

Jimmy Ngueguim.



📞 +1 (438) 465-0033
✉️ contact@jimmy-ngueguim.com
🌐 linkedin.com/in/jimmy-ngueguim/
🌐 https://jimmy-ngueguim.com
📍 Montréal, Québec
🇨🇦 Résident Permanent
🚗 🇨🇦 Permis catégorie B (Classe 5)

Fort de cinq années d'expérience en cybersécurité, je suis un professionnel certifié avec un éventail de qualifications prestigieuses. Reconnu pour mon efficacité et mon autonomie, je me distingue également par ma capacité à apprendre rapidement et à m'adapter aux environnements les plus exigeants. Mon expertise couvre les tests d'intrusion, la gestion des vulnérabilités, l'audit de code, la chasse aux menaces, la gestion d'incidents, ainsi que l'évaluation des risques opérationnels. Actuellement, je dirige un projet de recherche en cybersécurité, où je coordonne une équipe de 25 conseillers, démontrant ma capacité à travailler en équipe ainsi qu'à piloter et orchestrer des projets de sécurité complexe.

— DIPLÔMES.

- [2024]- **MAITRISE EN INFORMATIQUE CHEMINEMENT EN CYBERSÉCURITÉ**
Université de Sherbrooke
- [2020]- **DIPLÔME D'INGÉNIEUR SÉCURITÉ INFORMATIQUE**
École Nationale Supérieure Polytechnique de Maroua
 Équivalence du MIFI : Baccalauréat en Génie informatique et de la construction des ordinateurs

— EXPÉRIENCES.

- [03/2023 – NOW ()]- Sr. Conseiller en sécurité offensive
Lead Recherche & Développement en Cybersécurité
- [11/2018 - 03/2023]- Conseiller en sécurité offensive
Product Owner Test d'intrusion

— CERTIFICATIONS.

- [2024]- **PECB - EBIOS Risk Manager**
 ECCPT v2 – Certified Professional Penetration Tester
 OSEP – Offensive Security Experienced Penetration Tester
 CARTP – Certified Azure Red Team Professional
- [2023]- **eWPTXv2** – Web Application Penetration Tester eXtreme
 OSCP – Offensive Security Certified Professional
 CRTP – Certified Red Team Professional
 Certified Splunk Power User
 CRTP – Certified Red Team Professional
- [2022]- **EC-Council** – Mastering Pentesting Using Kali Linux
 EC-Council – Advanced Cryptography Engineering
 EC-Council – Mastering Database Reconnaissance&Exploitation
- [2021]- **NSE 1|2|3** – Fortinet Network Security Expert
- [2020]- Mastering Web and Infrastructure Reconnaissance
 C|EH – (formation) Certified Ethical Hacker
- [2019]- **Acunetix** – Vulnerability Scanner
 Nessus – Vulnerability Scanner
 Metasploit – Exploitation tools
 Burp Suite – Vulnerability Scanner

Sécurité offensive Sécurité défensive Gouvernance Outils & Technologies

— LANGUES.



— COMPÉTENCES ORGA.

- Leadership Exécutif : Gestion d'équipes pluridisciplinaires, Développement des talents, Résolution de conflits.
- Gestion de Projet en Sécurité Offensive: Planification et exécution de campagnes de tests d'intrusion, Gestion des ressources techniques et humaines, Coordination avec les équipes et parties prenantes.
- Relation Client : Développement et gestion des relations, Satisfaction client, Personnalisation des services
- Innovation en Sécurité Offensive : Conception de nouvelles techniques d'attaque et de détection, Recherche et développement en cybersécurité offensive, Intégration des dernières technologies dans les opérations de sécurité offensive.

— COMPÉTENCES TECHNIQUES.

♦ SECURITE INFORMATIQUE

- Évaluation de vulnérabilités: Expertise en tests d'intrusion (OSSTMM, OWASP, PTES, MITRE ATT&CK), gestion avancée des vulnérabilités (Nessus, OpenVAS, Qualys), développement d'exploits personnalisés, évaluation des surfaces d'attaque et des vecteurs de compromission.
- Revue de code & Configuration : Analyse statique (SAST) et dynamique (DAST) du code source, audit de configuration (Benchmark CIS, STIG Viewer), renforcement et durcissement des systèmes (Hardening).
- DFIR : Gestion des incidents (NIST SP 800-61), analyse forensique, collecte et préservation des preuves numériques, reverse engineering, analyse de malwares.
- Analyse de risques: Identification, évaluation et priorisation des risques liés à la sécurité informatique. Mise en œuvre de mesures de mitigation basées sur les meilleures pratiques (ISO 27005, EBIOS RM), évaluation de l'impact des vulnérabilités, analyse des menaces et gestion des risques résiduels...
- Automatisation: Développement de scripts d'automatisation (Python, Bash, PHP, Ruby), développement de scripts d'exploitation, analyse comportementale et détection des anomalies.

— COMPÉTENCES TECHNOLOGIQUE.

- ◆ **Évaluation de vulnérabilités** : Burp Suite, OWASP ZAP, Nessus, Qualys, Metasploit, Nmap, Checkmarx, SonarQube, Veracode, AppSpider, Dependency-Check, SQLmap, Bandit, nmap, BloodHound, AzureHound, PowerSploit, Mimikatz, SharpHound...
- ◆ **Gestion de Projet en Sécurité Offensive**: Jira, Lucid.app, Trello, Confluence.
- ◆ **Revue de Code & Configuration** : Checkmarx, Bandit, Veracode,
- ◆ **Analyse forensique**: Autopsy, EnCase, FTK (Forensic Toolkit), Volatility.

— COMPÉTENCES TECHNIQUES.

◆ RESEAUX

- ◆ **Conception et architecture des réseaux**: Création d'architectures réseau sécurisées incluant la segmentation, les VLAN, les VPN, et les pare-feu.
- ◆ **Administration et gestion des réseaux** : Gestion des configurations réseau, surveillance via des outils de gestion réseau (Nagios, Zabbix, SolarWinds).
- ◆ **Sécurité des réseaux** : Déploiement et gestion de systèmes IDS/IPS, analyse du trafic réseau avec des outils comme Wireshark.
- ◆ **Troubleshooting et optimisation des réseaux** : Diagnostic des pannes réseau et optimisation des performances (bande passante, latence, QoS).

◆ DEVELOPPEMENT

- ◆ **Développement sécurisé**: Intégration des pratiques de sécurité dans le cycle de développement, revue de code sécurisée.
- ◆ **Développement web**: Création de sites web et d'APIs sécurisés, gestion des sessions, validation des entrées, protection contre les attaques XSS/CSRF/SQLi/Upload/SSRF/XXE/LFI/RFI/...
- ◆ **Automatisation et scripting**: Développement de scripts en Python, Bash, PowerShell pour l'automatisation des tâches de sécurité et d'administration, création d'outils personnalisés..
- ◆ **Développement de logiciels**: Expertise en langages de programmation comme C/C++, Python, JavaScript, php, gestion des versions avec Git.
- ◆ **DevOps/CI/CD**: Mise en place de pipelines CI/CD sécurisés, utilisation de l'Infrastructure as Code (IaC) avec Artifactory, Ansible, ou CloudFormation...

◆ TESTS DE SECURITE SPECIFIQUE

- ◆ **Tests sur les API**: Évaluation de la sécurité des API REST et SOAP, en mettant l'accent sur l'authentification, l'autorisation, et la gestion des données sensibles.
- ◆ **Tests de sécurité SWIFT CSP**: Analyse de la conformité aux exigences de la Customer Security Programme (CSP) de SWIFT, incluant la vérification des contrôles de sécurité dans les environnements financiers.
- ◆ **Tests sur SCADA/OT/IoT**: Évaluation de la sécurité des systèmes SCADA et des environnements OT/IoT, avec un focus sur la détection des vulnérabilités dans les protocoles industriels et les dispositifs connectés.
- ◆ **Tests de sécurité Wi-Fi**: Réalisation d'audits de sécurité Wi-Fi, incluant l'évaluation des configurations de chiffrement, la détection des réseaux non autorisés, et l'analyse des attaques par déni de service (DoS).
- ◆ **Tests de sécurité RFID**: Évaluation des systèmes RFID pour détecter des vulnérabilités liées à l'interception, la modification ou la duplication des communications RFID, ainsi qu'à la sécurité physique des étiquettes.

— EXPÉRIENCES PROFESSIONNELLES.

No	1	Entreprise	Levio Inc	Lieu	Montréal, Canada
Rôle	Sr. Conseiller en sécurité offensive			Période	Mars. 2023 - Encours

Levio est une société de conseil en affaires et en technologies qui propose une gamme complète de services pour accompagner votre transformation numérique. Mes attributions chez Levio consistent principalement à réaliser des mandats au forfait ou en régie pour nos clients. De plus, dans le cadre des efforts de Levio visant à répondre aux exigences de la certification ISO 27001, je suis mandaté en interne pour réaliser les tests d'intrusion mensuels sur les assets de Levio et de ses filiales. En outre, je suis le responsable d'un projet de recherche où je coordonne les activités d'une équipe de 25 conseillers impliqués dans la recherche et le développement.

RÔLE ET RESPONSABILITÉS :

- **Réalisation de missions au forfait et en régie pour les clients, comprenant :**
 - o Tests d'intrusion sur divers périmètres : applications web, API, mobile, réseaux Wi-Fi, réseau interne, et environnements cloud.
 - o Audits de sécurité approfondis.
 - o Campagnes de phishing et sensibilisation à la sécurité.
- **Planification, coordination et gestion des tests d'intrusion mensuels sur les actifs de Levio et de ses filiales, incluant :**
 - o Exploration non intrusive d'adresses IP pour identifier de nouveaux hôtes actifs ou inactifs à inclure ou exclure du périmètre des tests mensuels.
 - o Exécution des tests d'intrusion sur les périmètres interne (réseau local, Wi-Fi, postes de travail) et externe (applications métier).
 - o Gestion des vulnérabilités identifiées durant les tests, avec suivi des correctifs et recommandations pour atténuer les risques.
- **Responsabilité de la gestion d'un projet de recherche, où je coordonne les activités d'une équipe de 25 conseillers impliqués dans la recherche et le développement.**



No	2	Entreprise	Sous-traitance industrielle Québec (STIQ)	Lieu	Montréal, Canada
Rôle	Conseiller en cybersécurité			Période	Aout. 2023 - Dece. 2023

STIQ est une association représentant divers secteurs d'entreprises industrielles québécoises. Sa mission est de favoriser le développement des relations d'affaires et d'accroître la compétitivité des entreprises manufacturières afin de stimuler la croissance économique au Québec. Pour atteindre ses objectifs ainsi que ceux de ses clients, STIQ dispose d'une gamme d'applications métier permettant de simplifier les opérations et de coordonner l'ensemble de ses processus. J'ai été chargé d'effectuer des tests d'intrusion sur les applications web InfoStiq+, InfoStiq, Stiq, Podium et de réaliser un audit de sécurité sur l'environnement O365 du STIQ. L'objectif de cette mission est de garantir la sécurité et l'intégrité des systèmes informatiques de STIQ, ainsi que de renforcer leur protection contre les menaces potentielles, conformément aux normes de sécurité.

RÔLE ET RESPONSABILITÉS :

- Exécution de tests manuels et automatisés sur des cibles variées.
- Analyse des vulnérabilités liées à la logique de l'application.
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.
- Révision et documentation des vulnérabilités majeures, avec la rédaction de fiches techniques détaillées.
- Coordination de réunions de travail avec les hauts responsables sécurité du STIQ pour présenter les fiches techniques sur les vulnérabilités critiques et évaluer le niveau de risque.
- Élaboration d'un rapport exhaustif sur les vulnérabilités détectées, incluant des démonstrations concrètes pour les équipes opérationnelles.
- Préparation d'un rapport de haut niveau sur les tests réalisés, avec une analyse des risques à l'intention des dirigeants.
- Animation d'ateliers de restitution avec les cadres supérieurs pour exposer les vulnérabilités et les risques associés.
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées.
- Élaboration d'un rapport exhaustif d'audit de sécurité conforme aux normes CISA et CIS



No	3	Entreprise	CNESST	Lieu	Montréal, Canada
Rôle	Conseiller en cybersécurité			Période	Dece. 2023 - Févr. 2024

La Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) joue un rôle central dans l'application des lois du travail au Québec, en garantissant les droits et les devoirs des travailleurs et des employeurs. Pour accomplir ses missions, la CNESST dispose d'un environnement interne destiné à son personnel, ainsi que de plusieurs applications web accessibles au public. J'ai été mandaté pour réaliser une évaluation approfondie des vulnérabilités, une analyse des risques, ainsi qu'une évaluation du niveau de résilience de l'infrastructure face aux attaques de type rançongiciels. J'ai également mené des tests d'intrusion sur l'application web LMRST M37. L'objectif de cette mission est d'assurer la sécurité et l'intégrité des systèmes informatiques de la CNESST, tout en renforçant leur capacité à résister aux menaces potentielles, en particulier celles liées aux rançongiciels..

RÔLE ET RESPONSABILITÉS :

- Mise en œuvre d'une simulation d'attaque par rançongiciel sur le périmètre de l'organisation.
- Évaluation de la capacité d'un rançongiciel à contourner les mécanismes de sécurité (antivirus, EDR) et à exécuter des activités malveillantes.
- Analyse de la capacité d'un rançongiciel à élever les privilèges sur un poste client de la CNESST.
- Évaluation de la propagation potentielle d'un rançongiciel à travers l'ensemble de l'infrastructure de la CNESST.
- Analyse des risques associés aux vulnérabilités identifiées.
- Réalisation d'un test d'intrusion sur l'application LMRSSST M37.
- Tests de vulnérabilités sur la logique de l'application.
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.
- Révision et documentation des vulnérabilités critiques, incluant la rédaction de fiches techniques détaillées.
- Élaboration d'un rapport exhaustif sur les vulnérabilités détectées, avec des démonstrations concrètes pour les équipes opérationnelles.
- Formulation de recommandations détaillées pour atténuer et corriger les vulnérabilités identifiées.

No	4	Entreprise	MIFI	Lieu	Montréal, Canada
Rôle	Conseiller en cybersécurité			Période	Févr. 2024 - Mars. 2024

Le ministère de l'Immigration, de la Francisation et de l'Intégration (MIFI) est l'entité gouvernementale du Québec chargée de la sélection des immigrants, de leur francisation, et de la fourniture des services nécessaires pour faciliter leur intégration dans la société québécoise. Il propose un portail permettant aux utilisateurs du monde entier de soumettre une déclaration d'intérêt pour immigrer au Québec, que ce soit de manière permanente ou temporaire, pour étudier ou travailler. De plus, le MIFI offre un portail dédié aux entreprises pour soumettre des demandes d'accompagnement, de validation de l'offre d'emploi, ainsi que des Études d'impact sur le marché du travail (EIMT) pour les candidats recrutés à l'international, désireux de venir travailler au Québec.

J'ai été mandaté pour réaliser un test d'intrusion sur l'application web PTET du MIFI et pour analyser les risques associés aux vulnérabilités identifiées. L'objectif de cette mission est de garantir la sécurité et l'intégrité de l'application web PTET du MIFI, tout en assurant son alignement avec les directives du gouvernement du Québec et les lois sur la protection des données.

RÔLE ET RESPONSABILITÉS :

- Exécution de tests manuels et automatisés.
- Analyse des vulnérabilités liées à la logique de l'application.
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.
- Révision et documentation des vulnérabilités majeures, avec la rédaction de fiches techniques détaillées.
- Coordination de réunions de travail avec les hauts responsables sécurité du MIFI pour présenter les fiches techniques sur les vulnérabilités critiques et évaluer le niveau de risque.
- Élaboration d'un rapport exhaustif sur les vulnérabilités détectées, incluant des démonstrations concrètes pour les équipes opérationnelles.
- Préparation d'un rapport de haut niveau sur les tests réalisés, avec une analyse des risques à l'intention des dirigeants.
- Animation d'ateliers de restitution avec les cadres supérieurs pour exposer les vulnérabilités et les risques associés.
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées.

No	5	Entreprise	Ministère de la Justice du Québec (MJQ)	Lieu	Montréal, Canada
Rôle	Conseiller en cybersécurité			Période	Mars. 2024 – En cours.

Le ministère de la Justice du Québec (MJQ) a pour mission de promouvoir la confiance des citoyens et de garantir le respect des droits individuels et collectifs en assurant un système de justice accessible, intègre et respectueux de la primauté du droit au Québec. Le MJQ travaille en collaboration avec diverses entités intégrées ou affiliées pour mener à bien ses missions. Dans ce cadre, le MJQ et ses entités associées ont mis en place une gamme de services en ligne accessibles aux utilisateurs pour faciliter leurs interactions avec le ministère.

J'ai été mandaté pour réaliser des tests d'intrusion sur l'ensemble des applications web du ministère de la Justice et pour analyser les risques associés aux vulnérabilités détectées. L'objectif de cette mission est d'assurer la sécurité et l'intégrité des applications web du MJQ et de ses entités affiliées, tout en garantissant leur conformité avec les directives du gouvernement du Québec et les lois sur la protection des données.

RÔLE ET RESPONSABILITÉS :

- Exécution de tests manuels et automatisés sur des cibles variées.
- Analyse des vulnérabilités liées à la logique des applications.
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.
- Révision et documentation des vulnérabilités majeures, avec la rédaction de fiches techniques détaillées.
- Coordination de réunions de travail avec les hauts responsables sécurité du MJQ pour présenter les fiches techniques sur les vulnérabilités critiques et évaluer le niveau de risque.
- Élaboration d'un rapport exhaustif sur les vulnérabilités détectées, incluant des démonstrations concrètes pour les équipes opérationnelles.
- Préparation d'un rapport de haut niveau sur les tests réalisés, avec une analyse des risques à l'intention des dirigeants.



- Animation d'ateliers de restitution avec les cadres supérieurs pour exposer les vulnérabilités et les risques associés.
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées.

No	6	Entreprise	Nimbuz (interne)	Lieu	Yaoundé, Cameroun
Rôle	Conseiller en cybersécurité			Période	Nov. 2018 - Mars. 2023

Nimbuz Cameroun est une entreprise spécialisée dans l'hébergement web, les audits et conseils en sécurité informatique, le développement web, ainsi que le marketing. La société met son expertise au service des administrations et des entreprises publiques et privées pour sécuriser leurs infrastructures, protéger leurs applications et garantir la confidentialité de leurs données. Elle offre une large gamme de services, allant du conseil à la mise en œuvre technique, pour répondre aux besoins spécifiques de ses clients en matière de sécurité informatique.

Mes responsabilités chez Nimbuz incluait principalement la réalisation de mandats au forfait ou en régie pour les clients. J'étais également mandaté en interne pour effectuer des tests d'intrusion mensuels sur les actifs de Nimbuz et de ses filiales. De plus, j'étais responsable d'une équipe de 7 conseillers développeurs, où j'assurais l'intégration de la sécurité dans le cycle de développement des produits destinés aux clients.

RÔLE ET RESPONSABILITÉS :

- Exécution de tests manuels et automatisés.
- Révision du code pour identifier les vulnérabilités potentielles dans la logique de l'application.
- Conduite de tests avancés à l'aide d'outils bien connus et de scripts Python développés en interne.
- Organisation d'ateliers de travail avec les développeurs pour promouvoir les meilleures pratiques de l'OWASP Top 10.
- Rédaction d'un rapport détaillé sur les vulnérabilités détectées, incluant des preuves de concept pour les équipes opérationnelles.
- Préparation d'un rapport de test de haut niveau comprenant une analyse des risques pour les cadres supérieurs.
- Proposition détaillée de correctifs pour atténuer et résoudre les vulnérabilités identifiées.
- Assistance aux développeurs dans la correction des vulnérabilités.



No	7	Entreprise	CEIDES	Lieu	Yaoundé, Cameroun
Rôle	Conseiller en cybersécurité			Période	Sept. 2019 - nov. 2019

Le Centre International d'Études Diplomatiques, Économiques et Stratégiques (CEIDES) a pour mission de "dresser des ponts entre le savoir et le pouvoir" en apportant une approche académique rigoureuse à l'analyse des enjeux contemporains, et en menant des recherches et des études pour informer et soutenir les décideurs politiques.

Pour accomplir cette mission, le CEIDES propose une application web métier offrant des services de conseil à ses clients, principalement des entités gouvernementales. J'ai été chargé de réaliser des tests d'intrusion sur cette application web métier et d'analyser les risques liés aux vulnérabilités identifiées. L'objectif principal de cette mission est de garantir la sécurité et l'intégrité des données sensibles des clients du CEIDES.

RÔLE ET RESPONSABILITÉS :

- Exécution de tests manuels et automatisés.
- Analyse des vulnérabilités liées à la logique de l'application.
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.
- Révision et documentation des vulnérabilités majeures, avec la rédaction de fiches techniques détaillées.
- Coordination de réunions de travail avec les hauts responsables sécurité du CEIDES pour présenter les fiches techniques sur les vulnérabilités critiques et évaluer le niveau de risque.
- Élaboration d'un rapport exhaustif sur les vulnérabilités détectées, incluant des démonstrations concrètes pour les équipes opérationnelles.
- Préparation d'un rapport de haut niveau sur les tests réalisés, avec une analyse des risques à l'intention des dirigeants.
- Animation d'ateliers de restitution avec les cadres supérieurs pour exposer les vulnérabilités et les risques associés.
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées.



No	8	Entreprise	UNESCO (Antenne Afrique centrale)	Lieu	Yaounde, Cameroun
Rôle	Conseiller en cybersécurité			Période	Jan. 2020 - Mai. 2021

L'antenne de l'UNESCO à Yaoundé est chargée de superviser la mise en œuvre des orientations stratégiques régionales, tout en répondant aux besoins spécifiques des pays couverts, à savoir l'Angola, le Burundi, le Cameroun, la République centrafricaine, la Guinée équatoriale, Sao Tomé-et-Principe et le Tchad, dans divers domaines relevant de la compétence de l'UNESCO. En 2020, en réponse à la pandémie de COVID-19, l'UNESCO pour l'Afrique centrale a lancé un projet Moodle visant à garantir la continuité des études, en particulier dans les régions reculées, pendant cette crise sanitaire.

J'ai été mandaté pour effectuer des tests d'intrusion sur les applications du projet Moodle de l'UNESCO et pour analyser les risques liés aux vulnérabilités identifiées. L'objectif était de renforcer la sécurité de ces applications et de garantir la protection des données des utilisateurs, assurant ainsi la fiabilité et la continuité de l'enseignement en ligne.



RÔLE ET RESPONSABILITÉS :

- Exécution de tests manuels et automatisés.
- Analyse des vulnérabilités liées à la logique de l'application.
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.
- Révision et documentation des vulnérabilités majeures, avec la rédaction de fiches techniques détaillées.
- Coordination de réunions de travail avec les hauts responsables sécurité du UNESCO pour présenter les fiches techniques sur les vulnérabilités critiques et évaluer le niveau de risque.
- Élaboration d'un rapport exhaustif sur les vulnérabilités détectées, incluant des démonstrations concrètes pour les équipes opérationnelles.
- Préparation d'un rapport de haut niveau sur les tests réalisés, avec une analyse des risques à l'intention des dirigeants.
- Animation d'ateliers de restitution avec les cadres supérieurs pour exposer les vulnérabilités et les risques associés.
- Formulation détaillée de recommandations pour atténuer et corriger les vulnérabilités identifiées.

No	9	Entreprise	MINTOUL	Lieu	Yaoundé, Cameroun
Rôle	Conseiller en cybersécurité			Période	Févr. 2022 - Nove. 2022

Le ministère du Tourisme et des Loisirs (MINTOUL) a pour mission de promouvoir le tourisme et les loisirs au Cameroun. Pour accomplir ses objectifs, le MINTOUL dispose d'un ensemble d'applications visant à promouvoir l'image du Cameroun à l'international, ainsi que d'applications métiers permettant de coordonner l'ensemble de ses services disponibles dans les ambassades à travers le monde. En outre, le ministère bénéficie d'un réseau interne et d'une gamme de services informatiques utilisés par ses employés sur site.

J'ai été mandaté pour réaliser des tests d'intrusion sur l'ensemble des applications web du MINTOUL, y compris l'environnement interne, les serveurs et les postes clients. L'objectif de cette mission était de renforcer la sécurité de l'infrastructure informatique du ministère, en identifiant et corrigeant les vulnérabilités potentielles, afin de protéger les données sensibles et de garantir le bon fonctionnement des systèmes.

RÔLE ET RESPONSABILITÉS :

- Tests d'intrusion web et infrastructure.
- Exécution de tests manuels et automatisés sur les cibles identifiées.
- Évaluation des vulnérabilités liées à la logique de l'application.
- Réalisation de tests avancés en utilisant des outils de référence et des scripts Python développés en interne.
- Vérification des vulnérabilités en se basant sur l'OWASP Top 10.
- Révision et documentation des vulnérabilités présentant des risques majeurs, accompagnée de la rédaction de fiches techniques détaillées.
- Coordination de réunions avec les hauts responsables sécurité du MINTOUL pour présenter les fiches techniques et évaluer le niveau de risque.
- Élaboration d'un rapport exhaustif sur les vulnérabilités détectées, avec des démonstrations concrètes pour les équipes opérationnelles.
- Préparation d'un rapport de haut niveau destiné aux dirigeants, comprenant une analyse des risques identifiés.
- Animation d'un atelier de restitution avec les cadres supérieurs pour exposer les vulnérabilités détectées et les risques associés.
- Formulation de recommandations détaillées pour atténuer et corriger les vulnérabilités identifiées.

No	10	Entreprise	Université afro-américaine d'Afrique centrale	Lieu	Yaounde, Cameroun
Rôle	Conseiller en cybersécurité			Période	Jan. 2023 – Mars. 2023

L'Université Afro-Américaine de l'Afrique Centrale (UAAC) est une institution autonome de droit public, dédiée à l'éducation, à la science, et à la recherche. Pour assurer la qualité de ses services, l'UAAC s'appuie sur plusieurs applications web, dont une plateforme Moodle et un système de gestion des étudiants et du personnel.

J'ai été mandaté pour réaliser des tests d'intrusion sur l'ensemble des applications web de l'UAAC et pour analyser les risques liés aux vulnérabilités détectées. L'objectif de cette mission est d'assurer la sécurité et l'intégrité des applications web de l'UAAC, en protégeant les données sensibles et en renforçant la résilience des systèmes face aux menaces potentielles.

RÔLE ET RESPONSABILITÉS :

- Exécution de tests manuels et automatisés.
- Analyse des vulnérabilités liées à la logique de l'application.
- Conduite de tests avancés à l'aide d'outils spécialisés et de scripts Python développés en interne.
- Révision et documentation des vulnérabilités majeures, avec la rédaction de fiches techniques.
- Coordination de réunions de travail avec les hauts responsables sécurité de l'UAAC pour présenter les fiches techniques sur les vulnérabilités critiques et évaluer le niveau de risque.
- Élaboration d'un rapport exhaustif sur les vulnérabilités détectées, incluant des démonstrations concrètes pour les équipes opérationnelles.
- Préparation d'un rapport de haut niveau sur les tests réalisés, avec une analyse des risques à l'intention des dirigeants.
- Animation d'ateliers de restitution avec les cadres supérieurs pour exposer les vulnérabilités et les risques associés.

