NAFIS MOHAMMED NIZAR

PENETRATION TESTER & SECURITY ANALYST

📍 Dubai,UAE | +971-552475659 | nafismohammednizar@gmail.com

🌐 linkedin.com/in/nafismohammednizar | TryHackMe

PROFESSIONAL SUMMARY

Penetration Tester & Security Analyst with hands-on experience in VAPT, Web & Network Security, and Threat Analysis. Proficient in tools like Metasploit, Burp Suite, Nmap, and Wireshark, with scripting skills in Python and Bash. Completed CEH training and preparing for certification. Practical exposure through labs, internships, and projects, including an AES-based Image Encryption Tool and assessments targeting OWASP Top 10, AD, and OS-level exploits. Skilled in reporting and committed to advancing offensive and defensive security skills.

WORK EXPERIENCE

Penetration Testing Intern - Corizo **Apr 2024 - May 2024**

Bengaluru, Karnataka, India

- Conducted penetration testing on networks, systems, and web apps using Metasploit, Nmap, Nessus, and Burp Suite.
- Identified XSS, SQLi, file upload, access control, and other common vulnerabilities and documented findings in reports.
- Proposed remediation plans to improve the overall security posture.

PROJECTS

Developed an AES-based Image Encryption and Decryption Tool using Python – GitHub

- Built a Python application using AES-256 encryption and a Tkinter GUI to securely encrypt/decrypt .jpg and .png files.
- Implemented PyCryptodome for cryptographic operations with key management and secure padding techniques.
- Followed secure coding practices to protect against cryptographic attacks.

JPMorgan & Mastercard Cybersecurity Virtual Labs (Forage)

- Simulated real-world cybersecurity scenarios, including phishing threat detection and internal security awareness campaigns.
- Built spam classifiers using NLP and scikit-learn; analyzed payment fraud patterns using Python and Pandas.
- Applied secure coding, hardened web apps with security headers, input validation, and access controls.

Hands-on Penetration Testing Lab (HackTheBox, TryHackMe, PortSwigger, VulHub)

- Simulated real-world attacks across web, network, and system layers in a controlled lab.
- Web Pentesting: Identified SQLi, XSS, and RCE using Burp Suite and Sqlmap. Manually exploited session management flaws.
- Active Directory: Performed Kerberoasting, Pass-the-Hash, and lateral movement using BloodHound, Mimikatz, and PowerView.
- System Exploitation: Gained root/system access on misconfigured Linux/Windows hosts using Metasploit and manual privilege escalation.

CERTIFICATIONS

- Certified Ethical Hacker (CEH) – Training Completed, Exam Pending – EC-Council
- Advanced Penetration Tester (APT) – RedTeam Hacker Academy
- Introduction to Cyber Security – TryHackMe
- Metasploit Essentials and Penetration Testing – LinkedIn
- Computer Forensics Best Practices – EC-Council

SKILLS

- **Offensive Security:** VAPT (Web, System, Network, Cloud)
- **Scripting & Languages:** Python, Bash, PowerShell (basic), SQL for automation and security tooling.
- **Tools & Technologies:** Nmap, Burp Suite, Sqlmap, Metasploit, Nessus, Wireshark, Hydra,CrackMapExec, Mimikatz, PowerView, BloodHound, OpenVAS, John the Ripper, Dirb, Kali Linux.
- **Security Frameworks & Standards:** Familiar with NIST CSF, NIST SP 800-30, ISO/IEC 27001
- **Soft Skills:** Analytical Thinking, Problem-Solving, Attention to Detail, Communication , Team Collaboration, Adaptability.
- **Defensive Skills:** SIEM (QRadar, Splunk), Log Analysis, Secure Configuration, Hardening

EDUCATION

Bachelor of Computer Science Engineering **Dec 2020 - May 2024**

Yenepoya Institute of Technology, India

- GPA: 7.5/10
- Relevant Coursework: Networking, Cryptography, Secure Coding Practices
- Programming Languages: Python, C++, Java, SQL, HTML, CSS
- Academic Projects: Sign language detection using ML, Online book store, Petrolpumb managment using Streamlit.

ADDITIONAL INFORMATION

- **Languages:** English, Malayalam, Hindi.
- **Licenses:** LMV Driving License