Dhruv Dolasiya

✉ dhruvdolasiya047@gmail.com   📞 9925770570   📍 Ahmedabad, Gujarat

in linkedin.com/in/dhruv-dolasiya-09117b2a2   ⭕ https://github.com/Dking9504

🔗 dhruvdolasiya-portfolio.vercel.app

🪪 Profile

- Cyber Security postgraduate with hands-on experience in Vulnerability Assessment and Penetration Testing. Skilled in identifying and analyzing security weaknesses using tools like Burp Suite, Metasploit, Nmap, and Kali Linux. Strong understanding of basic OWASP Top 10 vulnerabilities, web and network security testing, and reporting. Focused on offensive security techniques and delivering clear, actionable remediation recommendations.

💼 Professional Experience

Security Admin Associate L1, *Infotact Solutions*   09/2025 – Present   Remote

- Worked on deploying and configuring **Snort** as a Network Intrusion Detection System (NIDS).
- Created and tested custom Snort rules to detect malicious network activity.
- Analyzed network traffic, alerts, and logs generated by Snort.
- Simulated common attacks (port scans, brute-force attempts, service probes) to validate detection accuracy.
- Documented detections, alert patterns, and improvements for network monitoring

Cyber Security Intern, *SkillCraft Technology*   08/2025 – 08/2025   Remote

- Gained hands-on experience in cybersecurity concepts and practices.
- Assisted in vulnerability assessment and penetration testing tasks.
- Worked with tools and methodologies to analyze threats and enhance security measures.
- Collaborated with the team to document findings and propose security improvements.

Cyber Security Intern, *VAULT-TEC SECURITY*   06/2025 – 07/2025   Remote

- Completed hands-on projects in Python, Linux, and networking fundamentals, and worked on labs using TryHackMe and PicoCTF challenges to understand cybersecurity concepts.
- Conducted bug bounty tasks including live website analysis, vulnerability identification (XSS, SQLi, subdomain takeover), and reported findings with remediation methods in detailed documentation.

🎓 Education

M.SC. IN CYBER SECURITY, *JG UNIVERSITY*   06/2024 – Present   AHMEDABAD

- Pursuing Master's in Cyber Security with a focus on network security, penetration testing, and digital forensics.

Bachelor of Computer Application (BCA), *VIVEKANAND COLLAGE*   2021 – 2024   SURAT

- Completed BCA with strong foundations in programming, networking, and cybersecurity concepts.

🧠 Skills

Penetration Testing & Vulnerability Assessment
- Nmap, Burp Suite, OWASP ZAP, SQLMap, Metasploit, Hydra

Operating Systems & Platforms
- Kali Linux, Windows Server, VirtualBox, VMware

Linux Server (Ubuntu/CentOS)
- Apache/Nginx configuration, user & permission management, SSH hardening, cron jobs, Yum server , FTP server ,Samba Server

Digital Forensics
- FTK Imager, Autopsy, Wireshark

Windows Server (2016/2019)
- Active Directory, Group Policy, IIS, File Sharing, FTP, SSH,DHCP

Networking (Basics)
- TCP/IP fundamentals, OSI model, subnetting, VLANs, routing & switching concepts
- Configuration and troubleshooting of network devices and protocols (DHCP, DNS, FTP, SSH)
- Network monitoring, packet analysis (Wireshark), latency assessment, and basic diagnostics

📑 Certificates

Deloitte Australia Cyber Job Simulation on Forage - July 2025
- Completed a job simulation involving reading web activity logs
- Supported a client in a cyber security breach
- Answered questions to identify suspicious user activity

Tata Cybersecurity Security Analyst Job Simulation on Forage - July 2025
- Completed a job simulation involving identity and access management (IAM) for Tata Consultancy Services, collaborating with a Cybersecurity Consulting team.
- Acquired expertise in IAM principles, cybersecurity best practices, and strategic alignment with business objectives.
- Delivered comprehensive documentation and presentations, showcasing the ability to communicate complex technical concepts effectively.

📁 Projects

Network Intrusion Detection System (NIDS) Project, *Infotact Solutions*　　　　09/2025 – Present
- Developed and deployed a Network Intrusion Detection System using Snort for real-time detection of network threats and anomalies.
- Collaborated with Infotact Solutions for custom rule creation, attack simulation, and system optimization in a practical business environment.
- Analyzed alert logs, generated reports, and documented key findings to enhance security monitoring and response efforts.

Internal Pentest Lab, *Jg university*　　　　07/2025 – Present
- Built an internal pentesting lab using **Kali Linux, Windows 10, Windows Server 2016, and Metasploitable2**.
- Performed enumeration, scanning, and exploitation using **Nmap, Enum4linux, Hydra, and Metasploit**.
- Identified weak services, misconfigurations, and outdated software vulnerabilities.
- Executed brute-force attacks, SMB enumeration, and Windows/Linux exploitation scenarios.
- Documented vulnerabilities, exploitation results, and remediation steps.