AKSHAY PATEL

A: Ottawa, Ontario K2J 6N7 | M: +1 613 410 9091 | E: akshay03patel@outlook.com
LinkedIn: https://www.linkedin.com/in/akshay-patel-2303/
GitHub: https://github.com/AkshayPatel03

PROFESSIONAL SUMMARY

With strong problem-solving and analytical skills, Dynamic IT professional with 3 years in Network Security Administration and 2 years in System Administration. Currently pursuing CompTIA Security+ Certification to advance expertise in cybersecurity. Proven ability in troubleshooting, system enhancements, and Network/System vulnerability scans. Eager to apply practical experience and passion for Cybersecurity and Penetration testing in the Canadian IT industry.

TOP SKILLS

Cybersecurity *(Vulnerability Scan and Threat Assessment)*
Worked and gained network and system vulnerability scan experience by providing security service over 3 years in Australian IT companies. Pursuing CompTIA Security+ certification from last 2 months alongside working on my Pen testing skills from my home lab.

Vulnerability/Malware Scanning *(Nessus Essential)*
Employed as a Network Security Administrator at the renowned electronic store, JB Hi-Fi, in Australia for 3 years. Successfully managed the network infrastructure for two branches, each equipped with more than 20 workstations.

PROFESSIONAL EXPERIENCE

Network Security Administrator

Green Light Worldwide Pvt. Ltd. | Hobart, TAS Australia | Mar 2021 – Jan 2024 (Remote)

- Configured and deployed Nessus Essentials for conducting credentialed vulnerability scans targeting Windows systems.
- Assessed vulnerabilities with Nessus and remediated them.
- Implemented Vulnerability Management Function on sandbox networks including Discover, Priorities, Access, Report, Remediate and Verify.
- Configured routers, switches, firewalls, and other hardware to deploy and manage LAN, WAN, and wireless networks.
- Developed Python scripts and tools to automate malware scanning processes, enhancing the efficiency and effectiveness of security operations.
- Implemented custom vulnerability assessment scripts using Python frameworks like Metasploit and Nmap, enabling proactive identification and mitigation of security weaknesses.
- Monitored system performance to promote network speed, availability, and reliability using packet sniffers and Splunk/SIEM tools.
- Corrected network faults and malfunctions to restore connectivity to individual users and entire facilities.

Skills Developed:
Network Configuration | Network Performance Analysis | Nessus Configuration | Nessus Vulnerability Scan and Remediation | Malware Analysis | Cyber Kill Chain Framework | Git/Github | Python Automation | Metasploit Pen Testing | TCP/IP concepts | DNS/DHCP | Disaster Recovery Planning | Kali Linux Penetration testing tools | Wireshark | Nmap.

IT Systems Administrator

Absolute I.T.| Sunshine Coast, QLD Australia | Nov 2018 – Dec 2020

- Set up user accounts, permissions and passwords and defined network policies and procedures.
- Active directory Administration:
  PowerShell Automation, Maintaining and Deploying User Accounts
- Created configuration guides for deploying new desktops, laptops, and mobile devices.
- Configured Remote Access Server (RAS) feature to support NAT/PAT
- Supported, configured, and maintained Windows DNS and DHCP server on Server 2016-2019.
- Utilized cloud based Qualys Vulnerability Scanner for comprehensive vulnerability assessments, prioritized remediation efforts, and ensured compliance with industry standards.
- Maintained cloud-hosted and on-site servers by applying appropriate patches and monitoring hardware health.
- Proven proficiency in Burp Suite for web app security testing, covering active/passive scanning, manual testing, and automated vulnerability detection.
- Performed comprehensive web app security assessments with Burp Suite, identifying SQL injection, XSS, CSRF, and auth bypass vulnerabilities.
- Generated reports outlining network performance, costs, and downtime issues.

Skills Developed:
Microsoft Active Directory | Qualys Vulnerability Scanner | Burp Suite Web Scanning | Identifying SQL injection | Office 365 Administration | Windows Server 2016-2019 | Permissions and Access Control | Spam Management | Shell/PowerShell Scripting | System Maintenance | Performance Monitoring and Optimization | Windows 10/11/ Linux/CentOS/Ubuntu

Junior Java Developer

Softvan Pvt Ltd | Ahmedabad, GUJ India | Apr 2015 – May 2016

- Gathered and analyzed translated functional requirements into technical specifications.
- Obtained and evaluated hardware costs, reporting requirements and security needs.
- Conducted full lifecycle software development from planning to deployment and maintenance.

Skills Developed:
WordPress, Java, JSP| JavaScript, XHTML, CSS | MySQL | Data Structures and Algorithms | ITIL | Data Storage and Retrieval | Debugging and Troubleshooting | Software Deployment

EDUCATION

Master of Engineer – Information Technology (Network and Security Specialisation)

Charles Sturt University |Brisbane, QLD Australia | Jun 2016 – Jun 2018

Bachelor of Engineer – Information Technology

Gujarat Technological University |Ahmedabad, Guj India | Jun 2010 – Jun 2014

SKILLS DEVELOPMENT PROJECTS/ CERTIFICATIONS

Active Directory Environment – Virtualisation

Installed and configured Windows Server 2019, and Windows 11 into my Home Lab VirtualBox to practice Active Directory Administration using PowerShell Automation. Also, set up Remote Access Server (RAS) features to support NAT/PAT. The project also includes the implementation and maintenance of DNS and DHCP services. These services were tested on Windows 11 machines for DHCP IP address distributions.

Home Lab – Virtualisation

Installed and configured Kali Linux, Windows Server 2019, and Windows 11 to practice Vulnerability exploitation and remediation such as ZAP-OWASP, Burp Suit, Metasploit, Nmap and Zen map, Active Directory, DNS and DHCP servers.

Project Title: Automated Vulnerability Scanner and Port Scanner using Python

Developed an Automated Vulnerability Scanner using Python to automate the process of scanning for common security vulnerabilities in network devices and web applications. Leveraged the Nmap library for network scanning and the OWASP ZAP library for web application scanning.

Networking Devices and Initial Configuration – Completed (CCNA equivalent**).**

Cisco Networking Academic

SOFT SKILLS

Active Listening | Adaptability | Critical Thinking | Decision-making | Problem-solving | Teamwork | Time Management | Empathy | Flexibility | Excellent Phone Etiquettes | Self-motivated | Leadership | Troubleshooting | Communication | Multitasking and Prioritization

AVAILABILITIES

Full-time Mon- Fri (Available Weekends if needed) | Start Date: Immediately.

REFERENCES

Available on request