

# LIKHITH KUMAR P

CYBER SECURITY PROFESSIONAL 📍 CHENNAI, INDIA 📞 9498327052

## ◦ DETAILS ◦

Chennai  
India  
[9498327052](tel:9498327052)  
[kumarlikhith707@gmail.com](mailto:kumarlikhith707@gmail.com)

## ◦ TECHNICAL SKILLS ◦

Vulnerability assessment and risk management

Penetration testing

Security Information and Event Management

Cloud, Mobile device, Network, Asset and Application security

Identity and access management

Incident response

Security Frameworks (NIST, ISO 27001)

Threat detection (IDS/IPS)

Log Analysis

## ◦ TOOLS ◦

Nmap (network scanning)

Nessus (vulnerability assessment)

Wireshark (network security)

Gobuster (pentesting)

John the ripper (password cracking)

VMware

## ◦ SOFT SKILLS ◦

Communication and documentation

Time management and team player

Problem solving and analytical thinking

Flexibility and adaptability

Cross functional collaboration

## 👤 PROFILE

Proactive and detail-oriented Cyber security Professional with expertise in threat analysis, risk assessment, and security operations. Skilled in utilizing tools, identifying threats, and implementing protective measures to enhance cyber security defenses. Adept at analyzing attack patterns, ensuring compliance, and strengthening overall security posture. Passionate about safeguarding digital assets and mitigating risks in dynamic environments.

## 📁 INTERNSHIPS

### Investigation and Security Intern at Phoenix Screening Services, Bengaluru

January 2022 — April 2022

- Monitored and responded to security incidents, ensuring that all security threats were mitigated and appropriate counter measures were taken
- Assisted in the investigation of security breaches or other incidents and drafted reports to management

## 🎓 EDUCATION

### Pre-University College(PUC), Kendriya Vidyalaya, Chennai

June 2017 — August 2018

### Bachelors of Science in Forensic Science, Chemistry and Genetics, Garden City University, Bengaluru

June 2019 — July 2022

### Masters of science in Criminology and Forensic Science, Maharajas College, University of Mysore, Mysore

January 2023 — July 2024

## ★ TRAINING AND CERTIFICATIONS

Cybersecurity certification from Apponix Technology, Bengaluru

Ethical Hacking certification, Bengaluru

Insurance Fraud Investigator- Health & Life Insurance certification from Code F Solution, Nagpur

## ★ PROJECTS

### Network scanning using Nmap

Scope : Performed a network scan on a host system to identify open ports and detect potential vulnerabilities.

Tool : Nmap (Network mapper)

Execution : Conducted an Intense Scan using the command: `nmap -A -v -14(host IP address)`. The scan revealed several open ports and detailed information about the services and operating system. Identified port 5357 running Web Services for Devices (WSDAPI), which handles HTTP traffic. Researched the port in the National Vulnerability Database (NVD) and found a known vulnerability with a CVE score of 7.5 (high severity), potentially allowing remote code execution (RCE).

Mitigation : To reduce the attack surface, applied inbound firewall rules using Windows

Defender Firewall with Advanced Security to block the vulnerable port, preventing unauthorized access.

Impact : Enhanced the system's security posture by identifying and mitigating a high-severity vulnerability.

#### **Vulnerability scanning using Nessus**

Scope : Conducted a vulnerability scan on a host system to identify security weaknesses.

Tool : Nessus

Execution : Performed an Advanced Scan using Nessus with its default configuration. After the scan was completed, we obtained a vulnerability list for the system. The scan revealed a medium-severity vulnerability with a CVSS score of 5.3: SMB signing not required on port 445, making the system vulnerable to man-in-the-middle (MITM) attacks. Accessed the vulnerability's description and recommended solution in Nessus.

Mitigation : Enforced SMB signing by updating Local Group Policy configurations, significantly strengthening network communication security and reduced security vulnerabilities by 30% through regular network scans.

Impact: Improved the system's security posture by mitigating the SMB vulnerability and reducing the risk of MITM attacks.

#### **Network protocol analyzer using Wireshark**

Scope : Captured and analyzed network traffic in real time for security analysis, troubleshooting and security analysis.

Tool : Wireshark

Execution : Monitored the Wi-Fi network interface and captured live packets. Generated traffic by browsing websites and pinging a server. Applied filters and inspected individual packets to review source/destination IPs, protocols, and payload data, helping detect suspicious behavior or unencrypted information.

Impact: Strengthened network monitoring capabilities by identifying anomalous traffic patterns and analyzing packet-level data to detect potential security threats and unencrypted transmissions.

#### **Password Cracking Using John the Ripper in Kali Linux**

Scope : Used John the Ripper to test password strength by performing hash cracking on a target system.

Tool : John the Ripper (Kali Linux)

Execution : Extracted password hashes from the target system. Used the command and applied a dictionary attack using a predefined wordlist. For stronger passwords, performed a brute-force attack, Successfully cracked weak passwords, demonstrating vulnerability in poorly secured systems.

Impact : Strengthened penetration testing proficiency by successfully identifying weak credentials, emphasizing the need for robust password policies to mitigate unauthorized access risks.