NITIN SHARMA

SECURITY ENGINEER & SECURITY ANALYST

Aligarh City, 202001 • nitinsharmahd123@gmail.com • (+91) 9999999999

PROFESSIONAL SUMMARY

Developed critical analytical skills and problem-solving abilities in a fast-paced cybersecurity environment. Demonstrated success in identifying and mitigating security threats while maintaining network integrity.Seeking to transition into new fields, leveraging transferable skills to drive success in diverse environments.Offering solid understanding of cybersecurity fundamentals and willingness to learn and develop within this dynamic field. Contributes keen ability to identify and mitigate potential security risks through diligent monitoring and analysis. Ready to use and develop skills in network defense and threat analysis in a Security Analyst role.

WORK EXPERIENCE

GRADIENT CYBER **Southlake, Texas, United States**

CyberSecurity Analyst **07/2025-Present**

- Investigated security alerts, triaged incidents, and documented detailed findings in clear, actionable reports.
- Collected and analyzed Indicators of Compromise (IOCs) from multiple threat intelligence sources to enhance detection and response capabilities.
- Monitored and analyzed Active Directory (AD) events to detect suspicious activities and potential anomalies.
- Participated in proactive threat hunting and incident response activities to identify, contain, and remediate potential security threats.

FORTL **Alpharetta, Georgia, United States**

Security Analyst **07/2024-06/2025**

- Utilized SIEM tools to aid in real-time monitoring of events, enabling quicker identification of anomalies or potential threats.
- Maintained clear documentation of security processes and procedures, ensuring easy access to critical information for team members.
- Participated in penetration testing exercises to identify weaknesses and recommend strategies for remediation.

PARROT-CTFs **West Columbia. South Carolina, United States**

CyberSecurity Content Creator **06/2024-05/2025**

- Designed and developed hands-on CTF challenges and cyber security labs focused on Red Teaming, Blue Teaming, and vulnerability assessment.
- Created courses on PowerShell scripting, API security, Active Directory exploitation, and malware analysis and many more with step-by-step walkthrough.
- Collaborated with the team to improve CTF platform experience and provided mentorship to participants.

CYBER-CUT **Huston, Texas, United States**

Security Researcher and Consultant **08/2023-02/2024**

- Provide security consultancy services, including vulnerability assessments and penetration testing (VAPT)
- Conduct training sessions on cybersecurity best practices and security tools.
- Develop security policies and procedures to enhance organizational security posture.

EDUCATION

AKTU **Aligarh, IN**

Bachelor of Technology - Computer Science and Engineering **2019-2023**

CERTIFICATIONS

- Blue Team Junior Analyst,Security Blue Teams **22/06/2024**
- SOC L1, TryHackMe **07/09/2024**
- Certified AppSec Practitioner (CAP), The SecOps **22/09/2024**

PROJECTS

SOAR-Flow - Shuffle SOAR with Wazuh SIEM and TheHive

- Shuffle SOAR, Wazuh SIEM, and TheHive to automate security incident response. It enriches alerts using VirusTotal & AbuseIPDB, creates incidents in TheHive, and sends real-time Discord notifications.

FollowLink - Track URL redirects (Python, CLI)

- Python-based command-line tool that allows you to follow and analyze URL redirects. It tracks the history of HTTP redirects, color-codes the HTTP status codes for easy identification, and calculates the total response time. Anyone can install with (pip3 install followlink).

Fileless-PE - EXE & DLL load from URL (Python, CLI)

- Python program Fileless-PEloader.py generates a Python script (PEloader.py) to load a DLL or EXE file from a given URL. It provides functionality to specify a method to execute if the file is a DLL. The script utilizes the python memorymodule library for memory manipulation

SKILLS

Security Analyst – Vulnerability Assessment and Penetration Testing (VAPT), Burp Suite, Wireshark, Metasploit, Nmap, Web Application Security and Active Directory.
SOC L1 – Firewalls and Network traffic monitoring, IDS/IPS, SIEM, SOAR, DLP, EDR, IOCs and Malware Analysis.
Programming and Scripting Languages – Python, GoLang, PowerShell and Bash

ACHIEVEMENTS

Cybersecurity Influencer on Instagram:

- Built a community of over 7500+ followers by sharing valuable insights, tutorials guiding beginners on cybersecurity.
- Created engaging contents to educate and raise awareness about various cybersecurity topics, trends and best practices.
- Established a reputation as a trusted source of information in the cybersecurity field, fostering a community of like-minded professionals and enthusiasts.

Speaker at Parrot-CTFs Online Hacking Event:

- Delivered a session on **Malware Analysis**, covering static and dynamic analysis techniques.
- Showcased real-time analysis of a malicious Windows executable payload in a controlled lab environment.
- Engaged with an interactive audience, highlighting malware analysis techniques to strengthen cybersecurity defenses