Sécurité des systèmes et sécurité physique

Composante
ENSEIRB-MATMECA

Présentation

Code interne : EI9RE351

Description

Ce cours introduit les concepts nécessaires à la compensions de la sécurité des systèmes. Il est complété par une introduction à la sécurité physique (ouverture de porte, de cadenas et de verrous).

Syllabus

Introduction au reverse engineering
Introduction
Analyse statique: Premiers pas, Récupération d'informations, Représentation du code
Résultat: Analyse de fonctions, Suivi du flot de données, Bonus
Principes d'exploitation de vulnérabilités
Introduction: Règles du jeu, Vulnérabilités cryptographiques, Vulnérabilités logiques, Manipulation des chaînes de caractères
Attaques: Injections, Corruption mémoire, Programmation sécurisée
OS hardening: La part de l'administrateur, Protections
Sécurité des systèmes Linux
Introduction à la sécurité système: Généralités, Aspects juridiques, Concepts de base, Sécurité du matériel
Sécurité du système: Authentification, Autorisation, Audit
Conteneurs et virtualisation sous Linux
Contexte: De quoi veux-t-on se protéger ? Les mécanismes de protection
Conteneurs vs. Virtualisation: Définitions, Virtualisation:
émulation complète
émulation niveau logiciel (type 2)
émulation niveau hôte (type 1)
Disques durs virtuels
Exemple de vulnérabilité
Conteneurs
Premier pas : chroot()
Mécanismes avancés du noyau Linux

Sandbox
LXC, LibContainer et Docker
Exemple de vulnérabilité
Applications: Malware, Provisioning, Conteneurs, Aide au développement, Cloud, Virtualisation API : LibVirt, Compartimentation,
Contrôle d'accès renforcé : MAC, Modèles de politique de sécurité, Les plus courants : SELinux et AppArmor, Le rebelle : grsecurity
Sécurité des systèmes Windows
Principes généraux de sécurité: Les 3 "A", Structure internes, Comptes et groupes, Contrôle et accès
Mécanismes de sécurité système: Architecture système, Authentification, Stratégies de sécurité, Système de fichiers, Base de registre, Outils
Mécanismes de sécurité réseau: Active Directory, Partage de fichiers, IPSec sous Windows, Pare-feu
Sécurité des applications: Prévention des attaques par overflow
Prévention d'exécution (DEP/NX)
Contrôle des exceptions
PatchGuard
Autres mécanismes
Stratégies de restriction logicielle
Sécurité du boot
Principe de sandboxing (navigateurs)
Extraction et Analyse de malware : du forensics au reverse
"Ecosystème" des malwares: Qui sont les attaquants ? Définitions, Exploitation As A Service : les Exploits Kits, Les défenseurs, Monétisation
Forensics : extraction des malwares, Objectifs, Forensics réseau, Forensics système, Forensics applicatif
Analyse des malwares: Généralités de l'analyse, Outils d'automatisation, Analyse " à la main", Packers, Obscurcissement
Sécurité physique.

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
Epreuve Terminale	Ecrit	80		1		
Projet	Soutenance			0.5		
Projet	Rapport			0.5		

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		