PIRATAGE ÉTHIQUE ET CONTRE-MESURES CODE2UTF('8211',0) NIVEAU INITIATION

CODE STAGE : PECM1

OBJECTIFS

Initiation aux techniques de hacking sur des infrastructures, essentiellement Windows.

DURÉE

5 jours

PUBLIC

Consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur, pentester.

PRÉ-REQUIS

Avoir des compétences en systèmes et réseaux

PROGRAMME

Programme détaillé (par jour)

Jour 1

Section 1 code2utf('8211',0) Contexte actuel

Statistiques récentes
Terminologie
Principes de la sécurité de l'information
Les différentes phases d'une attaque
Définition d'un test d'intrusion
Aspects légaux et réglementaires liés aux tests d'intrusion
Méthodes et framework pour un test d'intrusion

Section 2 code2utf('8211',0) Cadrage et objectifs

Identification des objectifs

Définition du périmètre
TD/ Framework pentest ESD Academy
TP 1/ Questionnaire de pré-engagement
Gestion et affectation des ressources
Suivi des objectifs du test
Règles de pré-engagement (RoE)
TP 2/ Rédaction d'un contrat de pré-engagement

Jour 2

Section 3 : Préparer son test d'intrusion

Préparation d'une machine pour test d'intrusion
Automatisation et scripting
Outils matériel connus
TD/ Rubber Ducky
Templating de documents
TD/ Suivi test d'intrusion

Section 4 code2utf('8211',0) Collecte d'informations

Ingénierie des sources publiques (OSINT)
Relevé passif et actif dcode2utf('8217',0)informations sur l'organisation cible
TD/ Présentation des outils d'OSINT
TP 3/ Relevé d'informations code2utf('038',0) Reconnaissance

Section 5 code2utf('8211',0) Enumération de l'infrastructure

Énumération du périmètre
Evasion sur infrastructure sécurisée
Enumération des protocoles
TD/ Présentations des outils d'énumeration
TP 4/ Enumération de l'infrastructure

Jour 3

Section 6 code2utf('8211',0) Analyse des vulnérabilités

Scan de vulnérabilités
Présentation des différents outils
TD/ Présentation OpenVAS
Les vulnérabilités connues
TP 5/ Identification des vulnérabilités

Section 7 code2utf('8211',0) Exploitation

Recherche d'Exploits
Présentation des outils/frameworks d'attaques
TD/ Présentation metasploit
Déploiement et exécution de charges
TP 6/ Exploitation des vulnérabilités
Écoute passive et active des infrastructures
Bruteforcing

Jour 4 code2utf('038',0) 5

Section 8 code2utf('8211',0) Post-Exploitation

Désactivation des éléments de traçabilité
Élévation de privilèges (Méthodes, outils, vulnérabilités linux, ...)
Etude des persistances (ADS, base de registre, planificateur de tâches, services)
Mouvements latéraux et pivoting
Nettoyage des traces
TP 7/ Post-Exploitation et mouvement lateraux
TP 8 (BONUS)/ Exploitation et analyse des données interceptées

Exemple de travaux pratiques
TD/ Framework pentest ESD Academy
TP 1/ Questionnaire de pré-engagement
TD/ Rubber Ducky
TD/ Suivi test d'intrusion
(voir contenu du programme)

Modalité d'évaluation des acquis

Questions réponses, QCM ou passage examen Badge ESD Academy