Umar Mushtaq
Penetration Tester / Red Team Operator
WA/Cell: +971 55 7221997 | Umar.Mushtaq46@outlook.com
References: Available on Request

SUMMARY OF QUALIFICATIONS

Seasoned Penetration Tester and Red Teamer with 6+ years of hands-on experience, adept at evaluating web/mobile, network infrastructure, and social engineering. Accomplished in steering and executing high-impact international penetration test projects, serving as a trusted advisor to many organizations & companies, elevating their cybersecurity maturity. Devoted to bug hunting and excelling in CTF programs.

CERTIFICATIONS & BADGES

- **OFFSEC** OSCP **(**Offensive Security Certified Professional**)**
- **HACK THE BOX** CPTS **(**Certified Penetration Testing Specialist)
- **HACK THE BOX** CBBH (Certified Bug Bounty Hunter)
- **HACK THE BOX** CDSA (Certified Defense Security Analyst)
- **ZEROPOINT** CRTO (Certified Red Team Operator)
- **ALTERED SECURITY** CRTE (Certified Red Team Expert)
- **ALTERED SECURITY** CRTP (Certified Red Team Professional)
- **TCM SECURITY** PNPT (Professional Network Penetration Tester)
- **EC-COUNCIL** CEH v12 (P) (Certified Ethical Hacker Practical)
- **INE** eCPPT v2 (Certified Professional Penetration Tester)
- **SecOps** CNSP (Certified Network Security Practitioner)
- **HACK THE BOX – PRO LABS** ZEPHYR | DANTE | RASTALABS | CYBERNETICS

HALL OF FAME

- WHO (World Health Organization)

AREA OF EXPERTISE

- External / Internal VAPT & Audit
- Threat Modelling
- Phishing Assessments
- Security Tools (e.g. Burpsuite, ZAP, MSF)
- Cloud Penetration Testing
- Cobaltstrike, Sliver, Empire & Mythic
- BloodHound & Pingcastle
- Programing Skills (Python, PS, Batch, Bash)
- Social Engineering Assessments
- Secure Coding Review (SAST / DAST)
- MOBSF, DEX2JAR, GHIDRA, FRIDA, GDB
- Android & IOS / Web Application VAPT
- Malware Analysis & Reverse Engineering
- AD Red Teaming Assessments
- Nessus, NetSparker, Acunetix, Openvas & Nexpose

PROFESSIONAL EXPERIENCE

ValueMentor, Abu Dhabi (April 2025 – Currently)
Sr. Cybersecurity Specialist

- Led and executed comprehensive VAPT engagements across enterprise networks, web applications, APIs, and cloud infrastructure, uncovering critical vulnerabilities and delivering actionable remediation reports.
- Plan, execute, and report on Red Team operations to simulate real-world attack scenarios, assess organizational resilience, and enhance incident response strategies.
- Collaborated with Blue Teams to enhance detection rules and incident response procedures based on Red Team findings
- Orchestrated full-scope internal and external penetration tests, including OSINT, initial access, privilege escalation, and data exfiltration phases, simulating real-world attacker TTPs.

SoftTech Consultancy, Abu Dhabi (Oct 2024 – May 2025)
Sr. Security Analyst

- Develop and implement customized security recommendations, collaborating with cross-functional teams to strengthen overall security posture..
- Perform threat modeling and adversary emulation to replicate tactics, techniques, and procedures (TTPs) of advanced attackers, ensuring robust defensive measures are in place.
- Conducted automated and manual penetration testing to identify vulnerabilities and potential threats in web and mobile applications.
- Conducted in-depth manual testing to identify potential vulnerabilities that may be missed by automated scans.

Technolytics, United States (***Feb 2022 – May 2024) [Remote]***
Lead Penetration Tester

- Managed Special Penetration Test Projects Based in Several Countries UAE, OMAN & US
- Managed VAPT Program
- Spearheaded red team exercises to simulate cyber-attacks, revealing vulnerabilities and providing actionable insights.
- Led multi-platform Vulnerability Assessment and Penetration Testing (VAPT) campaigns covering web, mobile applications, and APIs, ensuring holistic security evaluation across diverse digital environments.
- Deployed Secure Enterprise Mail systems holding 250 to 15000 users using latest hardware Using the least hardware in private clouds away from big cloud providers such as Microsoft, Google, Amazon

HorizonTech *(May 2020 – Jan 2022)*
Senior Penetration Tester / Red Team Operator

- Team Lead in Red Team operations and led specialized Penetration Testing projects, enhancing cybersecurity posture.
- Provided expert-level Penetration Testing and Red Teaming services, identifying vulnerabilities and recommending mitigation measures.
- Managed specialized projects, collaborating across teams to assess and mitigate security risks effectively.
- Employed advanced attack methodologies to simulate real-world threats, uncovering potential weaknesses.
- Maintained comprehensive documentation and mentored junior team members to foster skill development.
- Performed physical security assessments on multiple companies

Bug Bounty Hunter (Jan 2019 – April 2020)

- Proficient in recognizing critical security risks through a strong grasp of OWASP Top Ten principles.
- Expertise in dissecting intricate application architectures to reveal potential avenues for exploitation
- Well-versed in authentication and authorization mechanisms such as JWT, OAuth, and session management.
- Demonstrated experience in identifying and exploiting privilege escalation vulnerabilities to evaluate system-wide security.

- Proficient in employing API fuzzing techniques to detect security weaknesses and injection flaws effectively.
- **Bugs Found**
    - ROZEE.PK (Information Disclosure) - Pakistan
    - NETSOLTECH.COM - Pakistan & (Several others)

KEY ROLE & REDTEAM ENGAGEMENTS

- Conducted Phishing assessments upon company requests & Ransomware mitigation.
- Executed red teaming exercises to simulate sophisticated cyber-attacks, emulating advanced adversaries and testing the effectiveness of defensive measures.
- Created custom exploits and payloads to demonstrate vulnerabilities and potential exploitation scenarios.
- Worked closely with cross-functional teams to develop and execute attack strategies, ensuring a holistic approach to security testing.
- Delivered detailed reports outlining identified vulnerabilities, along with prioritized recommendations for remediation.
- Assessed the overall security posture of organizations, including evaluating the effectiveness of security controls, incident response, and detection mechanisms.
- Maintained up-to-date knowledge of the latest cybersecurity threats, tactics, techniques, and procedures (TTPs) used by malicious actors.
- Designed and executed social engineering campaigns, including phishing exercises, to assess the susceptibility of personnel to targeted attacks.
- Evaluated physical security controls and protocols to identify potential weaknesses and vulnerabilities in the organization's premises.
- Managed and maintained the infrastructure used for red teaming exercises, ensuring a reliable and realistic testing environment.
- Articulated the business impact of security vulnerabilities, helping stakeholders understand the potential consequences and prioritize remediation efforts.

NETWORKING SKILLS

Network Technologies and Network Security

- Network Architectures, Protocols, IP Addressing, Subnetting, Routing, Switching, Network Security, and Network Troubleshooting.
- Practical skills in configuring and managing cisco routers and switches, implementing network security measures, and working with IP services.
- The knowledge and skills necessary to design, build, and maintain small to medium-sized networks.
- Endpoint Security, have a broad understanding of advance concepts of network security, as well as operating systems and endpoint security – networking devices and initial configuration, Cisco 2.

EDUCATION & PUBLIC PROFILE

Beaconhouse School System O-LEVELS (2012-2014)
Beaconhouse School System A-LEVELS (2014-2016)

LinkedIn: Umar Mushtaq | LinkedIn