FIKARA BILAL

●**Blog** ●**Portfolio** ●**LinkedIn** ●**GitHub** ●**Email: fikarabilal@outlook.com**

EDUCATION

Bachelor of Information Technology Engineering| ETS — In progress

DEC in Information Technology | Teccart Institute — 2018-2020

WORK EXPERIENCE

Offensive Security Analyst | Ville De Montreal - Internship — Winter 2025

- **Active scanning and reconnaissance** of office and server infrastructures using **Nmap, Rustscan, Nessus templates, SMBMap, and CrackMapExec** to identify open ports, exposed services, and potential vulnerabilities.
- **Automated report generation** with **Python scripts** to extract, organize, and visualize scan results (**.nessus, XML**) into **Excel** and create detailed **Word reports**.
- **Active Directory assessment** by collecting AD data with **SharpHound** and analyzing it with **BloodHound** and **Neo4j** to visualize relationships. Analysis of network impacts and artifacts generated by **SharpHound**.
- **Creation of Bash scripts** combining multiple tools (**GoWitness, Nuclei**) with **custom YAML files** to automate web scans.
- **Browser plugin security analysis** by analyzing **.crx** files with **ProcMon** to detect network exposures, privilege escalations, and security impacts.
- Implementation of a methodology for scans based on **OWASP WSTG** and **PTES**.

Cybersecurity Integrator| Ville de Montreal - Internship — Winter 2024

- Security incident management with **Trend Micro** and **Microsoft Defender**.
- **SIEM** alert Analysis and wesponse with **QRadar.**
- Task automation with Python scripts and Trend Micro API
- Management of antivirus agent deployments
- Presentation of deployments to the Change Advisory Board (CAB)
- Procedure documentation for effective knowledge transfer (SODOTO)
- Participation in the development of a cybersecurity awareness and training program for employees based on **OWASP TOP 10**.

PROJECT EXPERIENCE

Wazuh: Deployment, Installation, and Alert Configuration

Visiter la page

Complete setup of **Wazuh**, an open-source security management and threat monitoring solution, for a local environment under **Debian**. It includes the following steps:

- Install and configure core components: **server**, **indexer**, and **dashboard**.
- Deploy **Wazuh agents** on **Linux** and **Windows** systems.
- Advanced configuration for **File Integrity Monitoring** (FIM) with rule definition and alert management.

FIKARA BILAL

●**Blog** ●**Portfolio** ●**LinkedIn** ●**GitHub** ●**Email: fikarabilal@outlook.com**

- Integrating **Wazuh** with **ElasticSearch** for data analysis.

Bug Bounty Methodology

Visit the page

This is a structured methodology for vulnerability research, combining reconnaissance, scanning, and exploitation. It can be used in penetration testing, bug bounty, and other contexts. It includes the following steps:

- **Information Gathering**: Use Google Dorking, Bug Bounty Search Engine, GitHub Recon, Censys, and Enum4Linux to identify targets and collect information.
- **Subdomain Search**: Tools used: Crt.sh, Virus Total, Subfinder, Amass, Chaos ProjectDiscovery, Subfinder, and OneForAll.
- **Link Discovery**: Use Katana, GoSpider, and Hakrawler to explore and extract links and other resources.
- **Scanning & Analysis**: Explore ports and services with Naabu, Rustscan, Nmap.
- **Brute Force & Exploitation**: Use Ffuf, Gobuster, Subzy for deeper analysis and vulnerability detection.

TECHNICAL SKILLS

- **Offensive and Defensive Security** : Nmap, Metasploit, Naabu, Rustscan, Subfinder, Gobuster, Amass, Nessus, SharpHound, Wazuh, Microsoft Security Defender
- **Reconnaissance** : Censys, Crt.sh, Assetfinder, Virus Total, Chaos ProjectDiscovery, Ffuf, Subzy
- **Development & Scripting**: Python, Bash, PowerShell, JavaScript, PHP, Java
- **Virtualization & Systems**: VMware, VirtualBox, Linux
- **Data Management**: Power BI, Excel, SQL

CERTIFICATIONS

- **Blog:** Documentation and knowledge sharing on cybersecurity and web. Link here
- **Cisco Networking Academy** : Introduction to Cybersecurity
- **Udemy :** Ethical Hacking
- **Udemy:** Introduction to Cloud Computing on AWS