Umar Mushtaq
Penetration Tester / Red Team Operator
WA: +971 55 7221997 | rockstar.khan2@gmail.com
PK Cell: +92 303 3311313
Nationality: Pakistani

SUMMARY OF QUALIFICATIONS

Professional Penetration Tester with 4+ years of hands-on experience in Web Applications, Network & Infrastructure Penetration testing. Bugbounty hunter found log4j vulnerability in Github and LinkdIn. Also have penetration testing experience in embedded systems (BVS Devices, RFID, and Wireless Devices). Passionate to work in VAPT including security of Networks, Web/Mobile App, Cloud Security and automation. As a freelancer I have managed and delivered various international penetration test projects remotely. Consulted various government organizations by solving different security issues. Participated in international and local level CTFs Competitions. Recently worked on ChatGPT and was able to get its system internals.

AREAS OF EXPERTISE

PENETRATION TEST	DESKTOP, MOBILE, WEB APP, SERVERS & CLOUD SYSTEMS
PENETRATION TEST	EMBEDDED SYSTEMS INCLUDING PLC AND SCADA NETWORKS
REDTEAMING	NETWORK, SYSTEMS AND WEB APPS
TROUBLESHOOTING	LINUX & WINDOWS
SERVER MANAGEMENT	LINUX & WINDOWS

CYBER AWARENESS & TEACHING
FREQUENCY & WIRELESS
REVERSE ENGINEERING
MALWARE ANALYSIS

CERTIFICATIONS & PROFESSIONAL TRAINING

OFFENSIVE SECURITY	Offensive Security Certified Professional – In Progress
EC-COUNCIL	CEH (Certified Ethical Hacker)
INE	eCPPT v2 (Certified Professional Penetration Tester)
CISCO	CCNP (Certified Network Security Practitioner)
CISCO	CCNP (Cisco Certified Network Professional)
HUAWEI	HCNA (Huawei Certified Network Associate)
ISC2	CCSP (Certified Cloud Security Professional)
HTB	ZEPHYR (Hack The Box – Pro Labs)
HTB	DANTE (Hack The Box – Pro Labs)
HTB	RASTALABS (Hack The Box – Pro Labs)
HTB	CYBERNETICS (Hack The Box – Pro Labs

Artificial Intelligence
Advanced Wireless Hacking
Core Web Design & Development
Windows & Linux Based Operating Systems

SCRIPTING LANGUAGES

PYTHON
POWERSHELL
JAVASCRIPT
BASH
BATCH
PHP

HANDS ON NETWORK & SECURITY TOOLS

NESSUS PROFESSIONAL
OPEN VAS
NETSPARKER
WIRESHARK
BURPSUITE PROFESSIONAL
COBALTSTRIKE
EMPIRE
BYOD (BUILD YOUR OWN BOTNET)
PINGCASTLE
MOBSF
GHIDRA
GDB
NEXPOSE
ACUNETIX
NIKTO
TCPDUMP
METASPLOIT FRAMEWORK
SLIVER
MYTHIC
BLOODHOUND
IDA PRO
DEX2JAR
FRIDA
VARIOUS OTHER OPEN-SOURCE TOOLS

PROFESSIONAL EXPERIENCE

SKILL.PK, Pakistan
Application & Infrastructure Security Expert (2021 – Present)

HORIZON TECH, Pakistan
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, 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 Defence, Pakistan

Penetration Tester & Red Team Operator (2021 – 2023)

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

HackerOne, BUGCROWD, INTEGRITY

Bug Bounty Hunter (2013 – 2020)

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

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 basic 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.

Programming

- Python Essentials, have knowledge and skills in intermediate aspects of python programming, including modules, packages, exceptions, file processing, as well as general coding techniques and object-oriented programming (oop)

Personal Skills

- Communication
  - Presentation Skills
  - Active Listening
  - Good at Public Speaking
  - Teamwork

- Analytical Skills
  - Have the ability to analyze complex systems and identify vulnerabilities

- Research Skills
  - The ability to search for, locate, extract, organize, evaluate, and use or present information that is relevant to a particular topic.

- Problem Solving
  - Know how to define a problem; determine the cause of the problem; identify, prioritize, and select alternatives for a solution; and implement a solution. Attention to detail

- Continuous Learning
- Attention to detail
- Persistence

Languages

- English: Fluent
- Urdu: Native

LINKS

LinkedIn: Daud Khan | LinkedIn
HackerOne: Daud Khan | Profile | HackerOne
Hack-The-Box: Hack The Box :: User Profile
Try-Hack-Me: TryHackMe | HardCore