PIRATAGE ETHIQUE ET CONTRE-MESURES

Public	Consultants en sécurité, auditeurs en assurance de l'information, programmeurs, testeurs de la sécurité PCI, ainsi que les personnes impliquées dans la mise en œuvre et les mesures de cybersécurité
Durée	4 jours - 28 heures
Pré-requis	Une connaissance des concepts fondamentaux de TCP/IP serait utile.
Objectifs	Dans ce cours vous apprendrez à identifier des faiblesses dans votre réseau en utilisant les mêmes méthodes que les “hackers” : prise d'empreintes, énumération, exploitation et escalade de privilèges. Vous acquerrez les connaissances pour tester et exploiter systématiquement les défenses internes et externes en suivant une méthodologie établie. Les “exploits" seront utilisés pour effectuer ces tâches. Vous apprendrez également les contre-mesures à prendre, telles que les correctifs, pour atténuer les risques encourus par votre entreprise.
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l’éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d’application Mise en place d’ateliers pratiques Remise d’un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d’évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d’accès	L’inscription à cette formation est possible jusqu’à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d’affaires ELITE partenaire d’ACF à 20 m. Guide d’accessibilité à l’accueil.

INTRODUCTION AU PIRATAGE ÉTHIQUE

- Définition d'une méthodologie de tests de pénétration
- Création d'un plan de test de sécurité
- Respect des normes PCI
- Construction d'une « boîte à outils » de piratage

ACQUISITION D'INFORMATIONS SUR LA CIBLE

- Localisation d'informations utiles et pertinentes
- Récupération des données publiées
- Analyse de sites d'archive

SCAN ET ÉNUMÉRATION DES RESSOURCES

- Identification des méthodes d'authentification
- Analyse des pare-feu
- Scans avec HTML et XHP
- Recueil des informations contenues dans les courriels
- Interrogation des services réseau

MISE EN RELATION DES FAIBLESSES ET DES EXPLOITS

- Recherche dans les bases de données
- Détermination de la configuration de la cible
- Outils d'évaluation de vulnérabilité

TIRER PARTI DES POSSIBILITÉS D'ATTAQUE

- Découverte des sources d'exploits
- Attaques avec Metasploit

CONTOURNEMENT DE LISTES DE CONTRÔLE D'ACCÈS (ACL) DE ROUTEURS

- Identification de ports filtrés
- Manipulation de ports pour obtenir l'accès
- Connexion à des services bloqués

COMPROMETTRE DES SYSTÈMES D'EXPLOITATION

- Étude des modes de protection de Windows
- Analyse des processus Linux/UNIX

CORRUPTION D'APPLICATIONS WEB

- Injection de code SQL et HTML, piratage de sessions web par prédiction et cross-site scripting (XSS)
- Contournement des mécanismes d'authentification

APPÂTER ET PIÉGER LES UTILISATEURS INTERNES

- Exécution d'attaques côté client
- Prise de contrôle des navigateurs

MANIPULATION DE CLIENTS INTERNES

- Recueil d'informations client
- Énumération des données internes

DÉPLOYER UNE BOÎTE À OUTILS D'INGÉNIERIE SOCIALE

- Cloner un site légitime
- Détourner l'attention des clients en infectant le DNS
- Délivrer des payloads personnalisés aux utilisateurs

OUTILS DE PRISE EN MAIN À DISTANCE (REMOTE SHELLS)

- Connexion directe ou inversée
- Utilisation de l'outil Meterpreter de Metasploit

ATTAQUE PAR REBONDS

- Attaques de médias portables
- Routage via des clients compromis

VOL D'INFORMATIONS CIBLE

- Mots de passe « hachés »
- Extraction de données de routage, DNS et NETBIOS

TÉLÉCHARGEMENT ET EXÉCUTION DE CHARGES UTILES

- Contrôle des processus de mémoire
- Utilisation du Remote File System (RFS)

DÉGUISEMENT DU TRAFIC RÉSEAU

- Obfuscation de vecteurs et de charges utiles
- Contournement des défenses de périmètre

DÉJOUER LES SYSTÈMES D'ANTIVIRUS

- Falsification d'en-têtes de fichiers pour injecter un malware
- Identification des failles dans la protection antivirus

ATTÉNUATION DES RISQUES ET MESURES À PRENDRE

- Compte rendu des résultats et création d'un plan d'action
- Gestion des correctifs et de la configuration
- Recommandation de contre-mesures de cybersécurité
- Se tenir informé sur les outils, tendances et technologies

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 03/04/2020

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères :
Expérience, pédagogie, dynamisme et prévoyance.