ENSEIRB-MATMECA

# Module 4 : Intrusion sur les systèmes Linux

École / Prépa
ENSEIRB-MATMECA

## En bref

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

# Présentation

**Code interne :** ECI9-MODU4

## Objectifs

L'objectif de ce module est de réaliser des instructions sur les d'infrastructures de type Linux à travers l'exploitations de plusieurs vulnérabilités. Ce module comprend des cas d'utilisations pratiques et réalistes pour réaliser des intrusions discrètes à travers l'exploitation de systèmes et l'élévation de privilèges. Au cours de ce module, la méthodologie et les techniques utilisées seront exposés et détaillés.

## Heures d'enseignement

| | | |
|---|---|---|
| CI | Cours Intégrés | 24h |

## Syllabus

- Fonctionnement d'un environnement Linux (déroulement d'une intrusion, mécanismes d'administration, fonctionnement, authentification, hiérarchie des comptes, mécanismes de sécurité)
- Intrusion en mode anonyme (reconnaissance et méthodologie de cartographie, exploitation, vulnérabilités applicatives, interceptions réseau, cas d'un accès physique à un poste de travail)
- Intrusion en mode authentifié (reconnaissance locale sur un système, élévation de privilèges, rejeu d'informations d'authentification, exploitation de configurations : sudo, tâches planifiées, permissions, etc., exploitation de vulnérabilités publiques, contournement de restrictions logicielles : Sandboxing, Linux Security Module, persistance, gestion de l'empreinte sur le système)

- Exploitation de droits administrateur local (manipulation des ressources locales, extraction des secrets d'authentification, dissection de la mémoire Linux, exploitation d'éléments système live, compromission en profondeur, empoisonnement de services systèmes, empoisonnement de binaires, mise en place de mécanismes de persistance avancéq : rootkits utilisateur, rootkits noyau, portes dérobées, gestion de l'empreinte sur le système, méthodologie de rebond.

## Compétences visées

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

## 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 |