SONDIP ROY

Address: Harirampur, Manikganj
Phone: +8801616014176
Email: sondiproy4321@gmail.com
Linkedin: sondiproy0

OBJECTIVES

Highly motivated and result-oriented IT enthusiast with a strong networking, and cyber security foundation. Seeking an opportunity to leverage my technical skills and contribute to innovative projects within a dynamic IT environment. Eager to apply my academic knowledge and practical experience to drive organizational success.

TECHNICAL SKILLS

- **Reconnaissance:** Nmap, Masscan, theHarvester, Amass
- **Protocol Exploitation:** SMB (EternalBlue, SMBMap, CrackMapExec), FTP (Anonymous auth, vsftpd backdoor), SSH (Hydra), RDP (BlueKeep: CVE-2019-0708), HTTP/S: Shellshock
- **Vulnerability Scanning:** Nessus, Nikto, Nuclei, WPScan, Droopescan
- **Directory Brute Forcing:** Gobuster, FFuf, Dirbuster, Dirsearch
- **Security Tools:** Exploitation (Metasploit, SQLmap), Post-Exploitation (Mimikatz), Password Attacks (Hashcat, John the Ripper, SecLists)**,** Analysis (Wireshark, Burp Suite)

CERTIFICATIONS AND TRAINING

- **eJPT** (eLearnSecurity Junior Penetration Tester) - Certificate Credentials
- Cisco Certified Network Associate (**CCNA**) Training - PeopleNTech Ltd
- **Server Administration Including Windows Server** Training - Basis SEIP

HANDS ON EXPERIENCE & PROJECTS

- Complete hands-on labs focused on exploring **privilege escalation**, **network exploitation**, and enumerating network protocols.
- Competed in 4-5 CTF competitions, solving network, OSINT, and Digital Forensic problems.
- Hands-on practice on various CMS exploitation like WordPress, Drupal, Fuel CMS, Navigator CMS, Bolt CMS.
- Setting up a home lab and using vulnerable machines like Kioptrix, DC:1, and ICA:1, researched security flaws and exploits.
- Practice post-exploitation and privilege escalation using **Metasploitable.**
- Configure Windows Server 2016 (Active Directory, file sharing, DNS)

PROFESSIONAL EXPERIENCE

AIG Shields Up: Cybersecurity virtual experience program on Forage - April 2025

- Completed a cybersecurity threat analysis simulation for the Cyber Defense Unit, staying updated on CISA publications.
- Researched and understood reported vulnerabilities, showcasing analytical skills in cybersecurity.
- Drafted a clear and concise email to guide teams on vulnerability remediation.
- Utilized Python skills to write a script for ethical hacking, avoiding ransom payments by bruteforcing decryption keys.

Mastercard Cybersecurity virtual experience program on Forge - April 2025

- Completed a job simulation where I served as an analyst on Mastercard’s Security Awareness Team
- Helped identify and report security threats such as phishing
- Analyzed and identified which areas of the business needed more robust security training and implemented training courses and procedures for those teams

Cyber Security Analyst Intern - Arena Web Security **Oct 2024 - Oct 2024**

- Assisted in conducting vulnerability assessments and penetration testing on web applications
- Gained Hands-on experience with tools such as Burp Suite, Nmap, and Metasploit.
- Assisted in private investigations for clients.
- Practice common vulnerabilities.
- Documented security findings in detailed reports and presented them to the supervisor for review.

Network Support Engineer - RBA Online **Feb 2023 - June 2023**

- Assisted in network troubleshooting and resolving technical issues for end-users.
- Participated in network equipment maintenance and upgrades.
- Deployed full computer labs of various sizes, ranging from 20 to 35 machines each.
- Performed hardware upgrades to machines.
- Document all the processes and findings during the work period.

EDUCATION

Bachelor of Science in Computer Science and Engineering **Aug 2018 - Dec 2022**

Daffodil International University

- Data Structures and Algorithms, Computer Architecture, Operating Systems, Database Management Systems (SQL), Computer Networks, Artificial Intelligence, Programming Languages (C, Python).

ADDITIONAL

- Published 7-10 technical writeups: Detailed walkthroughs of CTF solutions and vulnerability analyses.
- Active on **TryHackMe:** Consistently complete new rooms/challenges to stay current with attack techniques. **TryHackMe** top 5% (70+ labs completed, 25+ privilege escalation scenarios)
- Mentored 5 peers through beginner CTFs.