Choppa Penchala Praveen

Bengaluru , Karnataka· 8688598476 · penchalapraveen221@gmail.com

Profile Summary

Certified Ethical Hacker (CEH) fresher with foundational knowledge in penetration testing, vulnerability assessment, and network security. Skilled in using tools like Metasploit, Nmap, and Burp Suite to identify and address security vulnerabilities. With a background in Computer Science and Engineering specializing in Artificial Intelligence and Machine Learning, I bring strong analytical and problem-solving abilities to enhance cybersecurity measures. Seeking an entry-level opportunity to apply and grow my skills in protecting digital assets.

Key Responsibilities & Achievements

Penetration Testing & Vulnerability Assessments

- Conducted penetration tests on networks, web applications, and IT infrastructure, uncovering critical vulnerabilities.
- Utilized Metasploit, Burp Suite, and Nmap to identify and exploit system weaknesses ethically.

Incident Response & Digital Forensics

- Investigated and resolved security incidents, identifying root causes and mitigating future risks.
- Collected and analyzed digital evidence for forensic investigations, strengthening incident response protocols.

Security Audits & Compliance

- Performed security audits aligned with ISO 27001, NIST, and industry standards.
- Ensured compliance with HIPAA and PCI-DSS regulations through thorough assessments and recommendations.

Risk Management & Threat Mitigation

- Conducted risk assessments to identify threats and prioritize mitigation strategies.
- Collaborated with IT teams to implement layered security measures, reducing the attack surface.

Security Tools & Vulnerability Scanning

- Proficient with tools such as Nessus, Wireshark, and custom scripts for vulnerability management.
- Automated scanning processes to streamline security evaluations and reporting.

Network & Application Security

- Hardened network infrastructure, including firewalls, VPNs, and IDS/IPS, to prevent unauthorized access.
- Implemented secure coding practices to mitigate OWASP Top 10 vulnerabilities like SQL Injection and XSS.

Training & Awareness

- Conducted employee training on cybersecurity best practices, focusing on phishing and social engineering threats.
- Led workshops to enhance security awareness across the organization.

Continuous Improvement & Research

- Actively engaged in cybersecurity forums and conferences to stay updated on emerging threats and technologies.
- Conducted research to enhance penetration testing methodologies and incident response strategies.

Projects

HSBox1 – Web Application Exploitation

- **Objective:** Conducted penetration testing on a vulnerable web application running on HSBox1, focusing on exploiting common web application vulnerabilities.
- **Actions Taken:**
  - Performed reconnaissance using Nmap to identify open ports and services.
  - Discovered and exploited a SQL Injection vulnerability in the login form using sqlmap, gaining unauthorized access to the application.
  - Bypassed authentication and escalated privileges by exploiting weak file upload functionality.
  - Obtained sensitive data (flag) from the web server by traversing hidden directories.
- **Outcome:** Successfully captured the flag and documented remediation strategies for securing web applications against common attack vectors.

HSBox2 – Privilege Escalation & Exploitation

- **Objective:** Focused on local privilege escalation and exploiting misconfigurations within a Linux-based system on HSBox2.
- **Actions Taken:**
  - Identified misconfigured SUID binaries and exploited them to escalate privileges from a regular user to root access.
  - Used LinPEAS to discover system vulnerabilities and escalate privileges on the compromised system.
  - Set up a reverse shell for post-exploitation access and analyzed logs for further attack vectors.
  - Extracted flags from protected directories by exploiting system weaknesses and gained full administrative control over the machine.
- **Outcome:** Achieved full system compromise and captured multiple flags, demonstrating effective use of privilege escalation techniques.

Technical Skills

- Vulnerability Scanning & Risk Assessment
- Incident Response & Forensics
- Network Security (Firewalls, VPNs, IDS/IPS)
- Security Audits & Compliance (ISO, NIST)
- Threat & Vulnerability Management
- Security Tool Proficiency (Metasploit, Burp Suite, Nmap, Nessus, Wireshark)
- Secure Coding Practices & Web Application Security
- Cybersecurity Training & Awareness Programs

Certification

- Certification of Certified ethical hacker V13 course completion (EC-Council)
- Practical Ethical Hacker - (TCM Security)
- Certified Lead Auditor (ISo/IEC 22001)

Education

SRI VENKATESHWARA COLLEGE OF ENGINEERING JUNE 2021 – JULY 2025
COMPUTER SCIENCE and ENGINEERING (AI and ML)