M. UMER FAROOQ

RED TEAM / OFFENSIVE SECURITY

+92 321 9400902 | Umerf2700@gmail.com | github.com/ben-slates
linkedin.com/in/m-umer-farooq-a2a0b7213 | HackTheBox — Hacker Rank

PROFILE

Offensive security enthusiast and Computer Science student with hands-on experience in red team operations, C2 framework development, and Active Directory exploitation. Hack The Box Hacker rank, 40–50% through the CPTS path, and 80% through the Junior SOC Analyst path. Passionate about adversary simulation and building offensive tooling from scratch.

PROJECTS

DNS-Based C2 Framework *Rust · Python · DNS · AES-256*

- Built a full C2 framework from scratch — Rust implant with DNS tunneling exfiltration and a Python C2 server with operator console.
- AES-256 encrypted comms over DNS TXT records, jitter-based beaconing, and process injection for EDR evasion.
- Modular post-exploitation: keylogging, screenshot capture, reverse shell, file transfer — all tunnelled over DNS.
- Low-and-slow stealth design: randomised subdomain generation and living-off-the-land execution techniques.

Offensive Security Toolkit — FYP *ESP32 · Python · Kali Linux · Hardware*

- Built a portable multi-vector attack platform: WiFi deauth/PMKID capture, RFID cloning (RC522), and HID injection.
- Combined ESP32 hardware with Kali Linux tooling for a field-deployable red team device.
- Attack surface spans wireless, physical access, and HID-based social engineering delivery vectors.

CyberSim — AI Incident Response Platform *Node.js · Express · Gemini AI · MongoDB*

- Simulated SOC environment powered by Gemini AI — generates realistic attack scenarios and scores analyst decisions in real time.
- Backend manages scenario state, threat narrative generation, and adaptive difficulty based on response quality.

TECHNICAL SKILLS

OFFENSIVE / RED TEAM

- Penetration Testing Methodology
- Active Directory Attacks (Kerberoasting, Shadow Credentials)
- Privilege Escalation — Linux & Windows
- C2 Framework Development
- HID / RFID Hardware Attacks
- WiFi Attacks (PMKID, Deauth)

DEVELOPMENT

- Rust — systems & implant development
- Python — automation, C2, scripting
- Node.js / Express.js
- Bash scripting

TOOLS & PLATFORMS

- Nmap, Burp Suite, Metasploit
- Wireshark, BloodHound, Evil-WinRM
- Hack The Box (Hacker Rank)
- Kali Linux (primary OS)

NETWORKING & PROTOCOLS

- TCP/IP, DNS, HTTP/HTTPS
- Packet analysis & traffic inspection
- DNS Tunneling
- Active Directory / LDAP

HTB TRAINING

Hack The Box — Hacker Rank

10+ machines pwned including CVE-based retired boxes: Next.js auth bypass, Node.js inspector privesc, AD Shadow Credentials + DLL hijack chain.

CPTS Path (HTB) — completed

Covers web app attacks, Active Directory exploitation, pivoting, post-exploitation, and professional reporting.

Junior SOC Analyst Path (HTB) — ~80% complete

Covers log analysis, SIEM, threat intel, phishing analysis, and incident response procedures.

EDUCATION

University of Agriculture, Faisalabad 2023 – 2027
B.S Computer Science

Bellows College 2021 – 2023
Intermediate (Biology)

INTERESTS

Ethical Hacking · Red Teaming · Exploit Development · Vulnerability Research · Security Automation · CTF Competitions · Malware Analysis