ENSEIRB-MATMECA

Module 5 : Intrusion sur les systèmes Windows

École / Prépa
ENSEIRB-MATMECA

En bref

- **Langue(s) d'enseignement:** Français
- **Ouvert aux étudiants en échange:** Non

Présentation

Code interne : EC9IT315

Objectifs

Ce module appartient au bloc de compétences de l'Activité A2 : Audit de sécurité technique

Tâche 1 (A2T1) : Réaliser des audits de sécurité technique, incluant des tests d'intrusion, pour évaluer la sécurité des applications Web, des systèmes d'exploitation (Linux, Windows) et des protocoles réseau.

· A2T1C1 : Identifier, analyser et documenter les vulnérabilités dans les applications, systèmes et réseaux à l'aide d'outils spécifiques.

· A2T1C2 : Exécuter des tests d'intrusion dans des environnements variés (Web, Linux, Windows) tout en respectant les normes et la réglementation en vigueur.

· A2T1C3 : Synthétiser les résultats des audits et tests d'intrusion dans un rapport clair et détaillé, incluant des recommandations pour améliorer la cybersécurité.

Tâche 2 (A2T2) : Participer à la mise en œuvre et au suivi des mesures correctives identifiées lors des audits de sécurité technique.

· A2T2C1 : Prioriser les vulnérabilités et proposer des solutions adaptées en collaboration avec les équipes techniques.

· A2T2C2 : Superviser le déploiement des correctifs et s'assurer de la conformité des systèmes aux standards de sécurité.

· A2T2C3 : Valider l'efficacité des mesures correctives mises en place et communiquer les résultats aux parties prenantes.

Tâche 3 (A2T3) : Concevoir et tester des scénarios d'attaque simulés pour évaluer la résilience des systèmes en conditions réalistes.

· A2T3C1 : Développer des scénarios de simulation réalistes en s'appuyant sur les tactiques, techniques et procédures (TTP) des attaquants.

· A2T3C2 : Simuler des attaques dans des environnements variés et évaluer la capacité de défense de l'infrastructure numérique.

· A2T3C3 : Documenter les résultats des simulations et fournir des recommandations stratégiques pour améliorer la résilience des systèmes.

Tâche 4 (A2T4) : Développer et animer des programmes de formation en cybersécurité

· A2T4C1 : Concevoir des supports pédagogiques adaptés aux différents publics (utilisateurs finaux, équipes techniques, dirigeants).

· A2T4C2 : Animer des sessions de sensibilisation et former les collaborateurs.

· A2T4C3 : Actualiser les contenus de formation grâce à la veille sur les menaces émergentes.

Heures d'enseignement

CI	Cours Intégrés	24h

Syllabus

- Bases théoriques des différents éléments de sécurité de Windows (stockage des mots de passe, protocoles d'authentification, protocoles de résolution de noms)
- Élévation de privilèges locales (contournement de compte utilisateur, Récupération d'informations, extension de la compromission)
- Élévation de privilèges au sein d'un domaine (Rebond, Chemins de contrôle, extraction d'information d'authentification, contournement de restrictions logiciels)
- Élévation de privilèges inter-domaines

Compétences visées

- Capacité d'identification et d'exploitation des vulnérabilités Windows.
- Capacité de faire des recommandations de correction et de remédiation sur les vulnérabilités Windows.
- Capacité de réaliser des développements sécurisés sur windows.

Modalités de contrôle des connaissances

Évaluation initiale / Session principale - Épreuves

Type d'évaluation	Nature de l'épreuve	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'épreuve	Note éliminatoire de l'épreuve	Remarques
Contrôle Continu	Contrôle Continu			1		

Seconde chance / Session de rattrapage - Épreuves

Type d'évaluation	Nature de l'épreuve	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'épreuve	Note éliminatoire de l'épreuve	Remarques
Epreuve terminale	Oral	30		1		sans document