Réf : ET_SEC_LP2

Lead Pentester

Encadrer un test d'intrusion 2/2

Objectif

Les tests d'intrusion sont devenus incontournables dans le contexte de la Cybersécurité. La réalisation de ces tests fait appel à des compétences techniques dans certains domaines tels que les réseaux Wi-Fi ou le Web.

L'objectif de ce cours est donc de vous transmettre les connaissances techniques de base sur ces domaines, nécessaires voire indispensables pour mener un test d'intrusion.

Public	Prérequis	Durée estimée pour le suivi des modules indispensables
Informaticiens	Des connaissances en systèmes et réseaux sont indispensables pour bien appréhender ce cours.	Durée des vidéos : 8h11 Durée des TP : 5h45

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

Sécurité Wi-Fi

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 2h11.

- Introduction aux réseaux sans fil
- Les principes du 802.11 - partie 1
- Les principes du 802.11 - partie 2
- Démonstration - Analyse de flux avec wireshark
- Contexte de la sécurité Wi-Fi
- Démonstration - Présentation de la suite aircrack-ng
- Démonstration - SSID caché
- Le protocole WEP
- Les protocoles WPA/WPA2
- Le mécanisme d'authentification WPS
- Le protocole WPA3
- Démonstration - Attaque sur le protocole WPA2
- 802.1X
- Architecture Wi-Fi sécurisée
- Démonstration - Chellam

Introduction aux applications web

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 1h05.

- Les composants du web
- Le protocole HTTP(S) - partie 1
- Le protocole HTTP(S) - partie 2
- Présentation de Burp Suite
- Démonstration - Présentation de BurpSuite

Top 10 OWASP 2017

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 3h19.

- OWASP et les injections
- Les injections SQL
- Les autres injections (LDAP, CRLF, de code, Header Spoofing, Xpath)
- Démonstration - Injection SQL manuelle
- Démonstration - Injection SQL automatisée
- Enoncé du TP - Injection SQL
- Faiblesse du système d'authentification
- Démonstration - Bruteforce avec Burp Suite
- Exposition de données sensibles
- Démonstration - Recherche de fichiers sensibles
- Enoncé du TP - Recherche de fichiers sensibles
- XML External Entities (XXE)
- Faiblesse des contrôles d'accès
- Enoncé du TP - Exploitation des faiblesses des contrôles d'accès
- Mauvaise configuration de sécurité
- Cross-Site Scripting (XSS)
- Démonstration - Vol de cookie via XSS
- Enoncé du TP - Exploitation XSS
- Déserialisation non sécurisée
- Composants vulnérables
- Enoncé du TP - Exploitation de composants vulnérables
- Logging et monitoring laxistes

Fuzzing et post-exploitation

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h46.

- Post exploitation web
- Fuzzing web
- Démonstration - Présentation des outils de fuzzing

Analyse et rapport

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h48.

- Mise en perspective des résultats
- Démonstration - Présentation du Scoring framework de pentest ESD
- Rédaction de rapport
- Restitution de livrables exploitable par un CODIR
- Recommandations, plan d'actions et suivi
- Enoncé du TP - Test d'intrusion web