NIKHIL MAKWANA   [Information Security Specialist]

Toronto, ON | nikhilmakwana1709@gmail.com | Phone: 437-299-8006 | LinkedIn

SUMMARY

Cybersecurity Analyst and graduating Computer Security and Investigations student with hands-on experience in incident response, vulnerability management, penetration testing, cloud security, and governance risk compliance (GRC). Skilled in firewall and SIEM configuration, endpoint protection, and digital forensics. Proficient in Windows, Linux, and cloud platforms (AWS, Azure) with strong knowledge of security frameworks (NIST CSF, ISO 27001, PCI-DSS).

ACADEMIC EXPERIENCE

OWASP ModSecurity WAF with Custom Rule Set | Final Semester Capstone, Winter 2025
- Deployed DVWA in Docker as an attack/defence test environment.
- Configured Apache2 with ModSecurity (OWASP CRS) to implement a custom WAF.
- Validated controls against SQLi, XSS, RCE, and brute force attacks.
- Analyzed ModSecurity audit logs to detect and block malicious traffic.
- **Tools:** Docker, Apache2, ModSecurity, OWASP CRS, Burp Suite, Hydra, Linux.

PROJECTS

Advanced Penetration Testing Labs | Fleming College, 2024–2025
- Conducted spear-phishing attack simulation with malicious VBA payloads.
- Performed fuzz testing against DVWA using Burp Suite to uncover SQLi and XSS.
- Documented findings and provided remediation recommendations aligned with OWASP Top 10.

Digital Forensics & Incident Response Labs | Fleming College, 2023–2025
- Used Magnet Axiom, PowerShell, and Autoruns to investigate malware samples.
- Collected forensic evidence, performed IOC hash analysis, and compared results with NSRL.
- Produced detailed reports suitable for legal or compliance review.

Mastercard Cybersecurity Virtual Experience Program on Forage, May 2024
- Recommended security training improvements and demonstrated expertise in security awareness.
- Analyzed data to recommend security training improvements to enhance security.

Captive Flask Project using Scotia Bank Login Page
- Gained expertise in incident response, vulnerability management, and security operations.
- Improved phishing defences by automating incident triaging within a Security Operations Centre.

CORE COMPETENCIES

Google Cybersecurity Certificate: Incident response, vulnerability management, & system hardening
Qualys PCI Compliance: PCI-DSS, vulnerability detection lifecycle, risk analysis, IAM/GRC
Microsoft Azure Fundamentals (Learning Path**):** Cloud security, governance, & identity management
AWS Cloud Practitioner (Learning Path**):** Core AWS services, shared responsibility, cloud security
TryHackMe Cybersecurity: Labs in penetration testing, network security, & incident response

CORE COMPETENCIES

- **Security Operations:** Firewalls, SIEM (Splunk), IDS/IPS, EDR, IAM/PAM, WAF.
- **Vulnerability Management:** Scanning, penetration testing, remediation planning, PCI-DSS compliance.
- **Governance Risk & Compliance (GRC):** Risk assessments, KPI/KRI reporting, frameworks (NIST CSF, ISO 27001, CIS).
- **Cloud Security:** AWS, Azure, Docker, Kubernetes, cloud security posture management.
- **Digital Forensics & IR:** Evidence collection, IOC analysis, malware investigations, incident triage.
- **Operating Systems:** Windows Server 2022, Windows 10/11, Kali Linux, Ubuntu.
- **Networking:** TCP/IP, DNS, DHCP, VPN, VLANs, Cisco LAN/WAN, Meraki.
- **Scripting & Automation:** Python, PowerShell, Bash (log parsing, automation).
- **Collaboration:** JIRA, Confluence, GitHub.

EDUCATION | Jan 2023 - April 2025

Fleming College | Advanced Diploma | Computer Security and Investigations | Peterborough
- Network and cloud security, forensic analysis, data management, cryptography, access control, security operations, risk management and compliance, and agile methodologies.