

# Michele Toccagni

✉ contact {at} toccagni {dot} info | 📍 Bergamo, Italy

## Education

---

### Univerity of Milan

MASTER IN CYBER SECURITY

Milan

2018 – 2021

### Univerity of Milan

BACHELOR IN DIGITAL COMMUNICATION

Milan

2013 – 2018

## Work Experience

---

### Accenture

SECURITY ASSOCIATE MANAGER

Milan, Italy

December 2022 – Present

- Involved in the security analysis of infrastructures, with focus on Web, Network, Mobile and Thick Client Penetration Test.
- Team management, both in managing activities and in relations with clients.
- Coordinate and direct all phases of product testing while managing and leading project teams.

SECURITY TEAM LEAD

December 2020 – December 2022

- Involved in the security analysis of infrastructures, with focus on Web, Network, Mobile and Thick Client Penetration Test.
- Developed a tool to generate automatically the reports of Penetration Tests (like Serpico). This tool is written in Python-Flask, create both Word and Excel reports and it's used by the whole team.
- Team management, both in managing activities and in relations with clients.

SENIOR SECURITY ANALYST

December 2019 – December 2020

- Web, Network and Mobile Penetration Test

SECURITY ANALYST

June 2019 – December 2019

- Web and Network Penetration Test

SECURITY ASSOCIATE

March 2018 – June 2019

- OSINT and Threat Intelligence activities
- Managed the server of the Threat Intelligence Platform
- Malware and Phishing Analysis

### Argo Software

EXTERNAL COLLABORATION

December 2017 – December 2017

- Security Audit Web Infrastructure

### Alpha Institute of Geopolitics and Intelligence

EXTERNAL COLLABORATION

December 2016 – January 2017

- External collaboration for the preparation of the Ransomware Report 2016 report.

## Skills

---

PROGRAMMING LANGUAGES

- Java, Python, PHP, Shell Scripting, C

WEB PENETRATION TEST

- Deep knowledge of OWASP Top 10.
- Knowledge of advanced attacks, like Bypass CSRF, Blind XXE and so on.
- Ability to perform a deep analysis on decompiled web app source code.
- Ability to exploit vulnerabilities by chaining them into complex attacks.

MOBILE PENETRATION TEST

- Static and Dynamic Analysis on Android and iOS applications.
- Usage of tools like Jadx, Objection, Frida, etc.
- Ability to read Java in order to craft custom exploit.

#### NETWORK PENETRATION TEST

- Using information gathering techniques to identify and enumerate targets running various operating systems and services.
- Conducting remote and local privilege escalation.
- Leveraging tunneling techniques to pivot between networks.

#### THICK CLIENT PENETRATION TEST

- Ability to enumerate services on Windows Platform.
- Knowledge of Decompilation tool like Dnspy, DotPeek, etc.
- Ability to perform a deep analysis on decompiled windows app source code.
- Ability to exploit vulnerabilities by chaining them into complex attacks.

#### SOFT SKILLS

- Ability to communicate technical vulnerabilities to developers and C-Level.
- Managed the activities from the planning to the delivery.
- Worked with application developers to validate, assess, understand root cause and mitigate vulnerabilities.

## Projects

---

### Hacktips

SITE FOCUSED ON INFORMATION SECURITY GUIDES

<https://hacktips.it>

### A Model Driven Approach to Generate Cyber Ranges

MASTER DEGREE THESIS

[https://toccagni.info/doc/master\\_thesis.pdf](https://toccagni.info/doc/master_thesis.pdf)

### Side channel cache attacks on ARM

BACHELOR DEGREE THESIS

[https://toccagni.info/doc/bachelor\\_thesis.pdf](https://toccagni.info/doc/bachelor_thesis.pdf)

## Awards

---

2023	<b>OSED</b> , An OffSec Exploit Developers (OSEDs) have the skills and expertise necessary to write their own shellcode and create custom exploits from scratch	<i>Offsec</i>
2021	<b>GIAC Mobile Device Security Analyst (GMOB)</b> , GMOB certification holders have demonstrated knowledge about assessing and managing mobile device and application security	<i>SANS</i>
2020	<b>CVE-2020-13872</b> , RoyalTS SSH Tunnel Authentication Bypass.	
2019	<b>OSCP</b> , An OSCP is able to research a network, identify vulnerabilities and successfully execute attacks.	<i>Offsec</i>
2018	<b>Hall of Fame</b> , Fastweb, Telecom Italia, Europa.eu	