BHARATH KUMAR

Bangalore • 7975216601 • LinkedIn • bharathreddy1405@gmail.com

OBJECTIVE

Cybersecurity professional with a strong interest in ethical hacking, penetration testing, vulnerability analysis, and network security. Hard-working, energetic, personable, and technical-minded individual. Possess exceptional customer service and communication skills with the strong ability to multitask and resolve issues quickly. Currently in a cybersecurity role where I continue to develop and learn new abilities while contributing to the overall success of the organization. I also possess:

- Experience in scripting languages including Python and Bash.
- Excellent task management. Ability to handle multiple projects simultaneously.
- Experience with security toolkits such as Nessus, Metasploit, Wireshark and Burp Suite.
- Proficient in translating information from technical to executive/management terminology.

EDUCATION

Dayananda Sagar University – B.Sc. Biotechnology.

- GPA: 6.8/10.0

Spoorthy Global School (ICSE) – Computer Science.

- CGPA: 6.7/10.0

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP. ongoing).
- Google Cybersecurity Professional Certificate.
- ISC2 Certified in Cybersecurity (CC).
- Infosys Ethical Hacking Certificate.

SKILLS

- Network Security • Threat Intelligence • Vulnerability Assessment. • Reporting & Debriefing • Social Engineering • Evasion & Exploitation Techniques • Communication Skills.

Experience

Read Team Intern, [DeepDefend]
[Remote], [Apr,2024] - Present

- Developed custom Windows-based malware to simulate real-world cyber threats.
- Executed comprehensive red team exercises, including social engineering and penetration tests, to identify vulnerabilities.
- Stayed abreast of cybersecurity trends to enhance offensive capabilities.
- Documented findings and presented reports to stakeholders, driving informed decision making.
- Contributed to the development of internal tools and frameworks for red team operations.

Cybersecurity Intern, **[NullClass]**
[Remote], [Dec,2023] - [Mar,2024]

- Assisted senior cybersecurity analysts in conducting penetration tests and vulnerability assessments of client systems.
- Contributed to red team exercises and threat intelligence reports.
- Collaborated on the preparation of threat intelligence reports, providing insights into emerging cyber threats and vulnerabilities
- Presented findings and recommendations to management in formal reports and presentations.

PROJECT

AD Penetration Testing: Web Exploits, Privilege Escalation and Lateral Movement [LINK]

- Conducted an Active Directory penetration testing project in a home lab, configuring deliberate vulnerabilities, including a compromised website. Executed multi-stage attacks using privilege escalation exploits and Mimikatz for lateral movement. Successfully accessed critical system hives and extracted admin hashes. Thoroughly documented findings, delivering actionable remediation suggestions.

Penetration Testing Project on DVWA [LINK]

- Conducted security assessment on DVWA, focusing on vulnerabilities like SQL injection and XSS.
- Utilized PTES methodology and tools like Nmap, Burp Suite, and Metasploit.
- Provided detailed report with exploits and recommendations for remediation.
- Emphasized the importance of continuous security testing for web applications.

SMB Share Scanner Tool (Python) [LINK]

- Developed a Python tool to scan network for SMB shares, attempting login with default guest password.
- Lists files and folders in each share, navigates into subfolders, retrieves all files.
- Provides seamless file downloading capability from discovered SMB shares.

Cybersecurity Blogger & Red Team Specialist [LINK]

- Write comprehensive write-ups for various Capture the Flag (CTF) machines and tournaments, detailing the methodologies, tools, and techniques used to solve challenges.
- Cover topics related to red teaming, including Active Directory (AD) hacking, privilege escalation, lateral movement, and persistence techniques.
- Continuously research and experiment with new tools and methodologies to stay abreast of emerging threats and defensive strategies.