Pietro F. **Tirenna**

Security Passionate · Software Engineer

me@pftirenna.tech madt1m.github.io madt1m pietroftirenna

"The modern masters promise very little; they know that metals cannot be transmuted and that the elixir of life is a chimera, but these philosophers, whose hands seem only made to dabble in dirt, and their eyes to pore over the microscope or crucible, have indeed performed miracles."

Education

Politecnico di Torino — *Torino, Italy*

LM-32 (DM270) in Ingegneria Informatica (Computer Engineering), 110L/110 (summa cum laude) — *2017 - 2020*

- Core Member of the CTF (Capture The Flag) team.
- Thesis with title "Techniques for malware analysis based on symbolic execution", an experimental study of how to extract interesting properties from malwares by using advanced binary analysis techniques such as symbolic execution (more in portfolio).

Politecnico di Torino — *Torino, Italy*

CyberChallenge.IT18 Trainee — *Feb. 2018 - Jul. 2018*

- Hands-On training on Secure Coding, Web Application Hacking, Binary Exploitation, Computer Forensics, Penetration Testing, Reverse Engineering.
- Finalist in the national security challenge with PoliTO team.

School of Entrepreneurship and Innovation — *Torino, Italy*

SEI Inventor — *Feb. 2018 - Feb. 2018*

- 10 days Bootcamp on Entrepreneurship and Innovation.
- 2nd place in final competition between start-ups.

University of Catania — *Catania, Italy*

B.S. in Computer Science and Engineering — *2013 - 2017*

- Member of the Linux User Group.
- Worked in a 3D-printing and Makers' lab building AirSoft prototypes.

Experience

Freelancer — *Remote*

Red Teaming & Software Engineering — *2018 - PRESENT*

- **Programming** - design and development of software projects such as command line utilities, web applications, scripts, data science.
- **Red Teaming** - Penetration testing, vulnerability assessments, threat modeling, code review, security research for exploits in various types of applications.
- **Technical Documentation** - Review of literature, tutorial & writeups, comparative analysis of different solutions and analysis of tools.

Appcensus — *California, US*

Software & Security Engineer — *Oct 2020 - PRESENT*

- **Security Engineering** - performing security reviews of web applications, using tools such as mitmproxy, AWS cloud architecture considerations with respect to security posture, security testing of android mobile applications through various tools such as adb, frida and JADX-GUI.
- **Software Engineering** - developing and engineering software in various programming languages and environment, such as Python, Javascript and C++. Implementing kernel-level modules and code on the iOS and Android ecosystems.
- **System Design** - consider various aspects, such as scalability, availability, security and other cross-cutting concerns while engineering systems to support business requirements.

Blueliv

Barcelona, Spain

Red Team Analyst

Sep 2019 - Sep 2020

- **Threat Intelligence** - conducting OSINT analysis through Google Dorks, VirusTotal API, Shodan, PassiveTotal RiskIQ, common bash utilities and other threat intelligence services to uncover interesting information in malware-related campaigns.
- **Pentesting** - information gathering of target networks using OSINT, service/content enumeration via tools such as nmap, burpsuite, wfuzz, dirbuster, exploitation/post-exploitation with exploitdb, manual exploits, metasploit and meterpreter to obtain/maintain shells on target, Active-Directory red-teaming techniques using Powershell, Empire, PowerSploit and similar tools (depending on the scenario).
- **Malware Analysis** - disassembling/decompiling malicious binaries through experienced usage of tools like IDA, Ghidra, dnSpy, hooking and analysing interesting malware properties via API hooking, memory introspection, network analysis and debugging. When needed, patching of binary code to skip unnecessary/dangerous sections or to facilitate the deobfuscation process.

Telsy

Torino, Italy

Cyber Specialist

May 2019 - Aug. 2019

- Developed code in Python to automate infrastructure-concerning tasks.
- Web Application Penetration Testing.
- Malware Analysis.

Politecnico di Torino

Torino, Italy

CyberChallenge.IT19 Trainer

Feb. 2019 - Jul. 2019

- Supported the CyberChallenge.IT Program at university with traning on Binary Exploitation and Reverse Engineering.

Google Summer of Code with Honeynet Organization

Torino, Italy

Python OS Developer - Apprenticeship Program

May 2018 - Aug. 2018

- Developed code for **mitmproxy** during the summer.
- Built a new serialization format based on Google Protocol Buffers, using it to lay the foundations for live Sessions on disk.
- Final Report at `https://madt1m.github.io//2018/summer_of_code/`

Skills & Tools

Programming Languages

Full-stack

- C/C++, Rust, ASM x86/ARM/MIPS
- Python, Go, Ruby, Java
- Javascript, HTML, CSS

Technologies

Network, Cloud, Operating systems

- ISO/OSI, HTTP, TLS, Websocket
- AWS EC2, ECS, Cloudwatch, Cognito, Lambda, S3
- Operating systems (memory, file, processes, threading handling)
- Firmware dumping, reverse engineering, binary-level analysis and patching, debugging

Tools

Web Analysis, Reverse Engineering, Binary Exploitation

- IDA, Ghidra, radare2, GDB
- Burpsuite, ZAP, mitmproxy
- Bash, Wireshark
- Wfuzz, ffuf, scrapy, gobuster

Selected Portfolio

Interesting projects in my path

- `https://github.com/madt1m/symba` - My MSc Thesis project, a tool written in Python which employs Symbolic Execution to extract interesting properties from malware.
- `https://madt1m.github.io//2018/icectftwitter/`, `https://madt1m.github.io//2018/icectffermat/` - Writeups compiled for a couple of CTF challenges concerning reverse engineering, binary analysis and exploitation.
- `https://madt1m.github.io//2018/summer_of_code/` - Final report for my Google Summer of Code experience.
- `https://github.com/madt1m/npmbeer-pedibus` - A web application written in Spring Boot + MongoDB + AngularJS to schedule and book reservations of a Pedibus.

Extracurricular Activity

Honeynet Organization - Sysenter Chapter

Worldwide

Contributor

2019 - PRESENT

- Open Source tools development
- Research on Honeypots and Threat Intelligence

PoliTHack - pwnthem0le

Torino, Italy

Core Member

Feb. 2019 - PRESENT

- CTF competitions.
- Activities to raise awareness.
- Pentesting and Scanning of the University Network Infrastructure.

Honors & Awards

2019	**Qualified for CSAW Finals**, CSAW Europe Finals - pwnthem0le	*Valence, Europe*
2019	**Cédric Blancher Memorial Scholarship**, Honeynet Annual Workshop	*Innsbruck, Austria*
2019	**3d Place**, CY4GAMES CTF	*Rome, Italy*
2018	**Finalist**, CyberChallenge.IT18 Finals	*Rome, Italy*
2018	**2nd Place**, SEI Inventor	*Torino, Italy*

Presentations

M0lecon 2019 - Web Exploitation Workshop

Torino, Italy

Speaker

Nov 2019

- Held a workshop on client-side web application techniques and how actors can use them in the wild.

Linux Hardening Open Day

Catania, Italy

Speaker

Jun. 2016

- Presented a comparison study on the effectiveness of OS Hardening solutions - SELinux, Tomoyo, App armor, GrSecurity - against 0-day exploits.