Stefano Paolo Costa

Formal education in Physics and Computer Science, a publication in each and four years of research. Self taught in offensive hacking and machine learning. Former leader of a successful hacking team 0x90skids. Hacked and disclosed JP Morgan Chase Bank vulnerability that could duplicate money. Currently building an ML/AI internet activity fingerprinter to track criminals even through VPNs. Versed in way too many tools and languages, best language is currently Python. Native English speaker, also fluent in French and Italian.

PROFESSIONAL EXPERIENCE

ORACLE — Senior Security Researcher *Sep 2022 – Present*

- Engaged in constant application pentesting and software assurance for users' security and privacy on services with direct effects world wide.
- Developing and managing cutting edge tools and practices for software assurance on extremely critical and hazardous infrastructure.
- Performing in-depth security assessments leveraging results from Static Code Reviews (SAST), Penetration Testing and Red Team Operations (DAST).
- Creating Python testing tools to help engineering teams identify security-related weaknesses and improve team efficiency and response time.
- Devised methods to incorporate knowledge of artificial intelligence tools in Python on large databases to identify threat actors' attempts to manipulate data.
- Mentoring and managing Security Researchers and Software Engineers on best defensive practices and offensive techniques.
- Planing and leading execution of cyber defenses aligning with program timelines while communicating vulnerabilities in a clear and concise manner to all the stakeholders.

PingIdentity — Product Security Engineer *Sep 2021 – Aug 2022*

- Black box pentested and managed external pentests on company acquisition for safe suite incorporation and market deployment.
- Refactored outdated architecture to increase security, efficiency and alleviated current and future technical debt.
- Regularly threat modeled products, advised engineers and practiced static code analysis in Java with dynamic runtime fuzzing and manual review.
- Consulted, trained and advised multiple development teams on best security practices using vulnerability PoCs, commercial tools such as Snyk and Fortify in addition to custom tools built in Python.
- Effectively communicate and formally present technical concepts, researched tools and techniques as well as personally developed skills from daily CTFs and OSCP practice and continued education.

poly — Security and Development Engineer *Jun 2018 – Aug 2021*

- Designed and built secure Python websockets and microservices, allowing hundreds of customers' jump server application passwords and log data to be updated and pulled remotely from a secure Django web application.
- Routinely practiced proper Dev Ops life cycle, including Jira ticketing systems, infrastructure and configuration management, static code analysis and built CI/CD pipeline for automated docker deployment.
- Regularly used various enumeration tools such as nmap, Wireshark, Burp Suite to solve and/or secure network infrastructure and application issues for virtual machines, firewalls, proxies and VPN access.
- Led white hat penetration testing to evaluate internal infrastructure and application security.

EDUCATION

Berkeley UNIVERSITY OF CALIFORNIA

— Professional Certificate in Machine Learning and Artificial Intelligence *Mar 2023*

Network Activity Fingerprinter Capstone Project: https://github.com/Charm-q/AI-Capstone

OFFENSIVE® security

Offensive Security Certified Professional *Jul 2022*

Highly regarded offense cyber security certificate requiring rooting five computers in 24 hours.

University of Colorado Boulder

Double Bachelor's in Physics and Computer Science *Dec 2019*

Four years of research with two publications, one in progress.

RESEARCH

— Li-Fi

Researching potential replacement for Wi-Fi using higher frequencies for theoretically faster transfer speeds.

Publication pending.

— Engineering Research

Professor Alan Mickelson's Engineering research group for off-grid solar powered communication systems in underdeveloped nations.

Publication: https://ieeexplore.ieee.org/document/8239268

— Nano-Optics Research

Under Markus Raschke, using near-field and far-field spectroscopy to probe material properties with nanoscale and femtosecond resolution.

Publication: Available on request.

VULNERABILITY DISCLOSURE

— JP Morgan & Chase Hall of Fame

Disclosed USD duplication exploit:
https://responsibledisclosure.jpmorganchase.com/hc/en-us/articles/360023828114

TOOLS AND TECHNICAL KNOWLEDGE

Python, Tensorflow, sklearn, numpy, seaborn, pandas, jupyter, C, C++, Bash, Javascript, Java, Node.js, PHP, HTML, Assembly, Cron, MySQL, PostgreSQL, Git, AWS, Wireshark, Kali, Metasploit, Mimikatz, Burp Suite, Postman, Nmap, Visual Studio, GitHub, React, Angular, Django, Flask, Powershell, Netcat, Arduino, Raspberry Pi, Active Directory, VMs, Bloodhound, Cryptography,