Amirhossein Roustaei

Red Team Operator · Penetration Tester

Portfolio Links

amir@eternull.ink · linkedin.com/in/amirhroustaei · github.com/EterNullSec · Hack The Box · HackerOne · Genoa, Italy

SUMMARY

Offensive security professional specializing in adversary emulation against enterprise Active Directory environments. I design and execute full-spectrum red team engagements simulating advanced threat actors — from initial foothold to domain dominance — utilizing Kerberos abuse, credential extraction, ACL exploitation, and OPSEC-aware C2 operations. Author of MadEzmaC2, a Python-based asynchronous C2 framework. Actively seeking pentesting and red team roles.

EXPERIENCE

Red Team Operator
Sep 2025 – Present

Eternull Security · Full-time · Italy

– Active Directory red team operations and full-scope adversary emulation engagements

– C2 infrastructure deployment, OPSEC-aware beaconing, and EDR evasion tradecraft

– Kerberos abuse, ACL exploitation, credential extraction, lateral movement, and domain dominance

Help Desk Operator
May 2020 – Jun 2024

MTN Irancell · Full-time

– Technical support and incident resolution for enterprise telecom infrastructure

PROJECTS

MadEzmaC2 — Asynchronous SSH-Based C2 Framework

Python-based proof-of-concept C2 framework using AsyncSSH and asyncio. Implements asynchronous multi-session handling, encrypted remote command execution, SFTP file transfer, and Ngrok-based NAT traversal. Optional SOCKS5/TOR proxy routing. Designed for red team labs and adversary emulation research.

Python · AsyncSSH · asyncio · Ngrok · SFTP · SOCKS5

Active Directory Attack Lab

Self-hosted enterprise AD environment for researching modern attack chains — ADCS ESC1–ESC8 abuse, Kerberoasting, DCSync, RBCD delegation, and ACL-based privilege escalation with full kill-chain documentation.

PUBLICATIONS

Exploiting Polkit (CVE-2021-3560): Race Condition to Root on Linux · Medium, Mar 2026
Technical analysis of CVE-2021-3560 — Polkit authorization model, D-Bus IPC, and step-by-step exploitation.

Unquoted Service Path Exploitation — Active Directory Lab Series · Medium, 2025
Deep dive into Windows service path resolution and reliable local admin privilege escalation.

CERTIFICATIONS

Certified Red Team Operator (CRTO) · Altered Security

Certified Penetration Testing Specialist (CPTS) · Hack The Box

Certified Red Team Professional (CRTP) · Altered Security

SKILLS

C2 & Implant Dev	MadEzmaC2 (authored) · Cobalt Strike · Havoc · AV/EDR bypass · In-memory execution
Active Directory	BloodHound · Kerberoasting · ASREPRoast · ADCS ESC1–ESC8 · DCSync · Pass-the-Hash · RBCD
Web & Bug Bounty	IDOR · Auth bypasses · Business logic flaws · SSRF · XXE · SSTI · API security testing
Tooling	Python · PowerShell · C# · Impacket · Certipy · Rubeus · Burp Suite Pro · Nmap · Nuclei
Platforms	Hack The Box · HackerOne

EDUCATION

MSc Engineering Technology for Strategy & Security (Strategos) — Sep 2024 – Present
Università degli Studi di Genova

BSc Electrical and Electronics Engineering — Sep 2019 – Aug 2023
Islamic Azad University, North Tehran Branch

LANGUAGES

English — Full Professional · Persian — Native · Italian — Elementary