Avnish Singh

9045158040 • avnishsingh.tech@gmail.com • linkedin.com/in/cybravnish

I'm into Cybersecurity because I enjoy solving problems and figuring things out. Curious about how things work—and how to break them safely. Exploring Cybersecurity through hands-on work and always looking to learn more.

EDUCATION

DR. BHIMRAO AMBEDKAR UNIVERSITY   MAY 2022 – JUNE 2025
Bachelor of Science in Computer Science
J.S. College of Education, Vijay Nagar, Kusmara, Mainpuri
CGPA: 8.76/10.0;
Relevant Coursework: Computer Networks, Cybersecurity Fundamentals, Cybersecurity & Cyber Laws, Operating Systems, Linux Administration, Python Programming, Network Security Lab

EXPERIENCE

CYBERSECURITY WITH AI – INTERNSHIP   JUN 2025 - PRESENT
NIIT FOUNDATION IN COLLABORATION WITH CISCO NETWORKING ACADEMY (REMOTE)
- Learning core concepts of network security, threat intelligence, and the application of AI in modern security operations.
- Exploring topics like ethical hacking, risk management, firewalls, and AI-driven anomaly detection.
- Overhauled obsolete legacy source code of two production applications, resulting in increased usability and reduced run time performance by 50%.

CYBERSECURITY INTERN   Mar 2025 – June 2025
Mizu solutions
- Conducted vulnerability assessments and penetration testing on Linux environments.
- Utilized Nmap, Wireshark, and Burp Suite for system analysis.

CYBERSECURITY CTF & PRACTICAL LABS   Nov 2024 - PRESENT
TRYHACKME & OVERTHEWIRE PLATFORMS
- Completed 40+ hands-on labs and CTFs focused on penetration testing, Linux exploitation, and web application security.
- Practiced with industry tools: Nmap, Wireshark, Burp Suite, Metasploit, Hydra, John the Ripper, netcat, and gobuster.

PROJECTS

CYBERSECURITY HOME LAB   SELF-HOSTED | ONGOING
- Built and managed a virtual lab using VirtualBox with Kali Linux, Metasploitable2, and pfSense for hands-on cybersecurity practice.
- Performed network scanning, vulnerability assessment, and exploitation using tools like Nmap, Metasploit, Burp Suite, and Wireshark.

NETWORK MAPPING AND TRAFFIC ANALYSIS USING NMAP AND WIRESHARK
- Utilized Nmap to map network topology, identify devices, open ports, and detect vulnerabilities.
- Analyzed live network traffic with Wireshark to identify anomalies and potential threats.

SKILLS

Security Tools: Nmap, Wireshark, Burp Suite, Metasploit
Scripting, Programming & Version Control: Python, Bash, Git, GitHub
Operating Systems & Virtualization: Linux, Windows, VirtualBox, OS Installation, Dual Boot Setup
Networking & Security: OSI Model, Firewall, Packet Analysis, Vulnerability Scanning, SOC Concepts

CERTIFICATIONS

- GOOGLE CYBERSECURITY PROFESSIONAL CERTIFICATE: COURSERA
- PYTHON FOR CYBERSECURITY: INFOSEC (COURSERA)
- Certified in Cybersecurity (CC): ISC2
- Network Defense Essentials (NDE): EC-Council