

NITHIEN AACHINTHYA

CYBER SECURITY ANALYST

MY CONTACT

✉ nithienaachinthya774@gmail.com

☎ +91 9717829344

📍 Bangalore, India

🐙 <https://github.com/JINSPLOITER>

SOFT SKILL

- Observation
- Decision making
- Communication
- Multi-tasking

HARD SKILL

- Linux
- Good understanding of network types such as LAN, WAN, WLAN, PAN, MAN, CAN
- understanding and working of IDS and IPS
- OSI model, TCP/IP, UDP, ICMP, HTTP, HTTPS, SMTP, SNMP, DNS, DHCP
- Configuring Routing protocols such as RIP, IGRP, EIGRP, OSPF
- Experience with tools: Aircracking, Hydra, Burpsuite, Metasploit, Nmap, Wireshark, Sqlmap, John-Ripper, Nesuss
- Network Traffic Analysis which includes recording, reviewing and analysing network traffic for the purpose of performance & security
- Establishing connections and firewalls, Troubleshooting network problems

EDUCATION BACKGROUND

● HIGHER SECONDARY SCHOOL

Little Flower Convent Matriculation
Higher Secondary School
2019 - 2020

● DATA SPACE ACADEMY

Diploma in Cyber Security
2022 - 2024

ABOUT ME

Results-driven cyber security professional with excellent academic credentials and a dedication to safeguarding sensitive data skilled in network security, vulnerability assessment and responding to incidents possesses a deep understanding of security frameworks and best practices ready to contribute expertise in securing digital assets and mitigating risks

PROJECT

EDUREKA

2024

Mini Project : Secure User Access Management in Linux

- Proficient in Linux user access management, employing commands like useradd, usermod, passwd, and groupadd to create, modify, and manage user accounts and permissions.
- Implemented robust user authentication and authorization mechanisms using PAM, LDAP, and sudo to secure system access and enforce granular permissions

Mini Project: Web Application Source code Vulnerability Analysis

- Conducted in-depth source code reviews to identify vulnerabilities (SQL injection, XSS, CSRF) and provided actionable remediation recommendations.
- Employed static and dynamic analysis tools to assess code quality, security posture, and compliance with industry best practices.

Mini Project: CTF NETWORK SECURITY (Capture The Flag) Challenge

- Enhanced network security expertise through CTF participation, specializing in vulnerability identification, exploitation, and defense mechanisms.
- Demonstrated proficiency in network protocols, packet analysis, and intrusion detection systems by successfully tackling CTF challenges.

NITHIEN AACHINTHYA

CYBER SECURITY ANALYST

PROFESSIONAL EXPERIENCE

Freelance Cybersecurity Analyst Experience

KIDS.COM PRE,SCHOOL

NETWORK SECURITY ASSESSMENT

JUNE 2023 - NOVEMBER 2023

- Conducted a comprehensive vulnerability assessment of the client's network infrastructure.
- Identified and prioritized critical vulnerabilities, including weak passwords and outdated software.
- Implemented security best practices, such as firewall configuration and intrusion detection system deployment.
- Provided detailed recommendations for improving network security and compliance with industry standards.

SELF-TAUGHT

SELF-TAUGHT MALWARE ANALYSIS

- **Specific Tools:** Mention proficiency in tools commonly used for malware analysis, such as IDA Pro, Ghidra, OllyDbg, Wireshark, and sandbox environments.
- **Programming Languages:** Highlight programming languages like Python, C, or assembly, which are essential for understanding malware behavior.
- **Technical Skills:** Include skills like reverse engineering, static and dynamic analysis, behavioral analysis, and network traffic analysis.

INTERNSHIP

DATA SPACE ACADEMY

JR. Penetration Tester

NOVEMBER 2023 - APRIL 2024

A Junior Penetration Tester internship provides an invaluable opportunity to gain hands-on experience in the field of cybersecurity. Interns typically work under the guidance of experienced professionals to learn the intricacies of identifying and exploiting vulnerabilities in systems, networks, and applications.

KEY RESPONSIBILITIES MAY INCLUDE:

- **Vulnerability Assessment:** Conducting thorough scans and tests to identify potential weaknesses in systems and applications.
- **Penetration Testing:** Simulating real-world attacks to assess system security and resilience.
- **Tool Usage:** Mastering penetration testing tools like Burp Suite, Metasploit, Nmap, and others to conduct effective assessments.
- **Report Writing:** Documenting findings clearly and concisely, providing actionable recommendations for remediation.
- **Research:** Staying updated with the latest security trends, vulnerabilities, and attack techniques.

Interns often participate in team projects, collaborate with other security professionals, and contribute to the overall security posture of the organization. This experience provides a strong foundation for a career in cybersecurity and offers opportunities for professional growth and development.

CERTIFICATIONS

- Certified Ethical Hacker (CEHv12)
- Certified Information Systems Security Professional Training (CISSP)
- Certification in web Application penetration Testing
- Certification in Network penetration Testing
- Certification in python programming
- Certification in Bug Bounty
- Certification in Networking (CCNA)
- Advance Diploma in cyber security (overall certificate)