ENSEIRB-MATMECA

Administration Microsoft et Cybersécurité en milieu industriel

École / Prépa
ENSEIRB-MATMECA

Présentation

Code interne : EIN9-SECU5

Description

Ce cours se compose en deux partis :

Parie 1 : Prise en main de l'administration Windows : couvre les bases de la gestion des systèmes d'exploitation Windows, incluant l'installation, la configuration, la maintenance et la sécurité des serveurs et des postes de travail. Elle vise à fournir les compétences nécessaires pour administrer efficacement un environnement Windows, en mettant l'accent sur les meilleures pratiques et les outils essentiels.

Partie 2 : Intrusion en environnement Active Directory : Active Directory représente aujourd'hui la solution de gestion d'un parc informatique la plus utilisée mondialement. Il est de ce fait une cible privilégiée pour les attaquants, et sa compromission un risque majeur pour les entreprises. Comprendre les principaux leviers d'attaque sur ce type d'environnement est ainsi indispensable, aussi bien dans une optique offensive que pour les équipes défensives.

Objectifs

- Comprendre les principes fondamentaux de l'administration des systèmes Windows.
- Apprendre à installer et configurer des serveurs et postes de travail sous Windows.
- Maîtriser les techniques de maintenance et de dépannage courantes.
- Mettre en œuvre des mesures de sécurité pour protéger les systèmes Windows.
- Utiliser les outils et les utilitaires de gestion Windows pour optimiser les performances et la fiabilité du système.
- Mécanismes de base en environnement AD
- Intrusion anonyme
- Mouvement latéral et élévation de privilèges
- Accès privilégiés et post-exploitation

Heures d'enseignement

CI	Cours Intégrés	32h
TI	Travaux Individuels	24h

Syllabus

Introduction
Historique de Windows
Architecture interne
Les éléments clés de Windows
Les applications et le système
TP : Découverte des binaires et des DLLs. Exploiter une faille pour élever les privilèges. Manipulation de la base de registre. Manipulation d'un emplacement de démarrage auto. Manipulation des services. Générer un BSOD
Mécanismes de protection de Windows
TP : Mise à jour de Windows . Signature des binaires et des drivers. Chiffrement de volume. Analyse mémoire. Désinstallation d'un patch
Gestion des comptes locaux
TP : Les privilèges utilisateurs. Attaque du processus lsass.exe . Injection de code à la volée. Modification hors-ligne de la base SAM. Crackage de mot de passe par table Rainbow
TP : Lecture d'un fichier hors ligne. Récupération d'un fichier effacéLe système de fichiers NTFS
Infrastructure Réseau
TP : Création d'un domaine AD. Création d'un utilisateur dans l'AD. Création d'un partage de fichiers. Intégration d'un poste sur l'AD
Les Malwares
TP : Récupérer les mots de passe des applications . Nettoyage d'un ranconware. Process explorer et Virus Total
La 2eme partie introduit la Cybersécurité des systèmes industriels :
Définition des différents types de systèmes industriels.
Composition d'un système industriel
Les langages de programmation d'un PLC
Les protocoles et bus de terrain
Architecture standard et sûreté de fonctionnement

Informations complémentaires

Ce module a est d'une part autour des outils d'administration Microsoft, et dans une perspective plus large, sur la cybersécurité des systèmes industriels.

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 Intégral	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
Projet	Rapport			1		