Umar Mushtaq

Penetration Tester / Red Teamer

Email: rockstar.khan2@gmail.com
Whatsapp: +971 55 7221997
Website: https://zettabyte.com.pk
Linkedin: https://www.linkedin.com/in/daudkhan007/
Nationality: Pakistani

Summary

Professional Pentester having 5+ years of hands on experience in Web Applications, Network & Infrastructure Penetration testing. Bugbounty hunter found log4j vulnerability in github and linkdin. Also have pentest 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 pentest 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 it's system internals.

Core Skills

- Pentesting Skills
  - Pentest desktop, mobile, web app & servers
  - Pentest cloud systems
  - Vulnerability assessment network and infrastructure
  - Redteaming network, systems and web apps
  - Pentest embedded systems including PLC and SCADA networks
  - Frequency & wireless
  - Linux & windows troubleshooting (basic + advance)
  - Linux & windows server management
  - cyber awareness & teaching
  - reverse engineering
  - malware analysis

- CTFs
  - Hack The box
  - try hack me
  - echo ctf
  - ctf.live
  - vulnhub
  - pentester lab

- Scripting Languages

- Python
- PHP
- JS
- Bash
- powershell
- Batch

- **Hands On Network, Security Tools & C2**
  - Nessus Professional
  - wireshark
  - tcpdump
  - BurpSuite Professional
  - Metasploit Framework
  - CobaltStrike
  - sliver
  - empire
  - mythic
  - byod (build your own botnet)
  - Bloodhound
  - pingcastle
  - Nexpose
  - Open VAS
  - Acunetix
  - netsparker
  - nikto
  - IDA pro
  - Various Open Source Tools
  - MOBSF, Dex2JAR, GHIDRA, FRIDA, GDB

- **Management Skills**
  - Problem solving and decision-making
  - Communication and motivation

Professional Experience

- Job Title: Application & Infrastructure Security Expert (2021 – Current)
- Software House: Penetration Tester (skill.pk)
- Company: horizon tech pakistan (Horizon Tech Services – Your Information Security Partner)
  - Manging special pentest projects
  - Team Lead Redteaming Operations
  - Managing Internal VAPT Program

- Job Title: Freelance PentesTer (2014 – 2021)
  Red-teaming

- Projects:
  - Manging special pentest projects
  - Team Lead Redteaming Operations

- Job Title: **Bug Bounty Hunter** (2013 – 2020)
- Bugcrowd, HackerOne, Intigrity

Achivements

- Bugs Found: Information disclosure (rozee.pk)
- Bugs Found: Critical vulnerabilities (netsoltech.com) & much more

CCNA

- 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.

- End Point 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

- Learned 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.

- 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)

Penetration Tester - Self Employed

June 2019 - Present

- Conducted automated and manual penetration testing to identify vulnerabilities and potential threats in web and mobile applications.

- Utilized tools such as Nikto, W3AF, Nessus, and Nuclei to conduct

comprehensive scans and identify common vulnerabilities, misconfigurations, and other potential security issues.

- 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.
- Stayed up-to-date with the latest trends and best practices in penetration testing, security testing, and vulnerability management to ensure the highest level of security for the organization.
- Conducted security assessments and audits to evaluate the effectiveness of existing security controls and identify potential areas of improvement.

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.
- Raised awareness of cybersecurity risks and best practices through training, presentations, and outreach efforts, educating individuals and organizations on how to protect themselves from cyber threats.
- Built strong relationships with clients, serving as a trusted advisor and resource for cybersecurity-related issues and concerns.
- 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.

- Delivered presentations and talks on cybersecurity to a variety of audiences, including individuals, organizations, and industry groups.

- 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.

- Collaborated with event organizers and hosts to ensure seamless and successful delivery of cybersecurity presentations and talks.

- Stayed up-to-date with the latest trends and developments in cybersecurity, continually expanding knowledge and skills to deliver the most relevant and impactful presentations and talks.

CERTIFICATIONS & TRAININGS

- OSCP (OFFENSIVE SECURITY CERTIFIED) – IN PROGRESS
- CEH V11 (CERTIFIED ETHICAL HACKING)
- CCNP (CISCO CERTIFIED NETWORK PROFESSIONAL)
- HCNA
- AI – ARTIFICIAL INTELLIGENCE
- CCSP
- ADVANCE WIRELESS HACKING
- CORE WEB DESIGNING & DEVELOPMENT
- WINDOWS & LINUX OPERATION SYSTEMS

PERSONAL SKILLS

- **Communication**

  - Presentation skills
  - Active listening
  - Good at Public speaking
  - Teamwork

- **Analytical skills**

  - Have the ability to analyze complex systems and identify vulnerabilities
    Continuous learning

- **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**

EDUCATION

- BEACONHOUSE SCHOOL SYSTEM MULTAN O-LEVELS (2013-2015)
- BEACONHOUSE SCHOOL SYSTEM MULTAN A-LEVELS (2015-2017)
- BAHAUDIN ZAKARIYA UNIVERSITY MULTAN BSCS (2017-2020)

LANGUAGE SKILLS

- ENGLISH: FLUENT
- URDU: NATIVE

LINKS:

LINKEDIN: (25) Daud Khan | LinkedIn
HACKERONE: Daud Khan | Profile | HackerOne
HACK-THE-BOX: Hack The Box :: User Profile
TRY-HACK-ME: TryHackMe | HardCore