Dev Kaushik

Cyber Security Engineer

+91 991[0]538888

xen1n@proton[.]me

New Delhi, India

Summary

Passionate about offensive security, specializing in Red Team Operations and Ethical Hacking. Skilled in exploitation, threat emulation, and OPSEC, with a focus on Physical Security techniques like lockpicking and covert entry. Committed to adversarial thinking to outpace threats and fortify defenses.

CERTIFICATES

Certified Ethical Hacker v13 Master | In Progress
EC-Council

Certified Network Defender v2
EC-Council

Google Professional Cyber Security
Google | Coursera

Practical Ethical Hacking
TCM Security

FREELANCE

Online Cybersecurity Trainer | Ongoing

- Delivered live, interactive sessions for students and professionals on topics such as ethical hacking, networking, operating systems, and web application penetration testing.
- Developed detailed course material and resources, tailored to current cybersecurity threats and evolving technologies.
- Provided live lectures for Networking and Operating System, Hands-on Labs for Web pentesting
- Guided students through ethical hacking techniques, vulnerability assessments, penetration testing, and incident response strategies.
- Mentored over 200+ students, achieving a 90% positive feedback rate based on post-session surveys.

RESPONSIBILITIES

Core Team Member | The Hacker's Meetup Delhi
2024 - Present

- Actively contribute to organizing and hosting monthly meetups focused on cybersecurity trends, tools, and techniques.
- Collaborate with a community of professionals, researchers, and enthusiasts to facilitate knowledge sharing and hands-on activities.
- Help plan workshops, webinars, and talks around ethical hacking, penetration testing, and red teaming.

Core Team Member | OWASP Noida
2024 - Present

- Contribute to the planning and execution of OWASP-related events, including security workshops and awareness campaigns.
- Lead discussions on web application security, vulnerability management, and secure coding practices.
- Engage in community outreach to raise awareness of OWASP initiatives and help individuals adopt security best practices.

PROFESSIONAL EXPERIENCE

New Delhi Television Ltd. | 2024 (6 Months)
Security Engineer Intern

- Supported the setup and optimization of **Palo Alto NGFW**, configuring advanced features like URL Filtering, Intrusion Prevention System, and security policy cleanup to maintain a robust security posture.
- Utilized **CrowdStrike Falcon XDR** to monitor endpoint activity, analyze alerts, and respond to potential security incidents, reducing false positives by 25%.
- Investigated suspicious activity, triaged incidents based on severity, and escalated issues to senior engineers, helping mitigate high-priority threats.
- Participate in **threat hunting** activities to identify potential indicators of compromise contributing to a 15% increase in early detection of potential threats.
- Help draft security policies, procedures and **Incident Response playbooks.**
- Work closely with senior security engineers to learn and implement security best practices.

Website Sketchers | 2023 (6 Months)
Full Stack Asset Management Project

- Developed a full stack web application for asset management, allowing users to create, read, update, and delete (**CRUD**) asset entries.
- Implemented a **RESTful API** using Node.js and Express for seamless user interaction.
- Utilized **MySQL** as the database to store, retrieve, and manage asset information, ensuring optimized queries and data integrity.
- Implemented a clean and modular code structure following MVC architecture for better scalability and maintainability.
- Used **Git** for version control and collaboration on **GitHub**, ensuring smooth code management and team collaboration.

PROJECTS

1. Active Directory Attack Simulation

Objective: Simulated attacks on a virtual Active Directory (AD) environment to identify vulnerabilities and misconfigurations.

- Built a full-scale AD lab including a domain controller, users, and GPOs.
- Conducted reconnaissance and enumeration using BloodHound, PowerView, and SharpHound.
- Performed attacks like Kerberoasting, AS-REP Roasting, and DCSync, leveraging tools like Impacket, Mimikatz, and CME (CrackMapExec).
- Gained persistence via Golden/Silver Ticket attacks and exploited delegation misconfigurations.
- Documented findings with detailed attack paths, mitigation strategies, and remediation steps.

2. Command and Control (C2) Server Development

Objective: Built and managed a secure Command & Control (C2) server to simulate advanced threat actor behavior.

- Configured C2 frameworks Ninja for remote endpoint management.
- Implemented payload obfuscation techniques using Veil, Obfuscation tools, and custom scripts to bypass security measures.
- Tested lateral movement, privilege escalation, and data exfiltration while maintaining operational security.
- Developed encrypted communication channels to ensure secure interactions between endpoints and servers.

3. Physical Security Penetration Testing

Objective: Assessed the effectiveness of physical security measures in a controlled environment.

- Gained expertise in lockpicking, RFID cloning, and bypassing magnetic stripe access systems.
- Tested physical security devices like locks, RFID badges, and CCTV systems for vulnerabilities.
- Conducted attacks like shoulder surfing, tailgating, and social engineering pretexts to exploit human factors.
- Designed a physical security awareness training module and presented findings with actionable recommendations.

EDUCATION

Bennett University | 2021-2024

Bachelors of Computer Application Cyber Security Hons.

- **CGPA: 7.3**
- Computer forensics, Incident Response, Threat Hunting and Malware Analysis (Sandbox)
- Networking, Python, Unix/Linux & Bash skills, Reverse Engineering, Cryptography
- Web Dev, Cloud, Virtualization, CI/CD, SDLC
- Microprocessors, Assembly Code, Hardware & IOT
- Technical supervisor @ **CSI BU**
- Contributed in building CTF challenges for Hackathons

Global Institute of Cyber Security and Ethical Hacking

Cyber Security Diploma

- Web Penetration Testing, Dynamic App Security Testing, API Security
- Open-source Intelligence using Maltego
- Advanced Red Teaming and Exploitation tools like buffer overflow, registry persistence, etc
- Security evasion using obfuscation and payload modification techniques
- Command & Control server setup, configuration, and remote endpoint management.
- Skilled in Operational Security measures to reduce footprint and traceability during offensive operations.
