AKHILA

CYBERSECURITY ENTHUSIAST

+91 7670989013
AKHILA.NETHA08@GMAIL.COM
HYDERABAD, TELANGANA

OBJECTIVE

Motivated and diligent cybersecurity enthusiast with hands-on experience in various aspects of cybersecurity through structured training. Proficient in Linux administration, network security, penetration testing, vulnerability management, cryptography, and web application security. Eager to apply theoretical knowledge and practical skills in a professional cybersecurity role to safeguard digital assets and networks.

SKILLS & ABILITIES

- **Operating Systems:** Linux, Windows
- **Cybersecurity Domains:** Network Security, Penetration Testing, Web Application Security, Vulnerability Management
- **Tools & Technologies:** Wireshark, BurpSuite, Nikto, OWASP-Zap, Sqlmap, Aircrack-ng, Metasploit
- **Penetration Testing:** OSINT, Exploitation (Automated), Password Cracking, Red Team vs Blue Team
- **Web Security:** OWASP Top 10, CMS Enumeration, Web Application Firewalls
- **Networking:** TCP/IP, IP Addressing, Subnetting, DNS, DHCP, VPN, IDS/IPS, NAT
- **Cryptography:** Symmetric and Asymmetric Ciphers, SSL/TLS, Hashing, Digital Signatures
- **Scripting:** Shell Scripting, Python (basic programming for automation)
- **Cybersecurity Frameworks & Compliance:** GDPR, HIPAA, SOX, ISO 27001, NIST, PCI-DSS

EDUCATION

June 2021-2025

Computer science engineering
Megha engineering college

B.TECH

june 2018-2020

M.P.C
Sri chathanya Junior college

Intermediate

June 2018 **SSC**
ST. Andrews grammer high school

Cybersecurity Training

Hacker shool
Cybersecurity Training Program

- **Introduction to Cyber Security:** Learned the fundamentals of cybersecurity, including the CIA Triad, vulnerability, threat, and risk management.
- **Linux Essentials:** Gained experience with Linux OS, including architecture, distributions, and command-line operations. Proficient in package management and system administration.
- **Linux Administration:** Administered users and groups, managed file permissions, implemented special permissions, and performed disk management and service management tasks.
- **Networking Fundamentals:** Acquired knowledge of computer networks, IP addressing, subnetting, OSI and TCP/IP models, and key protocols like TCP, UDP, ICMP, and ARP.
- **Network Security:** Hands-on experience with firewalls, IDS/IPS, VPN tunneling, DMZ, and honeypots. Familiar with DNSSEC and network services like DNS, DHCP, and SNMP.
- **Vulnerability Management:** Proficient in vulnerability scanning, assessment, risk categorization, and patch management. Knowledgeable in CVSS scoring and assessment tools.
- **Penetration Testing:** Experience with ethical hacking tools like BurpSuite, Nikto, and SQLmap. Understanding of penetration testing phases, OSINT, and automated exploitation.
- **Cryptography:** Knowledge of symmetric and asymmetric ciphers, SSL certificates, digital signatures, and disk encryption techniques.
- **Web Application Pentesting:** Practical experience in identifying and exploiting web vulnerabilities, including OWASP Top 10 risks and CMS exploitation.
- **Bug Bounty Insights:** Understanding of bug bounty platforms, reconnaissance techniques, and reporting vulnerabilities.
- **Mobile, IoT & Cloud Security:** Basic understanding of mobile app vulnerabilities, IoT security, and cloud security architectures.
- **Social Engineering & Wi-Fi Security:** Techniques for defending against social engineering attacks, and securing Wi-Fi networks.

Projects & Hands-on Experience

Capture the Flag (CTF) Challenges

- Participated in multiple CTF competitions, applying skills in penetration testing, web vulnerabilities, and cryptography to solve real-world cybersecurity puzzles.

Vulnerability Scanning and Penetration Testing (Personal Project)

- Conducted a vulnerability assessment of a virtual network environment using tools like Nessus, BurpSuite, and Metasploit.
- Successfully exploited common vulnerabilities such as SQL injection, XSS, and command injection.

Network Traffic Analysis (Wireshark)

- Captured and analyzed network traffic to identify malicious activities such as DNS spoofing and unauthorized access attempts.

Web Application Security (OWASP-Zap, Nikto)

- Identified security flaws in a vulnerable web application, focusing on OWASP Top 10 vulnerabilities, and reported findings with remediation suggestions.

COMMUNICATION

- **Languages:** English, Telugu, hindi
- **Interests:** Ethical Hacking, Cybersecurity News, Tech Blogs