DIPESH KUMAR KUSHWAHA

CYBER SECURITY

+91 8797596732
dipeskush15@gmail.com
linkedin.com/in/dipesh-kumar-22454b262
GUNTUR, ANDHRA PRADESH

OBJECTIVE

Certified cybersecurity enthusiast skilled in ELK Stack, penetration testing, and ethical hacking, eager to apply Python, Java, and OWASP expertise to innovative threat detection and incident response solutions.

SKILLS & ABILITIES

- **Cybersecurity:** Vulnerability Assessment and Penetration Testing (VAPT), Ethical Hacking, Cybersecurity Analysis, Web Application Security, Cryptography, Digital Forensics, Threat Detection, Incident Response.
- **Programming Languages:** Python, Java, c
- **Cybersecurity Tools:** Nmap, Metasploit, Burp Suite, Wireshark, ELK Stack, Splunk, OpenVAS, etc.
- **Systems & Networking:** Linux, Computer Networking, Network Security
- **Security Frameworks:** OWASP, CISCO
- **Automation & Analysis:** Developed Python scripts for SOC automation (log ingestion, alert enrichment, threat intelligence lookup using APIs like VirusTotal and MISP); Utilized ELK Stack to analyze logs and detect attack vectors (e.g., credential stuffing, DNS tunneling)
- **Client-Facing Skills:** Solution Demonstration, Interpersonal Communication, Effective Communication for Cybercrime Reporting

PROJECT

ELK Stack Log Analysis

- Utilized ELK Stack (Elasticsearch, Logstash, Kibana) to analyze log data, identifying indicators of compromise such as credential stuffing and DNS tunneling attack vectors.
- Configured dashboards in Kibana for real-time visualization of security events, supporting proactive incident response.

SOC Workflow Automation with Python

- Designed and implemented a Python script to automate Security Operations Center (SOC) workflows, including log ingestion, alert enrichment, and threat intelligence lookup using APIs (e.g., VirusTotal, MISP).
- Enhanced threat detection by automating correlation of security events with external threat intelligence feeds, streamlining incident response.

Web Application Security Testing

- Conducted penetration testing using Burp Suite and Metasploit to identify and mitigate vulnerabilities in web applications, adhering to OWASP standards.
- Implemented security measures to protect applications from threats like SQL injection and XSS, and documented recommendations for policy improvements

Network Intrusion Detection and Response

- Built a virtualized Network Intrusion Detection System using Snort and Wireshark on Linux, detecting malicious traffic and configuring firewall rules.
- Investigated security incidents and provided actionable recommendations, enhancing incident response strategies and system security

WEB APPLICATION SECURITY ASSESSMENT

- Conducted penetration testing on a web application to identify security vulnerabilities using ethical hacking techniques.
- Employed tools like WhatWeb, Wfuzz, Dirb, Curl, and SQLMap for reconnaissance, directory enumeration, and vulnerability exploitation.
- Identified critical issues: outdated software (Apache 2.4.3, PHP 5.4.7), directory listing vulnerabilities, exposed error logs, and SQL injection flaws.
- Provided actionable recommendations, including software updates, input sanitization, and Web Application Firewall (WAF) implementation.

EDUCATION

Bachelor of Technology in Cyber security

- Vignan's Foundation for Science, Technology, and Research (Vignan's University), Guntur, Andhra Pradesh, India
- CGPA: 7.6 out of 10 (till my completion of 3rd year)
- Year: 2022-2026

Intermediate

- DAV Sushil Kedia Viswa Bharati secondary school, Lalitpur, Nepal
- With PCM
- Year: 2022

Secondary School

- Viswa Niketan Secondary School, Kathmandu, Nepal
- GPA: 3.60 out of 4
- Year: 2020

CERTIFICATES

- Cybersecurity and Real-Time Security Operations Center (SOC) Project NULLCLASS
- Blue Team Junior Analyst
- Google Cyber security (Offered by coursera)
- Ethical Hacking Bootcamp (from Udemy)
- Digital Forensics
- Cisco LABS Crash Coures By EC-Council
- Practical Cyber Security for Cyber Security Practitioners by NPTEL.
- MERN Full Stack

COMMUNICATION

- **Technical Communication:** Delivered clear and concise presentations of cybersecurity solutions to technical and non-technical audiences, enhancing stakeholder understanding.
- **Interpersonal Communication:** Collaborated with cross-functional teams fostering effective communication to align project goals and share findings.
- **Cybercrime Reporting:** Articulated detailed incident analysis supporting cybersecurity operations and reporting requirements.
- **Languages:** English, Hindi, Nepali

LEADERSHIP

• **Technical Mentorship:** Mentored peers in cybersecurity concepts, including ELK Stack log analysis.

• **Initiative in Cybersecurity:** Spearheaded the development of custom correlation rules for ELK Stack.

• **Team Collaboration:** Fostered effective communication in interdisciplinary projects, aligning.