Darpan Neupane

London, ON | 519-488-7114 | darpanne1@gmail.com | www.linkedin.com/in/darpanne | https://darpanne.com/

Summary of Qualifications

CompTIA Security+ certified IT Cybersecurity Professional with expertise in threat detection, incident response, vulnerability management, firewall security and cloud integration. Experienced in database management, disaster recovery planning, scripting, SharePoint administration, and IT asset lifecycle management. Proficient in technical support, IT infrastructure management and enhancing security posture through automation and risk mitigation.

Education

Postgraduate Certificate in **Information Security Management** | Fanshawe College | January 2025 (Dean's Honor Roll)
Postgraduate Certificate in **Network and Security Architecture** | Fanshawe College | January 2024
BE in **Computer Engineering** | Pokhara University | January 2021

Professional Experience

Technical Support / Live Chat Support   *December 2021 – October 2024*
Integrity Info Tech | Sheridan, WY, USA | Kathmandu, Nepal
- Managed IT administration, troubleshooting, and Tier 1 & 2 support for hardware, software and networks.
- Resolved 90%+ of tickets on the first attempt, boosting efficiency and user satisfaction.
- Managed cPanel for website hosting, DNS records, email configuration, and SSL certificate renewal.
- Assisted in Active Directory management, DNS configuration, SharePoint, Teams and OneDrive setup.
- Managed IT asset lifecycle, ensuring accurate inventory tracking and timely upgrades of hardware, software.
- Assisted users in hardware rollouts, system setups, and remote troubleshooting, improving system uptime.
- Created knowledge base articles for common IT issues troubleshooting and self-service capabilities.

Cybersecurity Analyst   *July 2019 – January 2021*
Baruwals Group | Kathmandu, Nepal (Hybrid)
- Collaborated with senior analysts on threat detection and response strategies.
- Monitored and analyzed SIEM alerts, network logs, and security events to detect and mitigate threats.
- Investigated security incidents, malware infections, unauthorized access attempts, and phishing campaigns.
- Assisted in firewall configuration, VPN setup, and security policy implementation to enhance network defenses.
- Managed endpoint security, access control, and disaster recovery planning.
- Conducted security awareness training, reducing the risk of phishing and social engineering attacks.

Technical Projects

https://github.com/darpanne/cyberportfolio
- **Ethical Hacking Lab** – Conducted penetration testing using Kali Linux, Metasploit, and Burp Suite
  https://github.com/darpanne/Ethical-Hacking-Lab
- **Firewall Management** – Configured Cisco ASA, pfSense, and Palo Alto firewalls, managing rules and intrusion detection. https://github.com/darpanne/Firewall-Management
- **Security Onion & Wireshark** – Set up SIEM and network monitoring to analyze logs and detect threats
  https://github.com/darpanne/Security-Onion-and-Wireshark
- **Digital Forensics** – Performed disk imaging and forensic investigations using Magnet Axiom, Sleuthkit, and ProDiscover. https://github.com/darpanne/Digital-Forensic
- **Information Security Lab** – Implemented access control and encryption techniques. Conducted password cracking, steganography, and backdoor analysis. https://github.com/darpanne/Information-Security-Lab
- **Active Directory & Server Security:** Managed Windows Server, configured Active Directory, Group Policy, DNS, and access controls. https://github.com/darpanne/Securing-Server

Technical Skills

- **Programming Language**: HTML, JS, CSS, PHP, MYSQL, C, C++
- **Cybersecurity & Threat Detection:** Threat Hunting, Incident Response, SIEM Analysis (Splunk, Security Onion, Kibana), Security Monitoring, Vulnerability Assessment, Log Analysis
- **Network & Security:** Firewall Management (Palo Alto, Cisco ASA, pfSense), IDS/IPS, VPN Configuration, Secure Network Architecture, Encryption Techniques
- **Operating Systems**: Windows 10/11, Linux (Ubuntu, Kali), macOS, Windows Server 2016/2019/2022
- **Endpoint Security & Patch Management:** Windows Defender, BitLocker, Microsoft Endpoint Manager
- **Identity & Access Management:** Active Directory, Group Policy, Azure AD, User Authentication, Access Control
- **Digital Forensics & Compliance:** Disk Imaging, Steganography, NTLM & LM Password Cracking, Backdoor Analysis, Magnet Axiom, Sleuthkit, ProDiscover, Security Standards (NIST, ISO 27001, PCI-DSS)
- **Scripting & Automation:** Python, PowerShell, Bash (for security automation, log analysis, and task scripting)
- **Networking & Protocols:** TCP/IP, VLANs, DHCP, DNS, Secure Configurations, Wireshark
- **Virtualization**: VMware, Hyper-V
- **Ticketing & Remote Support**: Jira, Zendesk, AnyDesk, TeamViewer
- **Web & cPanel Management**: SSL/TLS certificate management, HTTPS configurations, DNS management, Cloudflare setup, and cPanel administration.

Certifications

- **CISSP** (In Progress)
- **CompTIA Security+ (SY0-701)** | December 2024
- **Google Cybersecurity Certificate** | November 2023
- **Registered Computer Engineer** | Nepal Engineering Council | March 2022