FIKARA BILAL

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

FORMATION

Baccalauréat en génie des technologies de l'information| ETS — Depuis hiver 2023
Diplôme d'études collégiales en technique de l'informatique| Institut Teccart — 2020

EXPÉRIENCES

Analyste en Sécurité Offensive| Ville De Montréal - Stage — Hiver 2025

- Scan et reconnaissance active des infrastructures bureautiques et serveurs avec **Nmap**, **Rustscan**, des templates **Nessus**, **SMBMap** et **CrackMapExec** pour identifier les ports ouverts, services exposés et configuration vulnérabilités.
- **Automatisation des rapports** avec des scripts **Python** pour extraire, organiser et visualiser les résultats des scans (fichiers **.nessus**, **XML**) dans Excel et générer des rapports Word détaillés.
- **Évaluation de l'Active Directory** par une collecte de données de l'AD avec **SharpHound** et analyse avec **BloodHound** et **Neo4j** visualiser les relations. Évaluation des impacts réseau et artéfacts générés par **SharpHound**.
- Création de **scripts Bash** combinant plusieurs outils, **GoWitness**, **Nuclei** avec des **fichiers YAML** personnalisés pour automatiser les scans web.
- Analyse de sécurité d'un plugin navigateur à travers le fichier **.crx**. Analyse des **scripts de contenus** et des interactions systèmes avec **ProcMon** pour d'éventuelles **expositions réseau**, **élévations de privilèges** et impacts sur la sécurité.
- Mise en place d'une méthodologie pour les balayages en se basant sur **OWASP WSTG** et **PTES**.

Intégrateur Cybersécurité | Ville De Montréal - Stage — Hiver 2024

- Traitement des incidents de sécurité avec **Trend Micro** et **Microsoft Defender**
- Analyse et traitement des alertes du **SIEM** avec **QRadar**
- Automatisation de tâches avec des scripts Python et **APIs Trend Micro**
- Analyse du comportement des antivirus face à un programme (**EICAR**) sur les systèmes
- Présentation des déploiements au comité de changements (CAB / Change-Advisory Board)
- Documentation de procédure permettant un transfert de connaissances efficace (**SODOTO**)
- Participation au développement d'un programme de sensibilisation et de formation des employés en matière de cybersécurité avec le **OWASP TOP 10**

PROJETS TECHNIQUES

Installation Déploiement et Configuration des alertes d'un SIEM Wazuh
Visiter la page
Mise en place complète de **Wazuh**, une solution open-source de gestion de la sécurité et de la surveillance des menaces, pour un environnement local sous **Debian**. Elle inclut les étapes suivantes :

- Installation et configuration des composants principaux : **serveur**, **indexeur**, et **tableau de bord**.
- Déploiement des **agents Wazuh** sur des **systèmes Linux** et **Windows**
- Configuration avancée de la surveillance de l'intégrité des fichiers **File Integrity Monitoring** avec définition de règles spécifiques et gestion des alertes.
- Intégration de **Wazuh** avec **ElasticSearch** pour l'analyse des données

FIKARA BILAL

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

Méthodologie Bug Bounty
Visiter la page
Il s'agit d'une méthodologie structurée pour la recherche de vulnérabilités, combinant **reconnaissance**, **scan** et **exploitation**. Elle peut être utilisée pour un contexte de **test d'intrusion**, de **bug bounty** et autre. Elle inclut les étapes suivantes :

- **Collecte d'informations** : Utilisation de Google Dorking, Bug Bounty Search Engine, GitHub Recon, et Censys, Enum4Linux pour identifier des cibles et collecter le maximum d'informations.
- **Recherche de sous-domaines** : Outils utilisés : Crt.sh, Virus Total, Subfinder, Amass, Chaos ProjectDiscovery, Subfinder et OneForAll
- **Découverte de liens** : Katana, GoSpider et Hakrawler pour explorer et extraire des liens et d'autres ressources.
- **Scan & analyse** : Exploration des ports et services avec Naabu, Rustscan, Nmap.
- **Brute force & exploitation** : Ffuf, Gobuster, Subzy pour approfondir les analyses et détecter des vulnérabilités exploitables.

COMPÉTENCES TECHNIQUES

- **Sécurité Offensive et Défensive** : Nmap, Metasploit, Naabu, Rustscan, Subfinder, Gobuster, Amass, Nessus, SharpHound, Wazuh, Microsoft Security Defender
- **Reconnaissance** : Censys, Crt.sh, Assetfinder, Virus Total, Chaos ProjectDiscovery, Ffuf, Subzy
- **Développement et Scripting** : Python, Bash, Powershell, JavaScript, PHP, Java
- **Virtualisation**: VMware, Virtual Box, Linux
- **Gestion des données** : Power BI, SQL, Excel

CERTIFICATIONS

- **Blog :** Blog Documentation et partage de connaissances sur la sécurité informatique.
- **Cisco Networking Academy**: Introduction to Cybersecurity
- **Udemy :** Hacking Éthique
- **Udemy :** Introduction au Cloud Computing sur AWS