Amirhossein Roustaei

Red Team Operator · Penetration Tester

Portfolio-Links

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

PROFIL

Offensive-Security-Spezialist mit Schwerpunkt auf Adversary Emulation in Active-Directory-Unternehmensumgebungen. Planung und Durchführung vollständiger Red-Team-Engagements - vom initialen Zugriff bis zur Domänenkompromittierung - mit Kerberos-Angriffen, Credential Extraction, ACL-Ausnutzung und OPSEC-bewussten C2-Operationen. Entwickler von MadEzmaC2, einem asynchronen C2-Framework auf Python-Basis. Offen für Positionen im Penetration Testing und Red Teaming.

BERUFSERFAHRUNG

Red Team Operator
Sep. 2025 - heute

Eternull Security · Vollzeit · Italien

– Red-Team-Operationen in Active-Directory-Umgebungen und umfassende Adversary-Emulation-Engagements

– Bereitstellung von C2-Infrastruktur, OPSEC-bewusstes Beaconing und Techniken zur EDR-Umgehung

– Kerberos-Angriffe, ACL-Ausnutzung, Credential Extraction, Lateral Movement und Domänenkompromittierung

Helpdesk-Mitarbeiter
Mai 2020 - Juni 2024

MTN Irancell · Vollzeit

– Technischer Support und Störungsbehebung für Telekommunikationsinfrastruktur im Unternehmensumfeld

PROJEKTE

MadEzmaC2 - Asynchrones SSH-basiertes C2-Framework
Python-basierter Proof of Concept mit AsyncSSH und asyncio. Unterstützt parallele Sitzungen, verschlüsselte Remote-Befehlsausführung, SFTP-Dateitransfer und NAT-Traversal über Ngrok. Optionales Routing über SOCKS5/TOR. Entwickelt für Red-Team-Labore und Adversary-Emulation-Forschung.

Python · AsyncSSH · asyncio · Ngrok · SFTP · SOCKS5

Active Directory Attack Lab
Selbst gehostete AD-Unternehmensumgebung zur Erforschung moderner Angriffsketten: ADCS ESC1-ESC8, Kerberoasting, DCSync, RBCD-Delegation und ACL-basierte Privilegienausweitung mit vollständiger Kill-Chain-Dokumentation.

PUBLIKATIONEN

Exploiting Polkit (CVE-2021-3560): Race Condition to Root on Linux · Medium, März 2026
Technische Analyse des Polkit-Autorisierungsmodells, der D-Bus-IPC und der schrittweisen Ausnutzung.

Unquoted Service Path Exploitation - Active Directory Lab Series · Medium, 2025
Analyse der Windows-Dienstpfadauflösung und einer reproduzierbaren lokalen Privilegienausweitung zum Administrator.

ZERTIFIZIERUNGEN

Certified Red Team Operator (CRTO) · Altered Security

Certified Penetration Testing Specialist (CPTS) · Hack The Box

Certified Red Team Professional (CRTP) · Altered Security

FACHKENNTNISSE

C2 & Implant Development	MadEzmaC2 (Entwickler) · Cobalt Strike · Havoc · AV/EDR-Umgehung · In-Memory-Ausführung
Active Directory	BloodHound · Kerberoasting · AS-REP Roasting · ADCS ESC1-ESC8 · DCSync · Pass-the-Hash · RBCD
Web & Bug Bounty	IDOR · Authentifizierungs-Bypässe · Business-Logic-Fehler · SSRF · XXE · SSTI · API-Sicherheitstests
Tooling	Python · PowerShell · C# · Impacket · Certipy · Rubeus · Burp Suite Pro · Nmap · Nuclei
Plattformen	Hack The Box · HackerOne

AUSBILDUNG

MSc Engineering Technology for Strategy & Security (Strategos) Sep. 2024 - heute
Università degli Studi di Genova

BSc Elektrotechnik und Elektronik Sep. 2019 - Aug. 2023
Islamic Azad University, North Tehran Branch

SPRACHEN

Englisch - Verhandlungssicher · Persisch - Muttersprache · Italienisch - Grundkenntnisse