ANAS MOHAMMED

Offensive Security Researcher · Red Team Operator · Malware Developer

Cairo, Egypt · +201062907978 · skoveit@proton.me · Portfolio · GitHub · LinkedIn

PROFILE

Final-year Computer Engineering student and **2nd highest** contributor to the **Sliver** C2 framework 2025, the industry-standard adversary emulation platform. Author of SkoveNet, a fully decentralized C2 framework built to simulate resilient APT operations. Discovered and responsibly disclosed multiple **CVEs**. Deep expertise in Windows Internals, EDR evasion, and adversary simulation at an advanced level.

CORE SKILLS

Web Application & API Pentesting

- Race conditions, SSRF, SSTI, XXE, logic flaws
- GraphQL introspection & injection attacks
- OAuth 2.0 / JWT — token forgery & misuse
- Chained multi-stage exploit development

Active Directory & Red Team

- Kerberoasting, AS-REP roasting, DCSync, ACL abuse
- Attack path analysis & privilege chain mapping
- DACL manipulation & GPO abuse
- Full adversary simulation engagements

Malware Development & Evasion

- Custom implants in C/C++, Go, Assembly
- EDR & AV evasion — syscalls, process injection
- Shellcode staging & reflective loading
- C2 framework development & operation

Security Research

- Source code auditing for novel vulnerabilities
- PoC exploit development for disclosed CVEs
- Zero-days in nHost, tempo, sliver c2
- Bug Bounty — HackerOne & Intigriti

Software Development

- Go / C / C++ / Python / Rust / Assembly
- Competitive programmer (Codeforces)
- Design patterns & system architecture
- Concurrent & asynchronous systems

Systems & Infrastructure

- Windows Internals — kernel, memory, NT APIs
- Linux internals & privilege escalation
- Networking — protocol-level attack chains & analysis
- Exploit dev — ROP chains, mitigation bypass

PROJECTS & RESEARCH

Sliver C2 Framework 2025 – Present

- Ranked **2nd** highest contributor to Sliver (industry-leading adversary framework) core features.
- Disclosed **CVE-2026-32941, CVE-2026-34227** and **CVE-2026-29781**.

SkoveNet

- Engineered fully decentralized C2 architecture to simulate resilient APT ops - no single point of failure.
- Modular post-exploitation: automated persistence, covert channels, lateral movement support. (Github - Docs)

Writeups & technical notes

Nhost Bug Bounty · Intigriti

High-severity vulnerability in Nhost open-source backend platform: **CVE-2026-34200**.

CERTIFICATIONS & TRAINING

OSCP	Offensive Security Certified Professional	*Labs Completed & Exam In Progress*
CRTO	Certified Red Team Operator — Red Team Ops	*Labs Completed & Exam In Progress*
Maldev Academy	Advanced Malware Development & EDR Evasion	*Completed*
PortSwigger WSA	Web Security Academy — 100% of Labs	*Completed*

EDUCATION

B.Sc. Computer Engineering — New Mansoura University Expected 2027