Vandankumar D. Pathak

• +1 647.573.8576 • vandanpathaks@gmail.com • Toronto, ON

Professional Summary:

- Proficient experience in penetration testing and vulnerability assessment of complex web applications, servers, wired and wireless networks that include pre-testing plans, enumerations and reconnaissance, vulnerability identification, exploitation and providing detailed remediations

- Proficient experience in deploying Palo Alto firewalls, implementing policies, integrating with authentication servers, implementing and managing Palo Alto traps on the network environment

- Management and integration of security information and event management (IBM QRadar) in a large network infrastructure

- Excellent communication skills with abilities to resolve intricate networking and software related issues and demonstrated skills in technical reports writing

Technical Skills:

- Operating system & operations: Debian & Kali Linux, Windows; Perform backup and restore, Linux file system, installing and managing packages using any package management tool or, troubleshooting dependency issues

- Security applications and exposure: Metasploit, TCPDump, Nmap, Nessus, Netcat, OpenVAS, Wireshark, Nikto, Burp Suite, w3af, Ettercap, Snort, iptables, reconnaissance, mapping and network scanning, port security, hydra, OWASP tools, sqlmap, dirbuster, exploit modification with python, privilege escalation, sql injection, cross site scripting, XML External Entity Injection and experience with various custom built open source tools, Burp Suite, OWASP ZAP

- Firewalls: Palo Alto Next Generation Firewall, deployment and configuration in the network environment, implementing policies, configuring IPSec and VPN tunnels for GlobalProtect, Configure SYSLOG, integrate with LDAP or RADIUS server, upgrading firmware, configure certificate-based authentication, managing with Panorama, installing traps on endpoints and managing it through the centralized console.

- Security Information and Event Management (SIEM): IBM QRadar, deploying and integrating it in large network infrastructure, configure external security

components such as Symantec ATP and TAXII Feeds threat intelligence, configure vulnerability scanning and prepare detailed reports, investigate offenses and policy tuning, collecting logs from various log sources

- CLI: Bash and PowerShell

Experience:

- **Optiv Inc. Canada** **June 2019 - Present**
  Application Security Consultant

  - As a application security consultant, my main responsibilities are including but not limited to assessing the web applications security posture for many well-known banking and defense clients.

  - Performed an automated scan using multiple scanning platform to map overall web application security and reported severer vulnerabilities.

  - Conduct a colloquy with client development team to address the vulnerabilities that was flagged high and help in the remediations steps.

  - Have discovered many well-known vulnerabilities such as SQL Injection, XML External Entity Injection, Cross-Site Scripting, XPath Injection or even Client-Side template injections.

- **IntelliGO Networks Inc., Toronto, ON** **Jan. 2017-May2019**
  Network Security Engineer

  - Implement IntelliGO Network's Managed Detection and Response (MDR) platform in the virtual environment of a large network infrastructure and configure all the required modules that include receiving logs from various devices, parse the logs using custom filters, prepare dashboards to hunt threats, log analysis and writing detailed MDR reports for various clients

  - Contrivance scanning scope and policies to perform vulnerability scanning against the critical assets or an organization, demonstrate vulnerability by exploiting, create a detailed remediation method and provide a hardening guide & recommendations

Declaration:

I hereby declare that the above-mentioned information is true to the best of my knowledge.

Date: 20th June 2020 Vandan D. Pathak