Rapport de Stage en Cybersécurité

Nom de l'étudiant(e) : Mikael Lacroix
Nom de l'entreprise : Ville de Gatineau
Période du stage : 21/04/2025 – 06/06/2025
Nom du superviseur : Sofiène Boulares
Nom de l'enseignant(e) responsable : Christian Kalla

Table des matières – Rapport de Stage en Cybersécurité

Introduction

Présentation de l’entreprise

La Ville de Gatineau est la quatrième plus grande ville du Québec, située en Outaouais, en bordure de la rivière des Outaouais, en face d’Ottawa. Avec une population de plus de 290 000 habitants, Gatineau joue un rôle clé dans la région en offrant des services municipaux essentiels aux citoyens, couvrant notamment les infrastructures, l’urbanisme, les services communautaires, les loisirs, la sécurité publique et les technologies de l'information.

Présentation du service des Technologies de l’Information et de la Cybersécurité

Le service des Technologies de l'information (TI) de la Ville de Gatineau a pour mission de soutenir l’ensemble des services municipaux dans la réalisation de leurs mandats à l’aide de solutions technologiques fiables, sécuritaires et innovantes. Ce service est composé de plusieurs unités, dont une équipe spécialisée en cybersécurité. Cette dernière veille à la protection des systèmes informatiques, des données sensibles, des infrastructures critiques et des communications numériques de la Ville.

Les responsabilités de l'équipe cybersécurité incluent :

- La gestion des politiques de sécurité de l'information.
- La détection et la réponse aux incidents de sécurité.
- La sensibilisation des employés aux risques cybernétiques.
- L’analyse des vulnérabilités et la mise en place de correctifs.
- La surveillance continue des menaces via des outils spécialisés comme les SIEM, antivirus centralisés, pare-feu et systèmes de prévention d’intrusion

Objectifs du stage

Le stage avait pour principal objectif de permettre une immersion professionnelle dans le domaine de la cybersécurité au sein d’une administration publique. Il visait à :

- Développer des compétences techniques en sécurité informatique dans un environnement organisationnel réel.
- Comprendre les enjeux de la cybersécurité dans une structure municipale.
- Contribuer à la protection des actifs informationnels de la Ville.
- Appliquer des notions théoriques à des situations concrètes de sécurité.
- Participer à la mise en place de bonnes pratiques en matière de cybersécurité.
- Se familiariser avec les outils, les politiques et les procédures liés à la gestion de la sécurité de l'information.
- Renforcer les capacités d’analyse, de collaboration et de communication dans un contexte professionnel en cybersécurité.

Tâches réalisées durant le stage

- Réalisation de **scans de vulnérabilités** à l'aide d'outils spécialisés afin d'identifier les failles potentielles dans les systèmes informatiques.
- Élaboration de **plans d'action** pour corriger les vulnérabilités détectées et renforcer la posture de sécurité.
- Participation régulière à des **réunions de l'équipe de cybersécurité** pour le suivi des incidents, la planification des projets et l'analyse des risques.
- Exécution de **tests de pénétration** en mode **black hat** (simulant une attaque externe sans connaissance du système) sans succès et **white hat** (avec autorisation et connaissance des infrastructures) sans succès.
- Contribution à la **documentation des résultats** et aux recommandations à la suite des analyses menées.

Encadrement et Collaboration

Durant le stage, j'ai bénéficié d'un encadrement technique assuré par un membre de l'équipe de cybersécurité de la Ville de Gatineau. Mon superviseur m'a guidé dans la compréhension des processus internes, la maîtrise des outils de sécurité et l'application des bonnes pratiques en cybersécurité. Des suivis réguliers ont permis de valider l'avancement de mon travail, de corriger certaines approches et de m'aider à progresser de manière structurée.

J'ai également eu l'opportunité de collaborer avec les analystes et les administrateurs en sécurité informatique. Cette collaboration s'est traduite par :

- La participation à des réunions techniques pour discuter de vulnérabilités, d'incidents ou de plans d'action.
- Des échanges quotidiens pour résoudre des problématiques spécifiques ou mieux comprendre certaines configurations.
- Une entraide active sur des projets communs, notamment lors des analyses de risques et des tests de sécurité.

Cette expérience m'a permis de développer mes compétences en travail d'équipe dans un environnement professionnel exigeant, tout en consolidant ma compréhension du rôle et de l'importance de la collaboration entre les différents acteurs de la cybersécurité.

Outils, Technologies et Méthodologies Utilisés

Au cours de mon stage, j'ai utilisé une variété d'outils et de technologies spécialisés en cybersécurité, tout en m'appuyant sur des méthodologies reconnues pour réaliser efficacement les missions confiées.

Outils et technologies

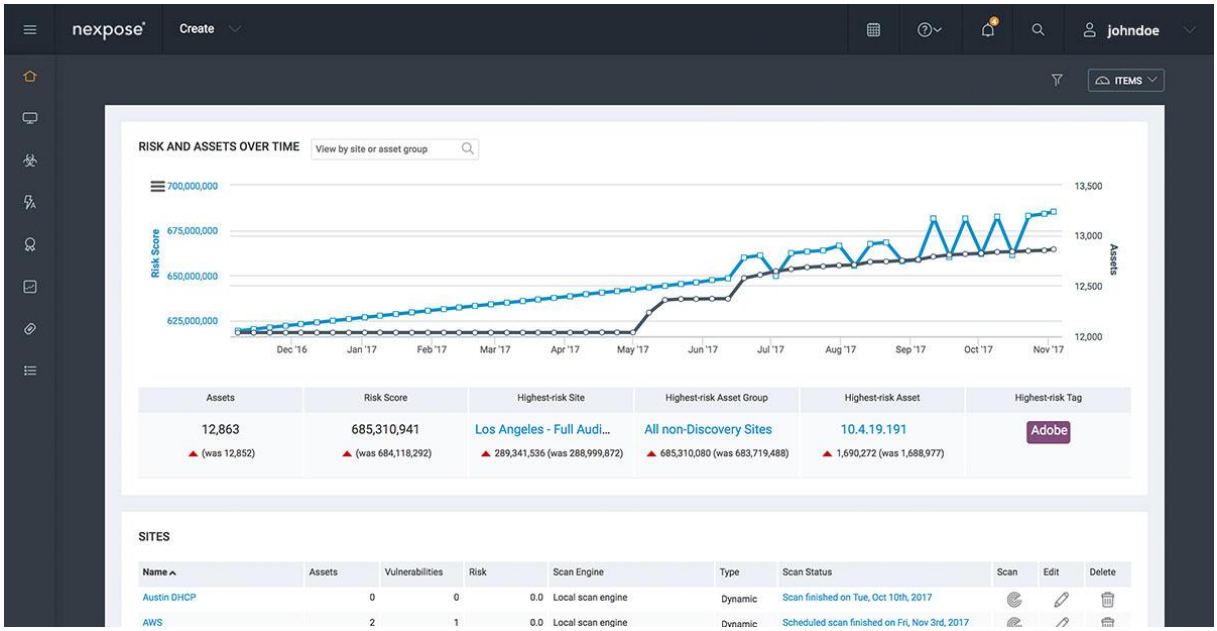
- **Nexpose** (Rapid7) : outil de gestion des vulnérabilités utilisé pour détecter les failles dans les systèmes et générer des rapports d'évaluation des risques.
- **C2 Atom** : plateforme de collaboration et de gestion de projets pour la documentation des actions de sécurité et le suivi des incidents.
- **Kali Linux** : système d'exploitation dédié aux tests d'intrusion, utilisé pour simuler des attaques en mode black hat et white hat.
- **Scripts Python pour le pentesting** : création de scripts personnalisés permettant d'automatiser certaines tâches de tests d'intrusion comme la reconnaissance, le scan de ports ou l'exploitation de vulnérabilités.
- **RDP (Remote Desktop Protocol)** : accès sécurisé à distance pour effectuer des analyses, correctifs ou interventions sur les systèmes cibles.
- **VPN (Virtual Private Network)** : utilisé pour établir des connexions sécurisées au réseau interne depuis l'extérieur.

Méthodologies et normes

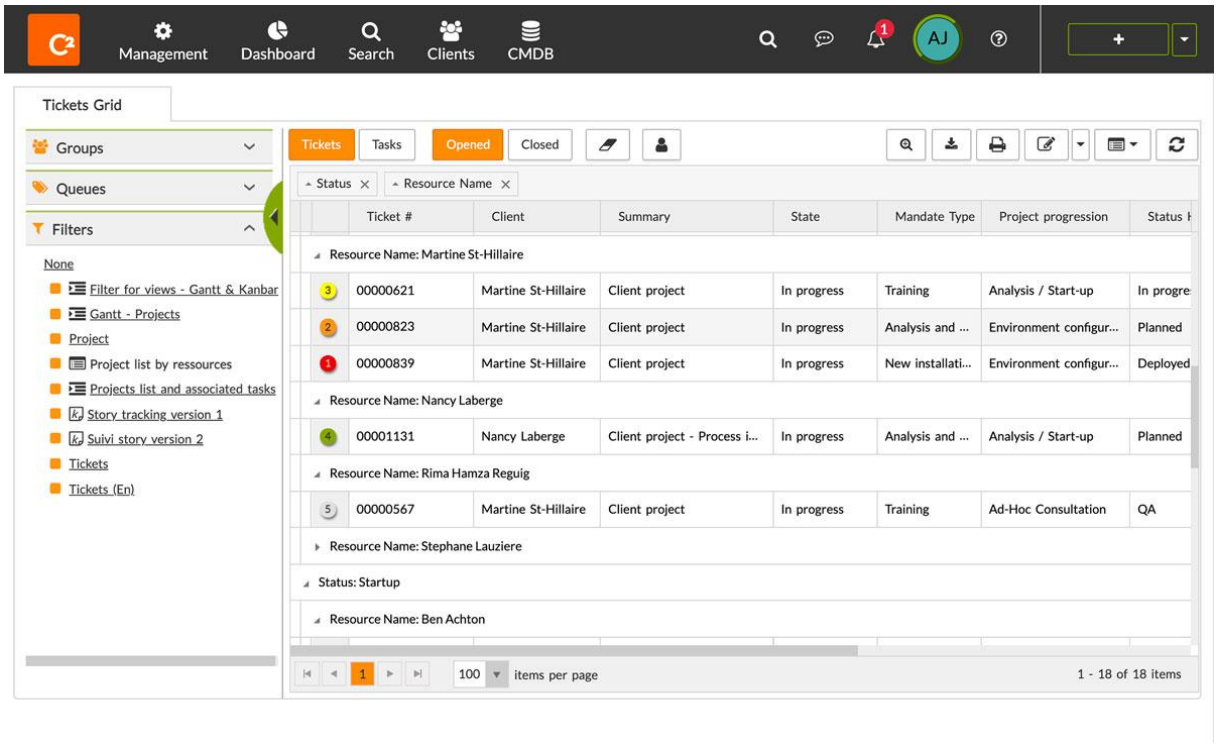
- Réalisation de tests d'intrusion selon les référentiels OWASP (Open Web Application Security Project) et MITRE ATT&CK (cadre tactique des menaces).
- Mise en œuvre d'une gestion des vulnérabilités structurée : détection, analyse, priorisation, documentation et suivi des correctifs.
- Utilisation de la base de données CVE (Common Vulnerabilities and Exposures) pour identifier et évaluer les vulnérabilités connues détectées lors des analyses.

Cette approche m'a permis de développer des compétences pratiques en sécurité informatique tout en respectant les standards de qualité et de rigueur exigés dans un environnement professionnel.

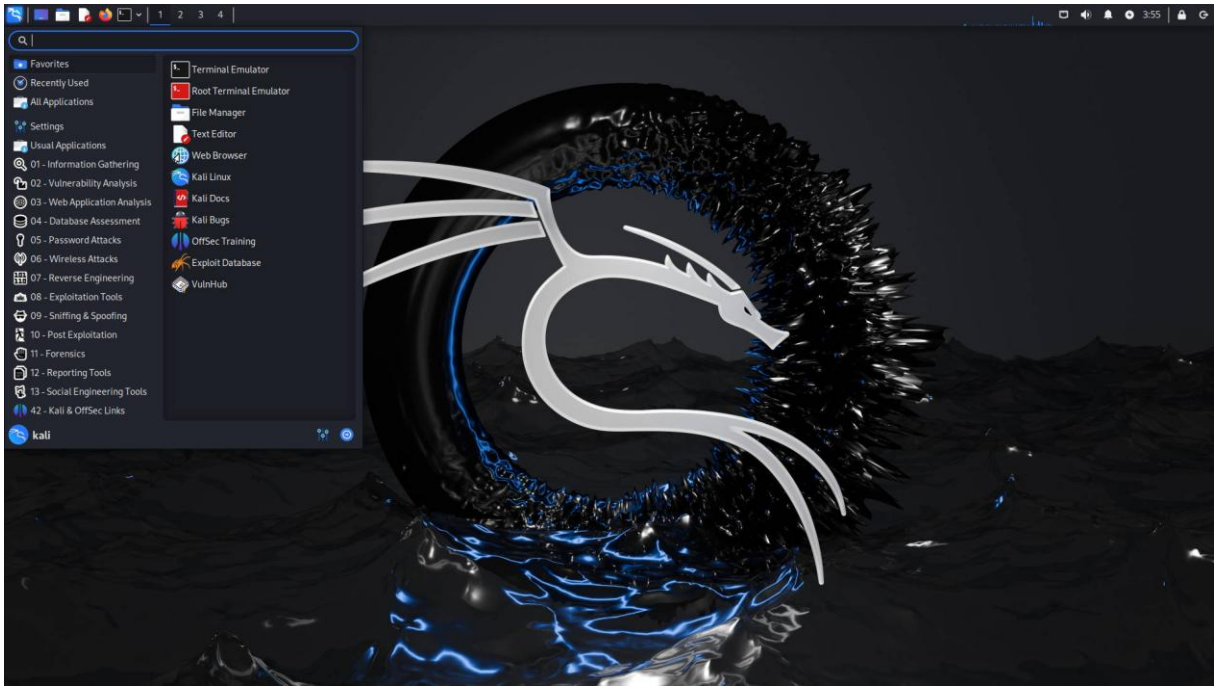
Nexpose :



C2atom :



Kali Linux :



Gestion de la Sécurité Opérationnelle

Dans le cadre de mon stage, j'ai activement participé à différentes activités liées à la gestion de la sécurité opérationnelle de la Ville de Gatineau. Ces activités m'ont permis de comprendre l'importance d'un suivi rigoureux des opérations quotidiennes en cybersécurité et d'assurer la conformité aux politiques internes.

Documentation et procédures internes

J'ai contribué à la **mise à jour de la documentation technique** en lien avec les outils de sécurité utilisés (scanners de vulnérabilités, scripts d'analyse, procédures de tests). Cela incluait la formalisation des étapes d'analyse, les bonnes pratiques à suivre ainsi que la traçabilité des actions entreprises, favorisant ainsi la continuité des opérations et le partage de connaissances au sein de l'équipe.

Réponse aux alertes de sécurité

J'ai pu assister à la **gestion d'alertes de sécurité**, notamment celles générées par les systèmes de détection de vulnérabilités ou d'anomalies. J'ai participé à l'analyse des causes potentielles et à la documentation des actions correctives, en collaboration avec les analystes en sécurité.

Veille et amélioration continue

Enfin, j'ai contribué à la **veille opérationnelle** en matière de cybersécurité, notamment en référençant des menaces émergentes ou des CVE critiques pouvant impacter les systèmes en place. Cette veille s'intégrait aux réflexions sur les mises à jour de procédures ou d'outils.

Lien avec les Cours au Collège

Le stage réalisé à la Ville de Gatineau a été directement en lien avec plusieurs cours suivis dans le cadre de ma formation en cybersécurité. Il m'a permis d'appliquer concrètement les notions théoriques abordées en classe dans un contexte professionnel réel.

SECS1028 – Cycle de vie du piratage éthique

Ce cours m'a fourni une base solide pour comprendre et appliquer les différentes phases d'un test de pénétration, de la reconnaissance à l'exploitation, en passant par la post-exploitation. Durant le stage, j'ai effectué des tests de pénétration en environnement contrôlé, ce qui m'a permis de suivre un cycle similaire à celui enseigné.

SECS1050 – Gouvernance et sécurité

J’ai pu constater l’importance de la gouvernance de la sécurité de l’information à travers l’application de politiques internes, de processus de gestion des vulnérabilités et de conformité aux normes comme ISO 27001. La documentation et les plans d’action de sécurité réalisés pendant le stage sont directement liés à ce domaine.

SECS1025 – Piratage éthique et contre-mesures

Ce cours m’a permis de mieux comprendre les outils et techniques utilisés en piratage éthique, ainsi que les mesures de défense qui y sont associées. Les tâches de pentesting réalisées durant le stage (à l’aide de Kali Linux, scripts Python, etc.) ont illustré concrètement les notions vues en classe.

SECS1030 – Gestion des menaces informatiques

Le stage m’a permis d’identifier, analyser et documenter des vulnérabilités en lien avec des menaces réelles. La veille de sécurité, la réponse aux alertes, et l’évaluation des CVE rencontrées sont des exemples d’activités en lien direct avec la gestion des menaces.

SECS1023 – Cryptographie

Bien que la cryptographie n’ait pas été au cœur de mes missions, j’ai pu observer son rôle dans l’infrastructure globale de sécurité (VPN, certificats, protocoles sécurisés) et comprendre son importance pour la confidentialité et l’intégrité des données.

LEGL1096 – Aspects éthiques et légaux des technologies de l'information et de la cybersécurité

Le respect des règles d’éthique professionnelle, du consentement dans le cadre des tests de sécurité, ainsi que la conformité aux lois et politiques de sécurité internes ont été omniprésents durant mon stage. Ce contexte m’a permis d’intégrer pleinement la dimension légale et morale du travail en cybersécurité.