

□ Formation certifiante PSI : Pentest et Sécurité des Infrastructures - niveau II

Vers une cybersécurité souveraine et résiliente au Cameroun

La formation PSI (Pentest et Sécurité des Infrastructures) ne se limite pas à une simple acquisition de compétences techniques. Elle incarne une vision stratégique et humaniste pour le Cameroun : celle de bâtir une souveraineté numérique en formant une nouvelle génération d'experts capables de protéger les infrastructures critiques, de répondre aux cybermenaces avec agilité, et de renforcer la résilience des organisations locales. Pour y parvenir, elle s'appuie sur des ressources pédagogiques souveraines (DokuWiki, Debian 12, outils open-source) et des environnements matériels adaptés aux contraintes locales, offrant ainsi une réponse concrète aux défis de la cybersécurité dans un pays où les enjeux sont à la fois technologiques, économiques et géopolitiques.

Intégrant les principes de la pédagogie ignatienne, cette formation va au-delà de la simple transmission de savoirs. Elle mise sur une approche holistique qui allie expérience concrète, réflexion critique et engagement éthique. En effet, chaque module est conçu pour que les apprenants expérimentent (via des labs, CTF et projets réalistes), relisent leurs actions (en analysant les impacts techniques, humains et sociaux), et discernent les meilleures pratiques pour agir de manière responsable. Cette méthode, inspirée des valeurs jésuites, permet de former des professionnels non seulement compétents, mais aussi conscients de leur rôle dans la protection des données et des infrastructures nationales.

En formant des experts autonomes, éthiques et innovants, cette initiative participe à la construction d'un écosystème cybersécurité camerounais robuste, moins dépendant des solutions étrangères, et mieux armé pour faire face aux menaces actuelles et futures. Ainsi, chaque apprenant devient un maillon essentiel dans la chaîne de sécurité numérique du pays, contribuant à un avenir où le Cameroun maîtrise pleinement sa souveraineté technologique et sa résilience face aux cyberrisques.

Durée totale : 35 semaines pour le socle de base (1400 heures)

Volume horaire : 40 h / semaine

□ Module 1 : Analyse des menaces et gestion des risques

Compétence visée

Comprendre l'écosystème de la cybersécurité, identifier les différents acteurs et vecteurs d'attaque, et maîtriser les méthodologies d'analyse de risques afin de concevoir des stratégies de sécurisation adaptées aux infrastructures des organisations locales.

Durée : 108h

Sous-module 1.1 : Panorama des menaces et acteurs

Ce sous-module permet d'appréhender le paysage mondial et local des cybermenaces, ainsi que la

typologie des attaquants.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
1.1.1	Comprendre l'écosystème de la cybersécurité	Séance 1 : Cartographie des acteurs de la menace (cybercriminalité, étatiques, hacktivistes). Séance 2 : Enjeux géopolitiques et économiques de la cybersécurité au Cameroun.	Cours interactif + études de cas.	Participation active.	12h
1.1.2	Identifier les vecteurs d'attaque	Séance 3 : Analyse des principaux modes opératoires. Séance 4 : Étude de la chaîne d'attaque (Cyber Kill Chain).	Analyse de rapports de cybermenaces.	QCM de validation.	16h

Sous-module 1.2 : Méthodologies d'analyse de risques

Ce sous-module apporte les outils normatifs et méthodologiques pour quantifier, qualifier et traiter les risques pesant sur un système d'information.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
1.2.1	Maîtriser EBIOS Risk Manager	Séance 1 : Les 5 ateliers de la méthode EBIOS RM. Séance 2 : Identification des socles, événements redoutés et scénarios de menace.	Travail dirigé sur un scénario type.	Exercice pratique noté.	12h
1.2.2	Appliquer ISO 27001/27005	Séance 3 : Principes fondamentaux du SMSI (ISO 27001). Séance 4 : Processus de gestion des risques selon l'ISO 27005. Séance 5 : Définition des mesures de traitement du risque.	Étude comparative et ateliers pratiques.	Soutenance d'une mini-analyse.	20h

Projet Intégrateur 1

Le projet met en pratique l'ensemble des compétences d'analyse stratégique acquises durant le module.

- **Mission** : Réaliser un **Audit de sécurité et une analyse de risques complète pour une PME fictive** camerounaise.
- **Livrables** :

1. Cartographie des actifs et des menaces potentielles.
 2. Rapport d'analyse de risques complet (EBIOS RM / ISO 27005).
 3. Plan de traitement des risques et politique de sécurité recommandée.
- **Outils** : DokuWiki, matrices d'analyse de risques.
 - **Durée** : 48h

□ Module 2 : Reconnaissance et collecte d'informations

Compétence visée

Maîtriser les méthodologies de collecte d'informations en sources ouvertes (OSINT) et les techniques de balayage réseau actif afin de cartographier de manière exhaustive la surface d'attaque d'une infrastructure cible.

Durée : 124h

Sous-module 2.1 : OSINT (Open Source Intelligence)

Ce sous-module enseigne l'art de collecter des informations publiques exploitables sur une cible sans interagir directement avec son infrastructure.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
2.1.1	Maîtriser les outils OSINT	Séance 1 : Recherche avancée (Google Dorking), utilisation de Shodan, Censys. Séance 2 : Collecte d'informations sur les noms de domaine (DNS, WHOIS, sous-domaines).	Lab de recherche guidée.	Exercices de collecte de données.	16h
2.1.2	Analyser les résultats	Séance 3 : Tri, corrélation et structuration des données récoltées. Séance 4 : Identification des fuites d'informations et des métadonnées compromettantes.	Atelier de relecture critique des données.	Rapport de synthèse OSINT.	16h

Sous-module 2.2 : Scanning et cartographie réseau

Ce sous-module permet d'interagir techniquement avec la cible pour identifier les machines actives, les ports ouverts et les services en écoute.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
2.2.1	Utiliser Nmap et Masscan	Séance 1 : Techniques de scan (TCP SYN, UDP, Connect, Idle scan). Séance 2 : Scripts Nmap (NSE) pour la détection avancée et scans de masse avec Masscan.	Lab réseau sur des cibles contrôlées.	Validation des flags de capture.	16h
2.2.2	Analyser les vulnérabilités	Séance 3 : Association des bannières de services à des vulnérabilités connues (CVE). Séance 4 : Utilisation de scanners automatisés et analyse critique des faux positifs.	Lab pratique.	Rapport de scan technique.	12h

Projet Intégrateur 2

Le projet valide la capacité à dresser un état des lieux complet de la surface d'exposition d'une organisation.

- **Mission** : Mener une **Campagne de reconnaissance sur une infrastructure fictive** complexe sans déclencher les alertes majeures.
- **Livrables** :
 1. Rapport d'OSINT (expositions web, fuites documentaires).
 2. Cartographie réseau détaillée (adresses IP, ports, systèmes d'exploitation, versions des services).
 3. Tableau de synthèse des vulnérabilités potentielles identifiées.
- **Outils** : Nmap, Masscan, Shodan, Maltego, Debian 12 / Kali Linux.
- **Durée** : 64h

Module 3 : Exploitation des vulnérabilités

Compétence visée

Comprendre les mécanismes techniques d'exploitation des failles applicatives et systèmes, utiliser de manière professionnelle les frameworks de pénétration et valider l'existence réelle d'un risque par la preuve (PoC).

Durée : 140h

Sous-module 3.1 : Exploitation avec Metasploit

Ce sous-module est dédié à la prise en main du framework de référence pour l'automatisation et la personnalisation de l'exploitation de failles.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
3.1.1	Prise en main de Metasploit	Séance 1 : Architecture du framework (modules, payloads, listeners). Séance 2 : Recherche, sélection et configuration d'un exploit.	Lab guidé sur machines vulnérables.	Exercices d'exploitation de base.	16h
3.1.2	Exploitation avancée	Séance 3 : Utilisation de payloads complexes (Meterpreter). Séance 4 : Post-exploitation initiale (collecte de hashes, exploration système).	Lab pratique d'exploitation système.	Obtention d'un accès Meterpreter stable.	12h

Sous-module 3.2 : Vulnérabilités web et systèmes

Ce sous-module permet d'analyser et d'exploiter les vulnérabilités classiques affectant les serveurs et les services applicatifs.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
3.2.1	Exploiter des failles web	Séance 1 : Exploitation des failles logiques simples (inclusions de fichiers LFI/RFI, injections de commandes de base).	Démonstration et pratique sur lab web.	Validation d'exercices dédiés (CTF).	20h
3.2.2	Exploiter des failles systèmes	Séance 2 : Exploitation de services réseau obsolètes (SMB, FTP, SSH). Séance 3 : Compréhension des mécanismes de compromission de serveurs Linux et Windows.	Lab d'exploitation de services.	Compromission réussie du serveur cible.	20h

Projet Intégrateur 3

Ce projet demande de combiner la reconnaissance et l'exploitation pour mener une attaque multi-cibles.

- **Mission** : Réaliser l'**Exploitation d'une infrastructure vulnérable** composée d'un laboratoire de 3 machines virtuelles interconnectées.
- **Livrables** :
 1. Fiches d'exploitation détaillant chaque faille utilisée (CVE, impact, remédiation).
 2. Preuves de compromission (accès utilisateur ou administrateur matérialisé par des flags).
- **Outils** : Metasploit, Debian 12, environnements de serveurs d'entraînement vulnérables.
- **Durée** : 72h

Module 4 : Tests d'intrusion (Pentest)

Compétence visée

Planifier et exécuter un test d'intrusion complet d'un réseau d'entreprise selon les standards du marché, et maîtriser les techniques de post-exploitation et de contournement pour évaluer la résilience réelle de la cible.

Durée : 180h

Sous-module 4.1 : Méthodologie de Pentest

Ce sous-module enseigne le cadre formel, contractuel et méthodologique qui distingue le hacking éthique professionnel du piratage informatique.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
4.1.1	Planifier un pentest	Séance 1 : Règles d'engagement, périmètre et aspects légaux. Séance 2 : Les référentiels professionnels (PTES, OSSTMM).	Analyse de contrats types de pentest.	Rédaction d'une proposition technique.	24h
4.1.2	Exécuter un pentest	Séance 3 : Déroulement logique (Reconnaissance → Scanning → Exploitation → Rapport). Séance 4 : Gestion du temps et des priorités en cours de mission.	Simulation de scénario réel en temps limité.	Respect de la méthodologie.	16h

Sous-module 4.2 : Post-exploitation et persistance

Ce sous-module aborde les actions menées par un attaquant après la compromission initiale pour étendre ses privilèges et maintenir ses accès.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
4.2.1	Techniques de persistance	Séance 1 : Élévation de privilèges (Linux/Windows). Séance 2 : Configuration d'accès persistants (Cronjobs, services légitimes modifiés, Web shells).	Labs d'élévation et de persistance.	Maintien d'un accès après redémarrage.	20h

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
4.2.2	Évasion des défenses	Séance 3 : Compréhension des mécanismes de détection (Antivirus, pare-feu applicatifs). Séance 4 : Techniques basiques d'obfuscation de scripts et de payloads.	Ateliers techniques pratiques.	Validation du contournement des blocages.	24h

Projet Intégrateur 4

Ce projet constitue l'évaluation majeure de la posture offensive sur une infrastructure d'entreprise réaliste.

- **Mission** : Conduire le **Pentest complet d'un réseau d'entreprise** virtuel composé de 5 machines interconnectées (comprenant serveurs, postes clients et contrôleur de domaine).
- **Livrables** :
 1. Rapport d'audit technique (destiné aux administrateurs réseau).
 2. Synthèse managériale (destinée à la direction générale, vulgarisant les risques et les impacts économiques).
- **Outils** : Kali Linux / Debian 12, outils de post-exploitation, DokuWiki pour la rédaction.
- **Durée** : 96h

□ Module 5 : Sécurité des applications web et APIs

Compétence visée

Identifier, exploiter et corriger les vulnérabilités les plus critiques affectant les applications web et les interfaces de programmation (APIs) en s'appuyant sur le référentiel international OWASP.

Durée : 184h

Sous-module 5.1 : OWASP Top 10

Ce sous-module offre une plongée technique approfondie dans les dix risques de sécurité applicative web les plus critiques.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
5.1.1	Déployer un environnement de test (Lab)	Séance 1 : Installation d'applications web volontairement vulnérables (DVWA, OWASP Juice Shop) sur Debian 12.	Lab de déploiement système.	Environnement de test fonctionnel.	8h

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
5.1.2	Comprendre les vulnérabilités web	Séance 2 : Injections (SQL, NoSQL, Commandes). Séance 3 : Failles d'authentification et de gestion des sessions. Séance 4 : Cross-Site Scripting (XSS) et injections de requêtes (CSRF/SSRF).	Analyse de code et exploitation pratique via Burp Suite.	Résolution des challenges du laboratoire.	64h

Sous-module 5.2 : Tests et sécurisation des APIs

Ce sous-module traite de la sécurité des architectures modernes basées sur les micro-services et les échanges de données programmatiques (REST/GraphQL).

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
5.2.1	Tester les APIs	Séance 1 : Découverte des endpoints, manipulation des requêtes et analyse des mécanismes d'autorisation (OAuth, JWT).	Lab d'analyse avec Postman et Burp Suite.	Capture de flags applicatifs.	16h
5.2.2	Sécuriser une API	Séance 2 : Principes de validation des entrées, implémentation du Rate Limiting et durcissement des configurations serveurs.	Atelier de remédiation et de configuration.	Validation de la disparition des failles.	16h

Projet Intégrateur 5

Le projet met l'apprenant dans une posture de consultant applicatif complet (audit et conseil).

- **Mission** : Réaliser le **Pentest et la sécurisation d'une application web de production** simulée présentant de multiples failles critiques.
- **Livrables** :
 1. Rapport technique détaillé décrivant les vulnérabilités web et API découvertes.
 2. Code corrigé ou guides de configuration serveur (correctifs d'architecture, règles WAF) pour éradiquer les failles.
- **Outils** : Burp Suite Community, Postman, OWASP Amass, serveurs Apache/Nginx.
- **Durée** : 80h

Module 6 : Détection et réponse aux incidents

Compétence visée

Adopter la posture défensive (Blue Team) en configurant des outils de surveillance centralisée, en analysant les traces d'activité pour détecter des attaques complexes et en appliquant une méthodologie rigoureuse de réponse à incident.

Durée : 160h

Sous-module 6.1 : Détection avec SIEM/IDS

Ce sous-module enseigne la mise en œuvre de la visibilité technique nécessaire pour repérer les anomalies et les comportements malveillants sur un réseau.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
6.1.1	Configurer un SIEM	Séance 1 : Architecture de la centralisation des logs (ex : suite Elastic ou Wazuh). Séance 2 : Déploiement d'agents de collecte et configuration de règles de détection (IDS/SIEM).	Lab d'installation et d'interconnexion.	Système de détection opérationnel.	28h
6.1.2	Analyser des logs	Séance 3 : Analyse des journaux système Linux, Windows Event Logs, et logs serveurs Apache/Nginx. Séance 4 : Corrélation d'événements pour reconstruire le scénario d'une attaque.	Analyse de scénarios d'attaque simulés.	Identification précise de la source de l'attaque.	12h

Sous-module 6.2 : Analyse forensique et réponse à incident

Ce sous-module traite des actions techniques urgentes et de l'investigation numérique post-mortem à mener lorsqu'une intrusion est suspectée ou confirmée.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
6.2.1	Outils forensiques	Séance 1 : Collecte de preuves respectant la chaîne de criticité (mémoire vive, artefacts disques, timelines). Séance 2 : Prise en main d'outils d'investigation numérique ouverts.	Exercice pratique sur image disque compromise.	Extraction des artefacts malveillants.	28h

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
6.2.2	Réponse à incident	Séance 3 : Les étapes de la gestion d'incident (Confinement, Éradication, Recouvrement). Séance 4 : Rédaction des fiches de suivi d'incident et communication de crise.	Simulation de gestion d'une crise cyber.	Plan d'action de remédiation validé.	12h

Projet Intégrateur 6

Ce projet place les apprenants face à une situation d'urgence informatique réaliste.

- **Mission** : Assurer la **Gestion complète d'un incident de sécurité majeur** au sein d'une infrastructure compromise par une équipe offensive.
- **Livrables** :
 1. Rapport d'investigation numérique (Forensics) décrivant le point d'entrée, les actions de l'attaquant et l'étendue des dégâts.
 2. Plan de confinement immédiat et rapport de relecture de l'incident (leçons apprises).
- **Outils** : Solutions SIEM/IDS Open Source, outils forensiques Linux (Volatility, Autopsy), Wireshark.
- **Durée** : 80h

Module 7 : Automatisation et scripting

Compétence visée

Développer des scripts autonomes pour automatiser les tâches d'audit et de surveillance, et intégrer les outils de sécurité au sein des processus de déploiement continu des applications (DevSecOps).

Durée : 104h

Sous-module 7.1 : Scripting pour la sécurité

Ce sous-module permet d'acquérir l'autonomie technique nécessaire pour concevoir ses propres outils d'audit sans dépendre uniquement des logiciels tiers.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
7.1.1	Python pour la sécurité	Séance 1 : Rappels de syntaxe, manipulation des sockets, automatisation de requêtes HTTP. Séance 2 : Écriture d'un scanner de ports sur-mesure ou d'un outil d'analyse de logs personnalisé.	Lab de programmation orientée sécurité.	Script Python fonctionnel et documenté.	16h
7.1.2	Automatisation avec Bash	Séance 3 : Écriture de scripts Shell pour automatiser la collecte d'informations systèmes. Séance 4 : Chaînage d'outils open source existants pour accélérer les audits.	Exercices de scripting système sous Debian 12.	Scripts d'automatisation validés.	12h

Sous-module 7.2 : Intégration DevOps

Ce sous-module démontre comment inclure la sécurité dès les phases amont du développement logiciel (sécurité par conception).

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
7.2.1	Sécurité dans la CI/CD	Séance 1 : Principes des pipelines de déploiement moderne. Séance 2 : Intégration d'outils de tests de sécurité automatisés statiques (SAST) et dynamiques (DAST).	Atelier pratique sur forge logicielle.	Pipeline avec contrôles de sécurité validés.	16h
7.2.2	Automatisation des pentests	Séance 3 : Configuration de lancements programmés d'audits de vulnérabilités applicatives et systèmes. Séance 4 : Génération automatisée de rapports d'alertes techniques.	Lab pratique.	Script de gestion globale d'audits.	12h

Projet Intégrateur 7

Ce projet finalise le volet technique par la création d'une brique logicielle réutilisable.

- **Mission** : Concevoir et coder un **Outil d'automatisation personnalisé pour le pentest ou la détection**.
- **Livrables** :

1. Code source du script proprement structuré, commenté et hébergé localement.
 2. Documentation technique utilisateur intégrée au wiki.
- **Outils** : Python, Bash, Git, Debian 12.
 - **Durée** : 48h

□ Module IS : Ingénierie sociale et manipulation psychologique

Compétence visée

Comprendre les biais cognitifs et les mécanismes de manipulation psychologique utilisés par les attaquants afin de concevoir, d'exécuter de manière éthique et d'évaluer des campagnes de tests de la résilience humaine, tout en mettant en œuvre des stratégies de sensibilisation efficaces.

Durée : 184h

Sous-module IS.1 : Fondamentaux de l'ingénierie sociale

Ce sous-module analyse les théories psychologiques de l'influence et les vulnérabilités comportementales qui font de l'humain la cible principale des cyberattaques.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
IS.1.1	Comprendre les mécanismes psychologiques	Séance 1 : Les principes d'influence sociale (autorité, urgence, rareté, sympathie, réciprocité). Séance 2 : Les biais cognitifs exploités par les cybercriminels.	Cours théorique + analyses de cas de manipulation.	Participation active aux débats.	8h
IS.1.2	Cartographier les vecteurs d'attaque	Séance 3 : Analyse des différentes approches de manipulation (attaque à distance vs attaque de proximité). Séance 4 : Modélisation des profils de cibles au sein de l'organisation.	Atelier de cartographie des risques humains.	Fiche synthétique d'analyse de risques.	12h

Sous-module IS.2 : Techniques d'attaque par ingénierie sociale

Ce sous-module présente les aspects pratiques et les scénarios techniques d'usurpation d'identité et de manipulation à des fins d'intrusion.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
IS.2.1	Maîtriser le phishing	Séance 1 : Conception de scénarios de harponnage (spear-phishing). Séance 2 : Déploiement technique de serveurs de test et configuration de modèles de courriels réalistes.	Lab guidé avec des outils open source.	Configuration réussie de la plateforme.	24h
IS.2.2	Pratiquer le vishing et smishing	Séance 3 : Techniques d'appel téléphonique simulé (vishing) avec prétextes élaborés. Séance 4 : Envoi et mécanismes des attaques par SMS (smishing).	Mises en situation et jeux de rôles encadrés.	Évaluation du réalisme du scénario.	16h
IS.2.3	Exploitation physique	Séance 5 : Techniques d'infiltration de locaux (tailgating, badge oublié, technicien fictif, dépôt de clés USB piégées).	Analyse de scénarios d'intrusion physique.	Rapport de vulnérabilités physiques.	8h

Sous-module IS.3 : OSINT et collecte d'informations

Ce sous-module est ciblé sur la recherche d'informations spécifiques aux individus afin de personnaliser et de crédibiliser les attaques par ingénierie sociale.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
IS.3.1	Exploiter les réseaux sociaux	Séance 1 : Collecte d'informations professionnelles et personnelles en sources ouvertes (LinkedIn, réseaux sociaux publics). Séance 2 : Organigrammes de fait et cartographie des relations internes.	Atelier pratique de recherche OSINT ciblée.	Dossier de profilage d'une cible fictive.	16h
IS.3.2	Analyser les fuites de données	Séance 3 : Recherche d'identifiants et de mots de passe compromis dans les bases de données publiques de fuites (Breach data).	Manipulation d'outils de vérification.	Synthèse des fuites trouvées.	8h

Sous-module IS.4 : Défense et sensibilisation contre l'ingénierie sociale

Ce sous-module apporte les clés pour construire une culture d'entreprise résiliente et transformer les collaborateurs en véritables acteurs de la sécurité numérique.

Séquence	Objectif	Contenu	Méthode pédagogique	Validation	Durée
IS.4.1	Sensibiliser les collaborateurs	Séance 1 : Conception de modules de formation courts, percutants et adaptés au contexte culturel local. Séance 2 : Création de chartes de bonnes pratiques.	Atelier de création de contenus pédagogiques.	Présentation d'un support de sensibilisation.	16h
IS.4.2	Mettre en place des mesures techniques	Séance 3 : Configuration de filtres de messagerie, mécanismes d'authentification forte (MFA) et alertes sur les courriels externes.	Configuration d'un serveur de messagerie sécurisé.	Validation des blocages techniques.	16h
IS.4.3	Tester la résilience humaine	Séance 4 : Indicateurs de performance (KPIs) des campagnes de tests. Séance 5 : Analyse comportementale post-test et processus de remédiation bienveillante.	Étude de tableaux de bord statistiques.	Rapport d'évaluation de la résilience.	20h

Projet Intégrateur 8

Ce projet demande une rigueur éthique et juridique absolue avant toute exécution technique.

- **Mission : Concevoir, cadrer et exécuter une campagne complète d'ingénierie sociale** simulée au sein d'une organisation d'entraînement.
- **Livrables :**
 1. Convention d'éthique et d'autorisation signée (définition stricte des limites).
 2. Scénario détaillé d'attaque multi-canal (Phishing + OSINT).
 3. Rapport d'analyse statistique de la campagne (taux de clic, taux de compromission de données) accompagné du plan de sensibilisation de remédiation proposé.
- **Outils :** Frameworks d'ingénierie sociale open source, outils OSINT, DokuWiki pour la documentation.
- **Durée :** 40h

▣ MODULE EVA : Projet final intégrateur

Compétence visée

Mobiliser l'intégralité des compétences techniques, méthodologiques, éthiques et organisationnelles acquises durant le parcours pour mener à bien une mission de cybersécurité d'envergure professionnelle en équipe, et défendre ses conclusions devant un jury d'experts.

Durée : 40h

Déroulement de l'Évaluation Finale

Cette semaine finale constitue le point culminant du cursus. Elle place les apprenants en situation réelle d'exercice professionnel de haut niveau, simulant l'activité de cabinets d'experts ou de cellules de crise nationales.

- **Format : Mission complète de cybersécurité en équipe - Scénario Red Team vs Blue Team** (Mise en situation sur une infrastructure d'importance vitale reproduisant les défis technologiques et de connectivité réels).
- **Déroulement de la mission :**
 1. **Phase d'action (32h)** : Les équipes doivent simultanément auditer l'infrastructure (approche offensive, détection de failles, exploitation, ingénierie sociale) et mettre en place les mécanismes de surveillance, de détection et de réponse à incident (approche défensive, confinement des attaques, analyse forensique). Une attention particulière est portée à l'utilisation exclusive de ressources open source maîtrisées (Debian 12, DokuWiki, scripts personnalisés).
 2. **Phase de restitution et soutenance (8h)** : Chaque groupe présente ses travaux devant un jury composé de professionnels chevronnés du secteur et de représentants institutionnels.
- **Livrables attendus pour la validation :**
 1. Un **Rapport d'audit et de vulnérabilités exhaustif**, structuré selon les standards internationaux (méthodologies de pentest) mais adapté aux réalités opérationnelles des infrastructures locales.
 2. Un **Cahier de remédiation technique et organisationnelle** détaillé, proposant des solutions concrètes, pérennes, à forte autonomie technologique (sans dépendance logicielle propriétaire coûteuse).
 3. Une **Présentation orale collective** articulée en deux temps : une démonstration technique des points critiques découverts ou défendus, et une synthèse d'aide à la décision stratégique destinée à une direction générale.
- **Critères de réussite** : Rigueur méthodologique, clarté pédagogique de la restitution, viabilité des solutions de sécurité proposées, respect absolu du cadre déontologique et de l'éthique professionnelle du métier.

From:

<https://wiki.bozocinformatique.fr/> - Hack the knowledge, secure the future

Permanent link:

https://wiki.bozocinformatique.fr/presentation_psi:start

Last update: **2026/10/16 17:26**

