Ethical Hacking

5 jour(s), soit 35 heures

Programme de formation

Public visé
Techniciens et administrateurs systèmes et réseaux, architectes sécurité, intégrateurs sécurité, personnes étudiant la cyber-sécurité, responsables sécurité, auditeurs sécurité

Pré-requis
Connaissances en système et réseaux

Objectifs pédagogiques
Comprendre la méthodologie du hacker
Apprendre le vocabulaire lié au Hacking
Mettre en pratique le cycle de l'attaquant
Rédiger un rapport de pentest

Description / Contenu
Principe et méthodologie du Hacking
- Définition.
- Typologie des attaquants.
- Vocabulaire.
- PTES.
- OWASP.
- OSSTMM.
- Red Team / Blue Team.
- Kill Chain unified.

Préparation audit + rapport
- Contrat.
- Contexte et périmètre.
- Rappels des lois en vigueur.
- La trousse à outil d'un pentesteur.
- Mise en place dans le cloud.
- Comment s'organise un rapport.

Vecteurs d'attaques
- Virus / ver / cheval de troie.
- Backdoor.
- Logiciel espion / Keylogger.
- Exploit.
- Rootkit.
- Ransomware.
- Pourriel / Hameçonnage / Canular informatique.
- Spearphishing.
- Botnet.
- Scanner de réseaux et de failles.

OSINT
- Présentation OSINT.

JCD and CO – 193 RUE DU GENERAL METMAN, 57070 METZ France – 03 87 37 97 70 – formation@jcd-groupe.fr – SIRET : 80187958600031
Déclaration d'activité enregistrée sous le numéro 41570348657 auprès du préfet de région Lorraine

- Méthodologie OSINT.
- Exemples : Google dorks, recherche d'emails, recherche de sous-domaines.

Reconnaissance active et vulnérabilités

- Principe.
- Méthodologie.
- Pratique : Nmap, metasploit, scapy.
- MITRE ATT&CK.
- Scanner de vulnérabilités.
- Social ingénierie.
- CVE.
- Défaut de configuration.

Typologie des attaques

- Exploitation réseau (MITM).
- Social ingénierie / Phishing / Deepfake.
- Server side (Exploit CVE, Cracking + Bruteforce).

Hacking Web & Application Web, attaques avancées

- Principe.
- Méthodologie.
- Typologie d'attaque : Client side, Back side.
- TOP10 OWASP.
- Exploitation de failles.
- Création de Payload.
- Customiser ses exploits.
- Mise en œuvre du Pivoting.
- Exploitation Browser.

Post-exploitation, rapport

- Mise en œuvre de techniques d'exfiltration.
- C&C.
- Les élévations de privilège.
- Effectuer une énumération locale.
- Effacer ses traces.
- Exemple et étude d'un rapport.
- Communication et résultats.

Mise en situation, focus sur des technologies spécifiques

- Pentest d'un lab.
- Rédaction du rapport.
- Hack Wifi.
- Hack Cloud.
- Hack IoT.
- Hack Mobile.

Modalités pédagogiques

10% d'apports théoriques pour 90% de mise en pratique des différentes formes d'attaques

Moyens et supports pédagogiques

Fourniture de documents et supports de cours qui restent la propriété des stagiaires
Salles équipées : vidéoprojecteur, paperboard, ordinateur individuel, support de cours papier ou électronique, outils de prise de notes

Modalités d'évaluation et de suivi

Compte rendu de fin de formation et analyse interne, quizz pour valider les acquis
Questionnaire « évaluation de la formation » rempli par le stagiaire

Validation de stage

Attestation de stage

Profil du formateur
Consultant spécialiste en cybersécurité

Lieu
JCD and CO - 193 RUE DU GENERAL METMAN, 57070 METZ France

Informations sur l'accessibilité
La formation est accessible aux personnes à mobilité réduite et toute demande d’adaptation peut être étudiée en amont de la formation en fonction du besoin des personnes. Nous contacter pour plus d’informations.