stars on GitHub: [github.com/edoardottt](https://github.com/edoardottt)

- **scilla**: Information Gathering tool - DNS / Subdomains / Ports / Directories enumeration
- **cariddi**: Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, tokens and more
- **csprecon**: Discover new target domains using Content Security Policy.
- **lit-bb-hack-tools**: Little Bug Bounty and Hacking Tools.

## SECURITY ADVISORIES

---

Discovered, reported and responsibly disclosed many undetected vulnerabilities in popular products (mainly with code reviews, but also testing, static and dynamic analysis): [edoardoottavianielli.it/cve](https://edoardoottavianielli.it/cve)

## LANGUAGES

---

- **Italian**: Native speaking.
- **English**: Professional Working Proficiency.

## SCIENTIFIC PUBLICATIONS

---

- **Simplify Node-RED for End User Development in SeismoCloud**  
Enrico Bassetti, Edoardo Ottavianielli, Emanuele Panizzi  
<https://arxiv.org/pdf/2012.05637.pdf>