AKSHAT MEHTA

Edmonton, Alberta, Canada 780-245-5616
www.linkedin.com/in/mehtakshat akshat.mehta42@gmail.com

SUMMARY

Results-driven Network Support professional with a master's degree in Information Systems Security and over 2 years of hands-on experience. Proven track record in providing comprehensive network support and security solutions. Adept at troubleshooting, optimizing, and maintaining network infrastructures. Eager to contribute my technical expertise in a challenging IT role, while staying abreast of the latest advancements in security technology. Access Control, Network, and Linux experience desired.

PROFESSIONAL EXPERIENCE

Prohost Network Inc. NOV 2021 – NOV 2023
Network Support Engineer | Edmonton, Alberta, Canada

- Utilizing backtracking methods and logs and performing tests, patches, updates and evaluations on software and hardware.
- Performing routine network start-up and shutdown and maintaining control records.
- Managing technical documentation by creating and updating SOPs and providing technical support to end-users and other IT team members.
- Contributed to the deployment of network devices, configuring and administering more than 1000 servers, routers, switches, and firewalls and conducted testing in the networking environment.
- Diagnosed a severe networking failure impacting about 20% of servers, resolving the issue through comprehensive unit tests and cross-checks. This proactive approach reduced downtime for clients, ensuring timely issue resolution.
- Improved network performance by 25% by implementing loop prevention techniques and redundancy.

Kraftek Inc. JAN 2019 - DEC 2019
Junior Network Engineer | Ahmedabad, Gujarat, India

- Configured and maintained network devices, such as switches, routers, and firewalls, ensuring seamless connectivity and network stability. Achieved a 99.5% uptime for critical network components.
- Monitored network performance, identified potential issues, and provided technical support to end-users. Implemented proactive measures, resulting in a 15% reduction in reported network incidents.
- Troubleshot network problems, ensuring timely resolution. Reduced system downtime by 10% through efficient issue resolution.
- Improved network performance by troubleshooting and promptly resolving technical issues.
- Assisted in the design and deployment of a new company-wide network infrastructure, leading to a 30% increase in operational efficiency and a 20% reduction in network-related support tickets.
- Attained an impressive network uptime of 99.9%, surpassing enterprise client SLAs and improving overall network dependability.

EDUCATION

Concordia University of Edmonton JAN 2020 - AUG 2021
Master of Information Systems Security Management

Ahmedabad University AUG 2015 – JULY 2019
Bachelor of Technology, Information and Communication Technology (ICT)

SKILLS & OTHER

- **Tools**: Autopsy, Nmap, Snort, Squert, Wireshark, Zap, MSF Framework, SharePoint, MS Office, PowerShell
- **Operating Systems**: Windows, Ubuntu, Kali, CentOS, MacOS, Security Onion, Parrot OS, Android
- **Protocols**: TCP/IP, FTP/SFTP, DNS, DHCP, SMTP, HTTPS, NAT, SSL/TLS, PPTP, L2TP, IPsec, SSH/Telnet
- **Soft Skills**: Time Management, Attention to Detail, Customer Focus, Conflict Resolution, Leadership, Teamwork, Proficient Communication, Problem Solving, Adaptability

CERTIFICATIONS

- Cisco Certified Network Professional (CCNP)
- CompTIA Security+
- IT Security by Google
- Focus on Privacy by Government of Alberta
- Fortinet NSE 1 & NSE 2

RESEARCH AND TECHNICAL PROJECTS

Creating a Penetration Testing Lab in a Virtual Environment JAN 2021 – APR 2021
Protocol analysis was conducted to exploit victims' PCs using the PCAPs collected and analyzed in Wireshark. The attacker's exfiltration of data was detected, prompting the suggestion for creating specific rules for the Snort IDS team to detect such attacks.

Chained Exploitation on a Network and Its Reconstruction AUG 2020 –DEC 2020
Conducted a chained attack with Nmap and Metasploit, exfiltrated files for the red team. The blue team reconstructed the attack using security tools like Snort, Squill, Bro, Wireshark, and Network Miner, implementing custom Snort rules to detect anomalies.