Muhammad Masab Bin Zahid

+923328913727 masadpd99@gmail.com Rawalpindi, Pakistan

Career Skills

- Vulnerability Assessment and Penetration Testing (Infrastructure, Active Directory, Web/Mobile Application, API, Network).
- Bug Bounty Hunting and CTF's.
- Proficient in Linux and Windows operating systems as well as scripting languages.
- Highly motivated to be Red Teamer/Exploit Developer.
- Familiarity with Reverse Engineering.
- Solid understanding of networking concepts, devices, and configuration.
- Virtualization & Containers.
- System Administration and System Engineer L1 Skills.
- Network Operation Center L1 Skills.
- Automation skills.
- Programming concepts.
- SDLC concepts.

Academic certifications

Practical Ethical Hacking **(PEH),** Practical Mobile Application, Penetration Testing **(PMAPT)**, Practical Web Security Testing **(PWST)**

Network Security Expert **(NSE-1)**
Network Security Expert **(NSE-2)**

Vulnerability Management Foundation **(VMF)**

API Penetration testing **(APT)**

Ethical Hacking Essentials **(EHE)**

Cisco Certified Network Associate **(CCNA)**

Professional Experience

Junior Penetration Tester **Secisys, Islamabad, Pakistan** **July 2023–Present**

- Performing vulnerability assessments and penetration testing on a variety of targets using Penetration Testing Execution Standard (PTE), including web applications, mobile applications, networks, active directories, infrastructure, servers, firewalls, and more.
- Executing Black Box testing by employing Red Team OSINT tactics and Bug Bounty OSINT strategies.
- Performing White Box penetration testing in accordance with established standards such as The OWASP Web Security Testing Guide (WSTG), and OWASP Mobile Application Security (MASTG).
- Identifying security vulnerabilities in web penetration testing, including issues such as File Upload leading to SSRF/Stored XSS, exploitation of the TURN protocol used by WEBRTC for SSRF and proxy to access internal web applications locally on the server, SSRF, SQL injections, Iframe injections, and more.

- Discovered numerous security issues within APIs, including authentication vulnerabilities, API Broken Function Level (BFLA), Broken Object Level Authorization (BOLA), Local File Inclusion (LFI), and more.
- Identified security issues in mobile applications, including authentication bypass and SSL pinning bypass, among others.
- Uncovered security vulnerabilities within the Active Directory environment, such as LLMNR Poisoning, SMB Relay, IPv6 attacks leading to DNS hijacking to Domain Controller LDAPS Command and Control, Zero logon, lateral movement, and various pivoting techniques.
- Conducting network scanning and obtaining system shells during infrastructure penetration testing through the use of well-known remote code execution (RCE) techniques like msf-17, and employing command and control (C2) tools such as msfconsole.
- Penetrating firewalls and overcoming their security measures, such as those provided by Fortinet, through the exploitation of known vulnerabilities (CVEs).
- Mastery in utilizing tools such as Burp Suite, msfconsole, Nmap, Nessus, and more.
- Employing the STRIDE method for threat modeling.
- Manual report composition for penetration testing.
- Familiarity with Security Frameworks such as GDPR, HIPAA, and PCI DSS.
- Providing clients with consultations on enhancing their security posture and promoting secure coding practices, utilizing OWASP Secure Code guidelines.

NOC/Security Engineer **Host break, Rawalpindi, Punjab** **November 2022–April 2023**

- Optimized firewall settings to reduce cyber-attack risks on servers/websites.
- Employed Modsecurity, pre-configured rules, and custom SecRule rules to enhance protection.
- Implemented IBM QRADAR CE for cloud network security monitoring and threat detection.
- Detected malicious activities via log analysis, IP tracing, and code analysis. Developed SOPs and documentation for future incident response.
- Successfully deployed new servers, performed VM backups, and implemented security and optimization configurations.
- Conducted disaster recovery scenarios to determine the optimal approach for maintaining uninterrupted services during disasters.
- Automated repetitive tasks via Bash/Python and PowerShell/Batch.
- Provided technical support to customers 24/7 using WHMCS/Call/Email for website, DNS, and hosting issues. Expertise in DNS Zone settings (A Records, MX, CNAME).

IT Support Engineer **United Bank Limited (UBL)** **March 2022–November 2022**

- Troubleshoot complex hardware and software issues while providing service to UBL staff.
- Managed remote branches across Pakistan, by coordinating with various departments, integrating new software and hardware, conducting research and testing for solutions, maintaining staff satisfaction, and ensuring smooth system operation through effective communication and problem-solving skills.
- Managed IT support for end-users in the UBL Call Center, ensuring uninterrupted services, troubleshooting technical issues, overseeing software/hardware upgrades, and delivering support.

Penetration Tester Internee **SecTechs, Lahore, Punjab** **December 2021–January 2022**

- Performed web app penetration testing on PHP and ASP.net-based applications utilizing tools like Burpsuite, OWASP ZAP, and Metasploit, following a methodology to identify vulnerabilities.
- Performed penetration testing on virtual machines utilizing Nmap, Metasploit, Burpsuite and publicly accessible exploits.

Cyber Security of Instrumentation and Control System	**Pakistan Institute of Engineering and Applied Sciences (PIEAS)**	**November 2021–January 2022**

- Provided SCADA security training to employees of multiple government organizations, covering detection and mitigation of critical vulnerabilities like Man-in-the-Middle attacks, network vulnerabilities, and vulnerable software, aiming to enhance their SCADA system knowledge and equip them with skills to cybersecurity defenses and improve overall security posture.
- Conducted training in a virtualized environment for safe scenario replication, security testing, and efficient task completion without impacting production systems.

Instrumentation and Control System Security Internee	**National Development Complex (NDC)**	**September 2021–November 2021**

- Conducted penetration testing on a virtualized SCADA system, identified vulnerabilities, and implemented security measures including firewall configuration, access controls, and software updates.
- Documented risks of man-in-the-middle attacks, vulnerable software, and publicly available exploits.

Web Development Internee	**Eziline Software House, Rawalpindi, Punjab**	**September 2020–December 2020**

- The venue booking system had features such as location-based booking, seating capacity viewing, menu browsing, customer feedback submission, owner communication, and filtered search options based on location, feedback, star ratings, and capacity.
- Water Management and Service Provider Online System, featuring ordering water bottles with home delivery, real-time notifications for riders, water subscription packages, and a return policy.
- Student login and submission of attendance are features of the student attendance system. The teacher will have a list of every student's attendance according to their subject enrollments.

EDUCATION

Barani Institute of Management and Sciences	**Bachelors in Information Technology**	**October 2018 – July 2022**

Final Year Project:

- Developing a Learning Management System (LMS) that caters to the requirements of facilitating interactions between students and teachers. This LMS will enable the creation of quizzes, tasks, and assignments, which can be easily assigned to relevant groups or classes. Additionally, the system will feature a chat support system that fosters communication and collaboration among group members, classes, and teachers.
- Leveraging the MVC framework Laravel for the backend, and employing Bootstrap along with customized HTML and CSS for the frontend. To ensure real-time feed updates, we've implemented AJAX. For streamlined version control and collaborative supervision, we have integrated GitHub into our development process.

Punjab Group of college	**F.Sc (Pre-Engineering)**	**September 2016 – August 2018**
Kay Zed High School	**SSC (Science: Biology)**	**March 2003 – April 2016**