

PUNEET GROVER

✉ pgrover.ca@gmail.com 📍 Toronto, Canada in LinkedIn 🐙 GitHub 📝 Medium

👤 Profile

A prudent risk-taker with a background in finance, currently seeking a role in cybersecurity. I possess endpoint and network analysis expertise, focusing on vulnerability assessment, identification, and management. Extensive operational understanding of IDS systems such as Snort and SIEM solutions, including Splunk. Working knowledge of MITRE ATT&CK and NIST.SP.800-53 cybersecurity framework and well-versed in GDPR and PCI-DSS compliance standards.

🧠 Technical Proficiencies

Cybersecurity Defensive Skills - Blue Teaming

- Proficient in utilizing Wireshark and Splunk, to actively monitor network traffic, logs, and system activities, adeptly identifying and responding to any suspicious or malicious behavior in a timely manner.
- Experience in conducting vulnerability assessments to identify and remediate weaknesses, contributing significantly to strengthening the overall security posture of an organization.
- Skilled in implementing incident response strategies, emphasizing using incident playbooks to mitigate and recover from security incidents efficiently.
- Adroit in conducting threat intelligence analysis to anticipate, prevent, and swiftly respond to cyber threats, fortifying security and minimizing potential attack impacts.

Cybersecurity Offensive Skills - Red Teaming

- Demonstrated proficiency in assessing and exploiting system, network, and application vulnerabilities.
- Knowledge of exploitation tactics, techniques, and procedures attackers use to compromise systems.
- Experience in identifying and addressing security flaws in web applications, including injections and cross-site scripting (XSS).
- Knowledge of digital forensics techniques for investigating security incidents and breaches.

Cybersecurity Tools Proficiency and Other Skills

- **Vulnerability Scanning:** Proficient in vulnerability assessment using tools like Nessus and OpenVAS.
- **Exploitation Frameworks:** Skilled in ethical hacking and penetration testing with tools like Metasploit, Empire, MsfVenom, SET (Social Engineering Toolkit), and BeEF (Browser Exploitation Framework).
- **Information Gathering:** Experienced in passive and active information gathering techniques, Open Source Intelligence (OSINT) practices, and tools such as Maltego and Recon-ng.
- **Digital Forensics:** Proficient in digital forensics tools, including Autopsy, FTK Imager, Volatility, and Wireshark, for evidence collection and analysis.
- **Scripting and Automation:** Competent in scripting and automation using Python, Bash, and PowerShell.

🏆 Certificates

CompTIA CNVP, <i>Network Vulnerability Assessment Professional</i>	2023 Canada
CompTIA Pentest+	2023 Canada
CompTIA Security+	2022 Canada
Cybersecurity, Data Protection and Digital Forensics, <i>Toronto Metropolitan University</i>	2022 Canada

Education

MasterSchool - Cybersecurity Program, Masterschool

2023 – present | United States

A comprehensive program providing advanced knowledge and skills to protect digital assets, mitigate threats, and lead in the evolving field of cybersecurity.

Masters of Business Administration, IMT

2011 | India

Specialization in Finance and Marketing.

Professional Experience

Masterschool, Junior Cyber Support Advisor

2023 – present

- Demonstrated a strong commitment to assisting students in their educational journey.
- Achieved a notable track record of rapid response times, consistently addressing student inquiries in under one minute.

CyberGrover, Founder / Self-Employed

2022 – present

- Operating a successful day trading business, demonstrating expertise in executing trades, analyzing market trends, managing risk, and achieving consistent profitability.
- Integrating day trading bots as a strategic component of business operations, utilizing automated algorithms, advanced market analysis, and risk management techniques to optimize trading outcomes and enhance profitability.

Scotiabank, Senior Financial Advisor / Financial Advisor

2018 – 2022

Industrial Development Bank,

2011 – 2017

Credit Manager / Internal Audit Manager

Projects

Cyber Forensics Investigation with Autopsy, FTK Imager, and Advanced Tools: A Practical Study

- The primary focus involved conducting thorough research and analysis of advanced tools such as Autopsy and FTK Imager, in addition to exploring the methodologies employed by cyber forensic investigators.
- Utilized virtualization technology to run a Kali Linux virtual machine alongside the target, employing tools like NMAP, Exiftool, Dirb, Metasploit, and JohnTheRipper to meet project goals.

Ethical Penetration Testing and Network Security Enhancement

- Conducted ethical penetration testing to replicate real-world attack scenarios, identifying vulnerabilities and potential data exfiltration risks.
- Utilized an array of advanced tools including netdiscover, Hydra, Nikto, Searchsploit, among others, to enhance the effectiveness of the testing process.
- Formulated and implemented robust mitigation strategies to reinforce network security measures, safeguarding sensitive information against potential threats.

Securing E-Commerce: Designing a Resilient LAMP-Based Webstore Architecture

- Designed a secure and scalable online website architecture employing the LAMP stack, guaranteeing the integrity of e-commerce transactions.
- Systematically addressed security aspects, including authentication, authorization, data encryption, and protection against common web vulnerabilities such as SQL injection, SSRF, XXE, and XSS.