Dhruv Ahuja

Contact

Address
München Germany

Phone
+4915510556326

E-mail
dhruvahuja888@gmail.com

Skills

Cybersecurity fundamentals & vulnerability assessment
Networking concepts (TCP/IP, DNS, HTTP, FTP)

Cloud security basics (AWS IAM, least privilege, RBAC, MFA)

Risk analysis, threat modeling (STRIDE), CVSS awareness

Linux & Kali Linux fundamentals

Security tools: Nmap, Burp Suite (basic), SIEM concepts

Scripting & programming: Python, Bash (basic), Java

Experience

2024-06 - 2024-08

Intern

WITZEAL TECHNOLOGIES PRIVATE LIMITED

- Gained hands-on experience in networking concepts and Java programming
- Worked on designing and implementing secure networking protocols.
- Later transitioned to a Cyber Security Analyst role, conducting vulnerability assessments
- Assisted in assessing security policies
- Analyzed and mitigated security risks using various industry-standard tools

Education

2024-05

BTECH: ELECTRONICS AND COMMUNICATION ENGINEERING

Vellore Institute Of Technology - Chennai

- I did some projects during the tenure of my bachelors. In the project titled 'Cross Country Crypto Transactor', my team made a mobile cryptocurrency wallet.
- In 'FTP Anonymous Login Scanner', through the Kali machine I scanned a range of IP addresses to search for FTP servers with anonymous access.
- In 'Malicious Account Detection', using the concept of neural networks, our team used algorithms to detect malicious profiles through various distinct features like profile pictures, username length and follower count.
- In 'Secure Healthcare Data Exchange With Cryptography' I attempted to make cryptographic solutions for securing healthcare data exchange.

2025-12

MSc.: CYBER SECURITY

Hochschule Der Bayrischen Wirtschaft (HDBW)

- Comprehensive postgraduate training in **computer systems security, network security, and cyber risk management**
- Studied **Information Security Management Systems (ISMS)** with focus on **NIS-2 Directive,**

Automation & cloud monitoring concepts

Security documentation & reporting

Microsoft Excel & PowerPoint

Strong analytical, communication, and teamwork skillsTeamwork and collaboration

Fast learner

Quick learner

Computer skills

Adaptability & eagerness to learn

GDPR compliance, and legal aspects of cybersecurity

- Hands-on experience in **system analysis and hardening**, including secure configuration of operating systems and networks
- Applied **cryptography concepts** including encryption algorithms, secure key management, and data protection mechanisms
- Learned **secure application development** and the **Secure Software Development Lifecycle (SSDLC)**, including peer code reviews
- Performed **requirements engineering and threat modelling** using industry methodologies (e.g., STRIDE, CVSS-based risk scoring)
- Covered **incident management and disaster recovery**, including response planning and business continuity concepts
- Specialized modules in:
  AI methods in cybersecurity (machine learning for threat detection)
  Intrusion Detection Systems (IDS) and **Digital Forensics**
  Security for IoT, cloud, mobile, and industrial systems
- Gained practical exposure to **Linux administration**, **Docker fundamentals**, and **network security monitoring**
- Participated in collaborative security seminars, threat assessments, and technical presentations

Cloud Security Automation & Continuous Compliance

- Automated IAM compliance checks using **AWS Config** and **Prowler**, aligned with **CIS AWS Foundations Benchmarks**, enabling continuous detection of identity misconfigurations.
- Designed and enforced **IAM Policy-as-Code workflows** using **Lambda and CloudFormation**, applying **least privilege** principles and **permission boundaries**.
- Implemented **CI/CD security guardrails** using **AWS CodeBuild and CodePipeline** to block insecure IAM configurations before deployment.

- Conducted **IAM risk assessments** by analyzing access policies, privilege escalation paths, and compliance findings across cloud resources.
- Implemented **identity lifecycle management** including **RBAC**, **MFA enforcement**, and **temporary access controls** using IAM roles and session-based permissions.
- Simulated **IAM security incidents** and performed forensic analysis using **AWS CloudTrail** and **CloudWatch Logs** to trace identity actions and policy violations.