Jen Henry

Toronto, Ontario M4E1R3
123-456-7890 | zoomefool@gmail.com GitHub: Jenai87 | Website: www.jenai87.com

Penetration Tester & Cybersecurity Specialist – CSIS

Highlight of Skills

- **Programming:** Python (scripting), C (machine compiled), C++, Java (JIT compiled), PowerShell, Visual Basic, Go, C#, JavaScript
- **Cybersecurity Tools:** Kali Linux, Metasploit, Tenable Nessus, Burp Suite, Wireshark
- **Cybersecurity Skills:** Incident Detection & Response, Malware Analysis, Vulnerability Discovery, Exploit Development, Penetration Testing, Network Security, Hardware/Firmware/Software/Network/RF Vulnerability Assessment, Cloud Security, OWASP Security Principles, CIS Controls, Anti-Tamper
- **IT Knowledge:** Windows, Linux, macOS, Networking (OSI Model), System Administration, CLI (Windows & Unix/Linux), Android & iOS

Work Experience

Cybersecurity Specialist **June 2019 – Present**
CSIS HQ

- Partnered with senior agents and engineers to develop security-focused Python scripts for vulnerability assessments, resulting in a 15% reduction in incident reports.
- Provided support for system administration tasks within Linux and Windows environments, ensuring secure configurations and patch management.
- As an intern in my first year in 2019 conducted initial penetration tests on client applications using Kali Linux, identifying and mitigating critical flaws.

Educational Experience

Juris Doctor (J.D.) (In Progress) **Sep 2021 - May 2026**
University of Toronto, ON

Computer Programming and Analysis Advance Diploma (In Progress) **Sep 2023 - April 2026**
George Brown College, Toronto, ON

Certification, License's & Projects

Embedded Hardware Penetration Testing Framework

- Designed a full-stack toolset using Python and C++ to simulate and execute penetration tests on embedded hardware, incorporating RF vulnerability analysis.
- Leveraged Metasploit for exploit development and Kali Linux for reconnaissance, enabling non-destructive and semi-invasive assessments.

Malware Analysis Simulator

- Built a Python-based simulator using scikit-learn to analyze malware behavior and predict attack vectors, enhancing forensic capabilities.
- Integrated with Tenable Nessus for real-time vulnerability correlation, improving detection accuracy by 18%.

Other: Security Clearance
Active Secret Security Clearance