Réf : ET_SEC_TECHA

Techniques de hacking avancées

Exploitation avancée des infrastructures Microsoft Windows

Objectif

L'objectif de ce cours est d'approfondir les techniques essentielles d'attaque sur les systèmes en environnements Microsoft et d'entreprise dans le but d'identifier et de comprendre les moyens de défense à mettre en œuvre.

Public	Prérequis	Durée estimée pour le suivi des modules indispensables
Informaticiens	Des connaissances en système/réseau et sur les environnements Microsoft sont nécessaires. Des notions sur les différentes étapes d'un test d'intrusion sont également conseillées.	Durée des vidéos : 8h45 Durée des TP : 7h00

Contenu pédagogique

Les modules indispensables

Présentation du cours

Cours	Ce module vous propose la consultation d'une vidéo d'une durée de 0h02.
	• Présentation du cours

Préparation des phases d'accès initiales

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 1h27.

- Objectifs
- Introduction et terminologie
- Etude des séquences d'exploitation
- Focus sur les types de charges
- Création de différents types de charges pour l'exploitation
- Déclencher les charges
- Automatiser l'exploitation
- Démonstration - Création et intégration d'une charge (partie 1)
- Démonstration - Création et intégration d'une charge (partie 2)
- Enoncé du TP - Création et exécution d'une charge

Positionnement attaquant externe

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h32.

- Objectifs du module
- Introduction sur les attaques externes
- Social Engineering
- Recherche d'identifiants sur les bases de leaks

Positionnement attaquant interne

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 1h14.

- Objectifs du module
- Introduction sur les attaques internes
- Etude des protocoles d'authentification Microsoft - partie 1
- Etude des protocoles d'authentification Microsoft - partie 2
- LLMNR et NBT-NS Poisoning (relais NTLM)
- Démonstration - Attaque par relay SMB via LLMNR et Netbios
- Enoncé du TP - Attaque Relay SMB via LLMNR et NBT-NS
- Vulnérabilités et exploits communs

Phases de post-exploitation

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 5h03.

- Objectifs du module
- Enumération post-exploitation
- Démonstration - Présentation des outils d'énumération
- Identification des chemins d'attaque (BloodHound)
- Démonstration - Présentation de BloodHound
- Obtention d'identifiants supplémentaires
- Démonstration - Extraction des informations d'identification stockées
- Enoncé du TP - Obtention d'identifiants supplémentaires
- Pivoting
- Démonstration - Pivoting post-compromission
- Enoncé du TP - Pivoting
- Escalade de privilèges verticale
- Démonstration - Service Unquoted et DLL Hijacking
- Enoncé du TP - Escalade de privilèges verticale
- Escalade de privilèges horizontale
- Démonstration - Technique d'escalade de privilèges horizontale
- Enoncé du TP - Escalade de privilèges horizontale
- Zoom sur la sécurité des systèmes industriels

Persistance

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h27.

- Objectifs du module
- Golden Ticket / Silver Ticket
- Skeleton Key / Admin SDHolder
- DC Sync / DCShadow
- DSRM
- Enoncé du TP - Intrusion externe