**Hanumanth Praneeth Palaparthi**

**Mail**: hanumanthpraneeth12@gmail.com | **Ph No:** +1 3652758987 | Ontario, Canada

**LinkedIn:** www.linkedin.com/in/hanumanth-praneeth-palaparthi

**PROFESSIONAL SUMMARY**

* Around **5+ years** of IT involvement as a **Technical Support Engineer**, specializing in **system administration**, **network troubleshooting**, and **cybersecurity** within diverse **client/server** and **cloud environments**.
* Experienced in monitoring and responding to security alerts using **SIEM**, **EDR**, and basic **NDR platforms**. Hands-on with **incident response**, including **escalation**, **investigation**, **containment**, and **remediation**.
* Skilled in **cyber threat hunting** and identifying **attack patterns** by analyzing **event logs**, **system behavior**, and **network traffic**.
* Well-versed with core **IT Support processes**, **incident management**, and **problem resolution**, ensuring high availability and performance of critical infrastructure.
* Expertise in managing and maintaining various **operating systems** including **Windows (Client & Server)**, **macOS**, and **Linux (Ubuntu, CentOS)**, performing **system hardening** and routine maintenance.
* **CCNA Certified** and proficient in **network administration** and **troubleshooting**, including **Cisco R&S fundamentals**, configuring **Firewalls**, **VPNs**, and **Routers**, and utilizing **network utilities** (**ping**, **traceroute**, **netstat**, **nslookup**) for effective diagnostics.
* Strong foundation in **cybersecurity measures**: implementing **MFA**, **Endpoint Protection**, conducting **Vulnerability Assessments** (**OpenVAS**, **Nmap**), performing **Ethical Hacking** (**Metasploit**, **Burp Suite**, **SQLMap**, **Hydra**), and contributing to **Incident Response** and **IT risk management** (**ISO 27002**, **PCI DSS**).
* Experienced in evaluating **system/application log files** (**Apache logs**, **Tomcat logs**, **Windows Event Viewer**, **Linux syslog**) for accurate problem diagnosis and **root cause analysis**.
* Familiar with **SOAR** and **Email Security** solutions and experienced in supporting **Microsoft 365** and **project documentation**.
* Proven expertise in **diagnosing** and **resolving** complex IT issues across **Windows**, **macOS**, and **Linux** environments.
* Adept at providing exceptional **user support, managing incidents**, and contributing to knowledge bases.
* Eager to leverage strong **problem-solving**, **communication**, and **analytical skills** to excel in an **IT Help Desk or Technical Support** role.

**SKILLS & CERTIFICATIONS**

**Operating Systems:** Windows (Client & Server), macOS, Linux (Ubuntu, CentOS, Red Hat Enterprise Linux)  
**Networking:** Cisco R&S, Firewalls, VPNs, Routers, Hardware Security, TCP/IP, DNS, DHCP; Utilities (ping, traceroute, netstat, nslookup, ipconfig, ifconfig)  
**Web Servers:** Apache HTTP Server (Configuration, Virtual Hosts, Modules), Apache Tomcat (Deployment, JVM Tuning)  
**Scripting/Automation:** Bash Shell Scripting, Python, Batch Scripting (Windows)  
**IT Services:** FTP, SFTP, SMTP, HTTP/HTTPS, SSH, RDP, DNS, Active Directory (basic interaction)  
**Cybersecurity:** SIEM (basic to intermediate), EDR, NDR (introductory), SOAR (familiar), Email Security (admin level), MFA, Endpoint Protection, Vulnerability Assessment (OpenVAS, Nmap), Ethical Hacking (Metasploit, Burp Suite, SQLMap, Hydra), Application Security, Information Security, Infrastructure Penetration Testing, Encryption, Incident Response, Access Control, Network Security **Cloud & Software:** Microsoft 365, SQL, NoSQL, MongoDB, Git, Jenkins, CI/CD, Servers **Troubleshooting & Monitoring:** System/Application Log File Analysis, Windows Event Viewer, Performance Monitor, Task Manager, Resource Monitor, Syslog **Tools & Methodologies:** Agile, Jira, Project Management Software, MS Office (Excel, Word, PowerPoint), Visio for flowcharts and diagrams **Soft Skills:** Communication, Collaboration, Problem-Solving, Attention to Detail, Decision-Making Under Pressure, Prioritization, Stakeholder Management

**CERTIFICATIONS:**

* Cisco Certified Network Associate (**CCNA**) (2025)
* Ethical Hacking (Beginner to Advanced)
* Penetration Testing

**PROFESSIONAL EXPERIENCE**

***Technical Support Engineer*** | ***Computenext Pvt. Ltd.*** | 01/2018 – 03/2023

* **Description:** Provided frontline and escalated technical support for a diverse user base, ensuring high availability and performance of IT infrastructure and applications. Managed IT risk and implemented cybersecurity measures in a fast-paced environment.
* **Responsibilities & Achievements:**
* Provided **IT and network support** to over 150 users across **Windows**, **macOS**, and **Linux** environments, maintaining a **95% first-call resolution rate**.
* Monitored **system and network security events** using **SIEM** and **EDR tools**; analyzed **logs** and escalated potential threats to the incident **response team**.
* Actively participated in **incident response processes**, applying **containment** and **remediation strategies** and documenting all actions.
* Applied knowledge of **security policies** to implement **endpoint protection**, **VPNs**, and **access controls**; performed **malware analysis and removal**.
* Supported and configured **network infrastructure** including **Cisco routers**, **firewalls**, and **VPN concentrators** to ensure **secure connectivity**.
* Conducted regular **vulnerability assessments** and **threat analysis** using **OpenVAS**, **Nmap**, and other tools, documenting **remediation steps**.
* Assisted in administering **Email Security (M365)**, applying **anti-phishing policies** and monitoring **secure email gateways**.
* Maintained **compliance** with **ISO 27002** and **PCI DSS** standards; supported **audits** by providing **reports and logs**.
* Reduced technical backlog by 40% by streamlining **escalation procedures** and implementing **remote support tools**.
* Trained junior staff on basic **incident response**, **network diagnostics**, and **log analysis techniques**.

**PROJECTS**

***1. Home Network Security Hardening & Threat Analysis Lab*** | (Jan - April 2025)

* Engineered a virtualized lab environment using **Kali**, **Ubuntu**, **Windows 10**, and **pfSense** to simulate and secure a realistic home network.
* Implemented system hardening techniques on **Linux** and **Windows VMs**; configured secure **SSH** access and robust **firewall rules** to enhance system resilience.
* Conducted thorough vulnerability assessments using **OpenVAS** and **Nmap** to identify and document critical security flaws across the simulated network.
* Performed hands-on penetration testing utilizing tools like **Metasploit**, **Burp Suite**, **SQLMap**, and **Hydra**, successfully exploiting identified vulnerabilities for educational purposes.
* Developed practical remediation strategies and configured basic **log aggregation (Syslog)** for centralized security monitoring and incident detection.
* *(Git: https://github.com/hanumanthPraneeth/home-network-security-lab)*

***2. Automated Network Vulnerability Assessment Tool (Python)***

* Engineered a Python-based tool for automated network vulnerability assessment, significantly reducing manual effort in identifying misconfigurations and security weaknesses.
* Developed and integrated modules for network scanning (e.g., port scanning, service enumeration) and vulnerability detection, leveraging libraries such as Scapy and Nmap-Python.
* Designed the tool to generate actionable reports with categorized vulnerabilities and suggested remediations, enhancing efficiency in security posture management.
* Git: https://github.com/hanumanthPraneeth/advanced\_network\_vuln\_assessment\_tool

***3. Keylogger (Ethical Research)***

* Developed an ethical keylogger using **Python**, leveraging libraries such as ***pynput*** for cross-platform keystroke capture and processing.
* Implemented robust **file I/O** for local logging of captured keystrokes, including timestamping for contextual analysis.
* Designed and integrated **simulated data exfiltration methods** (e.g., secure email transfer via ***smtplib***) to demonstrate data breach scenarios ethically within controlled environments.
* Structured the application for **background operation**, mimicking real-world threat actors' techniques for stealth, while ensuring clear ethical guidelines.
* Utilized **Git and GitHub** for version control, collaborative development, and project showcasing.
* Git: https://github.com/hanumanthPraneeth/keylogger\_project

**EDUCATION**

***Master of Science in Computer Science*** | Lakehead University, Canada | 2022

* ***Specialization***: Specialization in Artificial Intelligence & Machine Learning, complementing strong foundational IT and cybersecurity expertise.

***Bachelor of Technology in Computer Science*** | GITAM University, India | 2018

**ADDITIONAL HIGHLIGHTS**

* Experienced in **communicating cyber risks clearly** to both **technical and non-technical stakeholders**.
* **Proactive** and **self-motivated**, capable of working **independently** or **collaboratively** on **transformative security programs**.
* Comfortable **handling sensitive data** and responding to **cyber incidents under pressure**.
* Strong **documentation skills** with experience in creating **technical SOPs**, **diagrams (Visio)**, and **management reports** to support **security decisions**.
* Known for **clear judgment**, **adaptability** in **fast-paced environments**, and a **relentless drive to secure IT assets**.