Divyanshu kumar

✉ divyanshurds.kumar@gmail.com   📞 8448027610   in https://www.linkedin.com/in/divyanshu-kumar-883816206   🔗 Portfolio

🪪 PROFILE

Passionate computer science engineer with a robust academic background and a sincere interest in cybersecurity. Poised to launch a dynamic career as a Cybersecurity Engineer, dedicated to leveraging technical expertise to fortify digital security landscapes for organizations. A nimble learner, committed to staying at the forefront of evolving cybersecurity trends and best practices.

🧠 SKILLS

Operating Systems
Windows, Linux

Networking
TCP/IP, DNS, DHCP, VPN, Firewalls

Security Tools
Wireshark, Metasploit, Nmap, Burp Suite,Google Hacking Database (GHDB),Splunk

Programming Languages
Python, C/C++,Dart

Databases:
SQL, MySQL

Soft Skills
Communication , Teamwork , Problem-Solving , Adaptability/Flexibility , Leadership , Time Management

🖥 PRACTICAL EXPERIENCE

Splunk Training
- Gained experience in log monitoring, creating security dashboards, and incident analysis using Splunk.
- Developed skills in data analysis and search queries to identify security threats.

TryHackMe Practical Rooms
- Completed numerous security challenges, focusing on network security, penetration testing, and incident response.
- Enhanced skills in vulnerability assessments, web exploitation, and forensic analysis.

PortSwigger Web Security Academy
- Completed various labs focused on web application security, learning about vulnerabilities like cross-site scripting (XSS), SQL injection, and authentication flaws.
- Gained hands-on experience in testing and exploiting common web vulnerabilities.

🎓 CERTIFICATES

- CompTIA a+ Cyber (Coursera) 🔗
- Google Cybersecurity 🔗
- Python Essential (cisco) 🔗
- Introduction to cyber security (cisco) 🔗
- Introduction to cyber security tools and cyber attack (coursera) 🔗
- Scientific Computing with Python (Freecodecamp) 🔗
- Ethical Hacking Essentials (EHE) (code red) 🔗
- Network Defense Essentials (NDE) by code red 🔗
- Penetration Testing, Incident Response and Forensics (IBM) 🔗
- Assets, Threats, and Vulnerabilities (Google) 🔗

🎓 EDUCATION

Bachelor of Technology in Computer science - Cyber security
Parul unversity
2020 – 2024 | vadodara, India

💼 PROFESSIONAL EXPERIENCE

Cyber Security Engineer
Internship
12/2023 – 03/2024
Informatica Security Intern at CSCOI:
- Learning security assessments, vulnerability resolution.
- Exploring security policy creation, incident response.
- Gaining experience in log monitoring, project contribution, and training.

Cyber Security Management Virtual Experience Program
Internship 🔗
- Conducted regular security assessments and penetration tests to address risks.
- Monitored network traffic for rapid response to potential threats.

Cyber Security Global Virtual Internship
Internship 🔗
- Conducted security awareness training sessions for employees to promote best practices.
- Assisted in incident response activities and conducted post-incident analysis.

📁 PROJECTS

Security Awareness Training Program:
- Created an interactive security awareness training program covering topics like phishing awareness, password security, and social engineering.
- Educated and empowered students to make informed security decisions

Subfinder
- Python script for subdomain discovery: reads "subdomains.txt," combines with user's domain, attempts HTTP requests, prints to "discovered_subdomains.txt." Ethical use recommended.

Bug bounty
- Actively participated in bug bounty programs, identifying and reporting security vulnerabilities for web applications.
- Utilized tools like Burp Suite and Metasploit to uncover and address potential security risks.

Personal Portfolio:
- Designed and developed a personal portfolio website showcasing technical skills, projects, and achievements.
- Implemented a clean and modern user interface using HTML, CSS, and JavaScript for interactive elements.

ZIP-Cracker
- Python script: Brute-force attack on 'enc.zip' using 'rockyou.txt' for password attempts. Prints password if found. Ethical use advised.

Python Keylogger
- Python keylogger: captures keystrokes, timestamps entries, logs data in "Details.txt," auto-generates filenames, and provides periodic reports. For educational use, follow legal and ethical standards. Customize responsibly.