

## SUMMARY OF QUALIFICATIONS

---

Seasoned Penetration Tester and Red Teamer with 4+ 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 government organizations, elevating their cybersecurity maturity. Devoted to bug hunting and excelling in CTF programs.

## CERTIFICATIONS & PROFESSIONAL TRAINING

---

<b>OFFENSIVE SECURITY</b>	Offensive Security Certified Professional – In Progress
<b>EC-COUNCIL</b>	CEH (Certified Ethical Hacker) – 75%
<b>INE</b>	eCPPT v2 (Certified Professional Penetration Tester)
<b>ZEROPOINT</b>	CRT0 (Certified Red Team Operator)
<b>ALTERED SECURITY</b>	CRT0 (Certified Red Team Professional)
<b>SecOps</b>	CNSP (Certified Network Security Practitioner)
<b>HUAWEI</b>	HCNA (Huawei Certified Network Associate)
<b>HTB</b>	ZEPHYR (Hack the Box – Pro Labs)
<b>HTB</b>	DANTE (Hack the Box – Pro Labs)
<b>HTB</b>	RASTALABS (Hack the Box – Pro Labs)
<b>HTB</b>	CYBERNETICS (Hack the Box – Pro Labs)

## PROFESSIONAL EXPERIENCE

---

**SKILL.PK**, Pakistan

***Application & Infrastructure Security Expert (2020 – 2021)***

**HORIZON TECH**, Pakistan (2021 – 2023)

***Application & Infrastructure Security Expert***

- Managed Special Penetration Test Projects
- Team Lead Red Team Operations
- Managed Internal VAPT Program

***PENETRATION TESTER – Self Employed (2019 – Present)***

- 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.
- Worked with development teams to ensure that identified vulnerabilities were addressed and remediated in a timely and effective manner.
- Utilized Kali Linux & Parrot, a powerful and versatile penetration testing distribution, to conduct comprehensive security assessments of web applications, network systems, and infrastructure.
- Leveraged Kali Linux's extensive collection of pre-installed tools and utilities, including Metasploit, Nmap, and Wireshark, to conduct comprehensive scans and identify potential vulnerabilities and threats.
- Documented and reported identified vulnerabilities and potential threats to stakeholders, providing detailed recommendations for remediation and risk mitigation.

### **CYBER SECURITY CONSULTANT (2020 – Present)**

- Provided expert cybersecurity advice and guidance to individuals and agencies, helping them to prevent and mitigate security threats and attacks.
- Assisted individuals and organizations in the aftermath of security incidents, providing support and advice to restore security and minimize damage.
- Built strong relationships with clients, serving as a trusted advisor and resource for cybersecurity-related issues and concerns.
- Delivered presentations and talks on cybersecurity to a variety of audiences.
- Utilized engaging and interactive approaches to cybersecurity education, leveraging real-world examples and scenarios to make complex topics accessible and understandable to a broad range of audiences.
- Received positive feedback and high ratings from audiences for the quality and value of presentations and talks on cybersecurity.
- Stayed up-to-date with the latest trends and best practices in cybersecurity, continually expanding knowledge and skills to provide the most effective and relevant advice and guidance.

### **Ministry Of Defense, Pakistan**

#### ***Penetration Tester & Red Team Operator (July 2021 – May 2023)***

- Provided Penetration Testing and Red Teaming services to the Government
- Managed Special Penetration Testing and Red Teaming Projects
- Team Lead Red Team Operations

### **Hacker One, BUGCROWD, INTEGRITY**

#### ***Bug Bounty Hunter (2013 – 2020)***

- Bugs Found
  - ROZEE.PK
  - NETSOLTECH.COM
  - Several others

### **KEY ROLE**

---

- Performed thorough penetration tests and vulnerability assessments to identify weaknesses in systems, networks, and applications.
- 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.
- 10. Conducted security awareness training for staff, educating them on the latest threats and promoting a culture of security.

- Collaborated in the development of incident response plans, ensuring readiness to effectively respond to security incidents.
  - 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
- Characteristics and benefits of cloud and virtualization, explored how to provide internet protocol (ip) addresses to devices, calculate an IP addressing scheme, configured Cisco devices to create a small network and tested for connectivity issues. Participated in up to 7 labs and 12 Cisco Packet Tracer Activities. Plus having hands-on on GNS3

### ***Programming and scripting languages***

- |          |              |
|----------|--------------|
| • Python | • Bash       |
| • PHP    | • PowerShell |
| • SQL    | • Batch      |

### ***Personal Skills***

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• Communication <ul style="list-style-type: none"> <li>○ Presentation Skills</li> <li>○ Active Listening</li> <li>○ Good at Public Speaking</li> <li>○ Teamwork</li> </ul> </li> <li>• Analytical Skills <ul style="list-style-type: none"> <li>○ Have the ability to analyze complex systems and identify vulnerabilities</li> </ul> </li> <li>• Research Skills <ul style="list-style-type: none"> <li>○ The ability to search for, locate, extract, organize, evaluate, and use or present information that is relevant to a particular topic.</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Problem Solving <ul style="list-style-type: none"> <li>○ Know how to define a problem.</li> <li>○ determine the cause of the problem.</li> <li>○ identify, prioritize, and select alternatives for a solution .</li> <li>○ implement a solution. Attention to detail.</li> </ul> </li> <li>• Continuous Learning</li> <li>• Attention to detail</li> <li>• Persistence</li> </ul> |
|---|--|

### ***Languages***

- English: Fluent
- Urdu: Native

## EDUCATION & LINKS

---

Beaconhouse School System Multan O-LEVELS (2013-2015)

Beaconhouse School System Multan A-LEVELS (2015-2017)

Bahaudin Zakariya University Multan BSCS (2017-2020)

Try-Hack-Me: [TryHackMe | Hardcore](#)

LinkedIn: [Daud Khan | LinkedIn](#)

HackerOne: [Daud Khan | Profile | HackerOne](#)

Hack-The-Box: [Hack The Box :: User Profile](#)