EduGroupe
Accompagner pour réussir

Ethical Hacking

Durée : 4 jours (28 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des systèmes d'exploitation Windows et Linux.
- Maîtrise des concepts réseaux (TCP/IP, DNS, routage, services réseau).
- Connaissances de base en cybersécurité.
- Une première expérience en administration système ou réseau est recommandée.

PROFIL DES STAGIAIRES

- Administrateurs systèmes et réseaux
- Administrateurs sécurité
- Analystes SOC
- Ingénieurs cybersécurité
- Consultants en sécurité informatique
- Responsables infrastructures
- Auditeurs techniques
- Toute personne souhaitant acquérir les fondamentaux du pentest et de l'Ethical Hacking.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre la méthodologie d'un test d'intrusion.
- Identifier les principales vulnérabilités d'un système d'information.
- Réaliser des phases de reconnaissance et de collecte d'informations.
- Exploiter des vulnérabilités dans un environnement contrôlé.
- Comprendre les techniques utilisées par les attaquants.
- Évaluer le niveau d'exposition d'une infrastructure.
- Formuler des recommandations de remédiation adaptées.
- Adopter une démarche éthique et conforme aux bonnes pratiques du pentest.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et de démonstrations techniques.
- Travaux pratiques réalisés sur une plateforme de laboratoire dédiée.
- Exercices de reconnaissance, d'analyse et d'exploitation de vulnérabilités.
- Études de cas inspirées de scénarios réels de compromission.
- Mises en situation de type pentest encadré.

- Débriefings techniques et échanges de bonnes pratiques.

FORMATEUR

- Consultant expert en cybersécurité offensive disposant d'une expérience significative dans la réalisation de tests d'intrusion, d'audits techniques, d'évaluations de sécurité et d'accompagnement des organisations dans le renforcement de leur posture cyber.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Validation continue des acquis à travers les travaux pratiques.
- Exercices de reconnaissance, d'analyse et d'exploitation supervisés.
- Quiz de validation des connaissances.
- Cas pratique de synthèse en fin de formation.
- Questionnaire d'évaluation des acquis en fin de parcours.

CONTENU DU COURS

Jour 1 : Introduction au pentest et phase de reconnaissance (7h)

Module 1 : Comprendre l'Ethical Hacking et la méthodologie de pentest (2h)

Objectifs

- Comprendre les principes de l'Ethical Hacking.
- Identifier les différentes phases d'un test d'intrusion.
- Maîtriser le cadre légal et éthique.

Contenu

- Définition de l'Ethical Hacking.
- Typologie des attaquants.
- Cycle de vie d'une attaque.
- Méthodologies de pentest.
- Cadre juridique et responsabilités.
- Présentation des principales normes et référentiels.

Mise en pratique

Brainstorming collectif :

- Analyse d'incidents réels et identification des techniques utilisées par les attaquants.

Module 2 : Collecte d'informations et reconnaissance passive (2h)

Objectifs

- Identifier les informations accessibles publiquement.
- Comprendre les techniques d'OSINT utilisées lors d'un pentest.

Contenu

- Principes de l'OSINT.
- Recherche d'informations sur une organisation.
- Collecte d'informations sur les domaines et sous-domaines.
- Analyse des infrastructures exposées.
- Recherche de données publiques et métadonnées.

Mise en pratique

Atelier pratique :

- Réalisation d'une phase de collecte d'informations sur une cible fictive.

Module 3 : Reconnaissance active et cartographie des systèmes (2h)

Objectifs

- Identifier les services exposés.
- Découvrir les surfaces d'attaque disponibles.

Contenu

- Découverte d'hôtes.
- Scan de ports.
- Identification des services.
- Fingerprinting des systèmes.
- Énumération des ressources accessibles.

Mise en pratique

Travaux pratiques :

- Réalisation d'une cartographie d'un environnement cible.

Module 4 : Atelier de synthèse Reconnaissance (1h)

Objectifs

- Consolider les techniques de collecte d'informations.

Mise en pratique

Cas pratique :

- Élaboration d'une cartographie complète d'une cible avant audit.

Jour 2 : Analyse et exploitation des vulnérabilités (7h)

Module 5 : Identifier les vulnérabilités d'une infrastructure (2h)

Objectifs

- Comprendre les différentes catégories de vulnérabilités.
- Prioriser les risques associés.

Contenu

- Vulnérabilités systèmes.
- Vulnérabilités réseau.
- Vulnérabilités applicatives.
- CVE et scoring CVSS.
- Outils d'analyse de vulnérabilités.

Mise en pratique

Atelier :

- Analyse de rapports de vulnérabilités.

Module 6 : Exploitation des vulnérabilités systèmes et réseaux (3h)

Objectifs

- Comprendre les mécanismes d'exploitation.
- Mesurer l'impact des vulnérabilités non corrigées.

Contenu

- Concepts d'exploitation.
- Exploitation de services vulnérables.
- Failles de configuration.
- Élévation de privilèges.
- Mouvements latéraux.

Mise en pratique

Travaux pratiques encadrés :

- Exploitation de vulnérabilités sur un laboratoire sécurisé.

Module 7 : Post-exploitation et maintien d'accès (1h)

Objectifs

- Comprendre les actions menées après compromission.

Contenu

- Collecte d'informations internes.
- Escalade de privilèges.
- Déplacement latéral.
- Persistance.
- Limites éthiques et légales.

Mise en pratique

Démonstration commentée :

- Analyse d'un scénario post-compromission.

Module 8 : Atelier de synthèse Exploitation (1h)

Objectifs

- Consolider les acquis techniques.

Mise en pratique

Étude de cas :

- Analyse d'une chaîne complète d'attaque.

Jour 3 : Sécurité des applications Web et attaques courantes (7h)

Module 9 : Comprendre les vulnérabilités Web (2h)

Objectifs

- Identifier les principales vulnérabilités applicatives.

Contenu

- Présentation du Top 10 OWASP.
- Injection SQL.
- Cross-Site Scripting (XSS).
- Contrôle d'accès défaillant.
- Gestion des sessions.
- Exposition de données sensibles.

Mise en pratique

Atelier :

- Analyse de vulnérabilités Web courantes.

Module 10 : Exploitation de vulnérabilités applicatives (3h)

Objectifs

- Comprendre les mécanismes d'exploitation Web.
- Évaluer les impacts des failles applicatives.

Contenu

- Techniques d'exploitation.
- Manipulation de paramètres.
- Exploitation d'injections.
- Contournement de contrôles.
- Exfiltration de données.

Mise en pratique

Travaux pratiques :

- Exploitation contrôlée d'applications vulnérables.

Module 11 : Mesures de protection et remédiation (1h)

Objectifs

- Définir les mesures correctives adaptées.

Contenu

- Bonnes pratiques de développement sécurisé.
- Durcissement des applications.
- Gestion des correctifs.
- Contrôles compensatoires.

Mise en pratique

Atelier :

- Élaboration d'un plan de remédiation.

Module 12 : Atelier de synthèse Web (1h)

Objectifs

- Mettre en perspective l'ensemble des vulnérabilités étudiées.

Mise en pratique

Étude de cas :

- Analyse complète d'une application Web vulnérable.

Jour 4 : Réaliser un pentest et restituer les résultats (7h)

Module 13 : Construire une mission de pentest (2h)

Objectifs

- Structurer une mission d'audit de sécurité.

Contenu

- Définition du périmètre.
- Règles d'engagement.
- Préparation des tests.
- Gestion des risques liés à l'audit.
- Collecte des preuves.

Mise en pratique

Atelier :

- Construction d'un plan de mission de pentest.

Module 14 : Rédiger un rapport d'audit efficace (2h)

Objectifs

- Formaliser les résultats d'un audit.
- Produire des recommandations exploitables.

Contenu

- Structure d'un rapport de pentest.
- Présentation des vulnérabilités.
- Évaluation des risques.
- Recommandations de remédiation.
- Communication aux parties prenantes.

Mise en pratique

Travaux pratiques :

- Rédaction d'extraits de rapport à partir d'un audit simulé.

Module 15 : Cas pratique fil rouge : Pentest d'une infrastructure (2h)

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Mise en pratique
Exercice complet :

- Reconnaissance.
- Cartographie.
- Identification des vulnérabilités.
- Exploitation contrôlée.
- Analyse des impacts.
- Recommandations.

Module 16 : Restitution et débriefing (1h)

Objectifs

- Présenter les résultats d'un audit.
- Défendre les recommandations formulées.

Mise en pratique
Présentation orale :

- Restitution des conclusions du pentest devant le groupe.
- Débriefing collectif et retour d'expérience.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.