Prajwal Kumar Pandey

Nepal prajwal5809@gmail.com +9779867454595 in/prajwal-kumar-pandey-215568280

SUMMARY

Security Engineer specializing in Cloud Security, Incident Response, and Threat Hunting. Experienced in both offensive and defensive security, with a focus on securing cloud environments, threat detection, and risk mitigation. Proficient in cloud-native security tools, vulnerability analysis, and real-time threat monitoring across multi-cloud infrastructures. Skilled in implementing proactive security measures, security hardening, and automation to enhance security posture. Adept at leveraging offensive testing and defensive strategies to identify and mitigate complex cyber threats in fast-paced environments.

SKILLS

Cloud Security & Incident Response: Microsoft Sentinel, MS XDR/EDR, ENTRA, Microsoft Defender for Cloud

Network Security & Log Analysis: Firewalls, Security Event Logs Analysis

Web Application Security: Overthewire(Natas, Bandit), PWN College(Taking web, Web security), DVWA, OWASP TOP 10

Ethical Hacking: Nmap, Burp Suite, Metasploit, Nessus, Openvas, Wireshark, ZAP

Operating systems: Linux, Windows

Frameworks and Tools: Git, Docker, Powershell, Python

EXPERIENCE

Cybersecurity Consultant

DanpheLink **March 2025 - Present**

- Deliver security consulting services to clients, including SOC, IR and best practice implementation.
- Create cybersecurity training content and conduct workshops for diverse audiences.
- Led the response to a **Redtail brute-force malware attack**, managing incident detection, analysis, and remediation processes.
- Identified and mitigated **unauthorized SSH access**, effectively containing the breach by implementing robust **UFW rules** and restricting access to only the organization's public IP.
- Conducted a **deep-dive investigation**, discovering malicious files, unauthorized SSH keys, and modified cron jobs used for persistence.
- Implemented a full system **hardening** strategy, including revoking compromised SSH keys, changing user passwords, and applying **SSH security** best practices (key-based authentication, root login restrictions).
- Performed detailed analysis to track malicious activity, identified **Indicators of Compromise (IOCs)**, and ensured full **system recovery**.
- Enhanced the security posture of the server through **continuous monitoring**, malware detection, and vulnerability scanning using **chkrootkit** and **rkhunter**.
- Delivered a comprehensive **Incident Response report** detailing the attack vector, timeline of events, and recommended actions for future prevention, which was communicated to stakeholders.
- Investigated and mitigated an **insider threat incident** involving **unauthorized MongoDB database access** by a former developer who exploited an exposed **Cloudflare tunnel** to access the system and disrupt operations.
- **Regained control** through quick detection of unmodified credentials, and reset root and user passwords.
- Identified and remediated multiple system configuration weaknesses, including **residual database credentials**, **improper access controls** on **Cloudflare tunnels**, and lack of real-time monitoring of database access.
- Provided actionable insights for tightening security, including **removing residual credentials**, implementing **strong access control policies**, and ensuring **proper offboarding** of former employees to prevent similar future incidents.

Security Engineer – Incident Response

Stellar Computer Systems **August 2024 - January 2025**

- Lead end-to-end incident response and security monitoring in Azure-based environments, utilizing Microsoft Sentinel, XDR/EDR, Entra, and Recorded Future threat intelligence.
- Proactively detect, investigate, and mitigate security threats by analyzing SIEM (Microsoft Sentinel), Fortinet, and Palo Alto network logs.
- Improved team incident response times by 46.43%, reducing average resolution from 56 to 30 minutes, with personal average under 20 minutes.
- Collaborate closely with internal stakeholders and external vendors for incident escalation, containment, remediation, and post-incident reviews.
- Develop and enhance Standard Operating Procedures (SOPs) to streamline incident response workflows, ensuring faster and more consistent outcomes.
- Produce detailed True Positive (TP) reports to provide actionable threat intelligence for the SOC team and customers, enhancing threat visibility and response strategies.
- Continuously optimize detection, triage, and response processes to minimize operational overhead and improve the SOC's overall effectiveness and agility.

Mentorship

GAJABAR **May 2023 - July 2023**

- Successfully led the development of the "Gwitter" project using PHP, HTML, and CSS, demonstrating strong web development leadership.
- Enhanced cybersecurity knowledge through intensive training on OpenVAS scans and SQL injection..

CERTIFICATIONS

Microsoft Certified: Azure Security Engineer Associate(Az-500)

Azure Administrator Associate (Az-104)

Azure-900

Cloud Penetration Testing with Azure

DevSecOps with Azure

Hacking and Securing Docker Containers

ISC2 CC

Certified Network Security Practitioner (CNSP)

Blue Team Junior Analyst

API Security Fundamentals

Foundations of Operationalizing MITRE ATT&CK v13 Advent of Cyber 2023

AWS Cloud Practitioner Essentials

Incident Response on Windows

Linux for Blue Team

EDUCATION

Bachelor in Computer Engineering

Institute of Engineering, Pulchowk Campus, Tribhuvan University • Lalitpur, Nepal • 2024

Major in Physics and Mathematics

Tilottama College • Butwal, Nepal • 2019

PROJECT

Web-Based Question Collection and Search Application

- Developed a web application focused on collecting and searching for related questions from past IOE exams, with React for the frontend and Django for the backend, ensuring adherence to software engineering principles throughout the development process..

Comprehensive Network Design for Organizational Efficiency

- Designed and implemented a scalable network infrastructure, improving connectivity and scalability.
- Developed detailed network topologies with edge/core routers, OSPF, and VLANs to enhance communication.
- Configured IP pools, DNS, DHCP, and ISP connectivity to ensure reliable network performance..

Crop Yield Prediction Using Remote Sensing

- FInal year project integrating remote sensing, satellite imagery, climate, and soil data, which employs a CNN-LSTM model to predict rice yield in Morang and Jhapa.

INVOLVEMENT

Volunteer

WORLDLINK & LOCUS • November 2023 - December 2023

- Coordinated CTF program in state 5.
- Led volunteers supported by LOCUS and Worldlink, an undergraduate-led non-profit from IOE, Pulchowk Campus.
- Collaborated with school administrators, teachers, and team members for seamless execution..

CTF player

Logpoint • September 2023 - September 2023

- Achieved top 3 placement in Logpoint CTF by effectively analyzing and resolving complex security challenges using advanced problem-solving techniques and Logpoint SIEM