RISHI RAJ SACHAN

+91 9826869761 · rishirajsachan2001@hotmail.com · Linkedin:rishi-raj-sachan-896422201

SUMMARY

A dedicated cybersecurity enthusiast with a keen interest in protecting data and countering cyber threats. Skilled in networking basics, vulnerability assessment, and ethical hacking. Experienced in performing thorough penetration tests, vulnerability assessments, and participating in advanced networking initiatives. Proficient at recognizing and resolving critical security weaknesses, producing detailed reports, and suggesting efficient remediation plans. Excited to apply my expertise to improve organizational security and reliability.

SKILLS AND EXPERTISE

Penetration Testing	Risk Assessment	Team Leadership
Networking Concepts	VAPT	Communication
Python, Bash, C/C++	Cybersecurity Concepts	Nmap, Wireshark, Metasploit

PROFESSIONAL EXPERIENCE

Albus Security **January 2024 - Present**

Cyber Security Intern

I played a role in improving and advancing Netprobe, an innovative networking lab platform. My responsibilities included creating and executing intricate lab scenarios in the Netprobe system, with a focus on real-world network setups and security issues.

Accomplishments:

- Configuring OSPF in the Central Network, addressing DNS misconfigurations and configuring IP phones to enhance network security.
- Implementing IPv6 Addressing with Minor Misconfigurations, deploying AAA across primary network devices and setting up network sniffers for monitoring purposes.
- Collaborated closely with senior developers and project managers to ensure the successful implementation and testing of Netprobe features.
- Provided valuable insights and recommendations for improvement based on the analysis of lab scenarios and platform functionalities.

HackersForYou **February 2024 - May 2024**

Pentesting Intern

During my internship at HackersForYou, I conducted external penetration tests following industry-standard methodologies such as NIST SP 800-115 and OWASP Testing Guide (v4.2).

Accomplishments:

- Utilized a wide range of penetration testing tools and techniques to identify vulnerabilities in client systems, such as server configuration information disclosure, blind SQL injection vulnerabilities, disclosure of user and order details, insecure direct object references (IDOR), and URL parameter pollution vulnerabilities.
- Generated detailed vulnerability reports outlining findings, exploitation techniques used, and recommended remediation strategies to enhance client security posture.
- Collaborated with team members to prioritize and address identified vulnerabilities, ensuring effective risk mitigation and security improvement.

Skill Vertex **August 2022 - October 2022**
Cyber Security Intern

- Conducted in-depth Vulnerability Assessment and Penetration Testing (VAPT) on the Metasploitable2 virtual machine, identifying and exploiting security weaknesses and potential vulnerabilities.

Accomplishments:

- Utilized a comprehensive suite of tools including Nmap, Nessus, Metasploit Framework, Burp Suite, Nikto, Wireshark, Hydra, John The Ripper, Dirb, and Enum4linux for thorough scanning and analysis of target systems.
- Generated detailed reports documenting vulnerabilities discovered, exploitation techniques used, and provided recommendations for remediation to enhance overall security posture.
- Collaborated with team members to analyze and interpret findings, prioritize remediation efforts, and implement security best practices..

PROJECTS

- **KeyLogger**: A Python-based program that records all keystrokes on a target machine and reports them to a remote listener via email.
- **Socket-Listener**: A network utility tool for reading from and writing to a network using a TCP connection on the target machine from a remote machine.
- **MITM (Man In The Middle)**: A tool for ARP poisoning and monitoring packets transmitted to and from the target machine.
- **Google Dorking** *(Ongoing)*: A Python tool that performs Google dorking on a list of domains, sending requests to scrape content and check for specific results. It includes threading for parallel processing and proxy rotation to handle 429 "too many requests" status codes.

EDUCATION & CERTIFICATION

Indian Institue of Information Technology Vadodara
Bachelor of Technology Computer Science And Engineering
EC-Council
Certified Ethical Hacker *(CEH)*
