EC-Council

Certified ethical hacker

CEH

Version : v12
5 jours

Objectifs

Apprendre et maitriser les 5 phases du piratage éthique :

I. Repérage
II. Scannage
III. Obtenir l'accès
IV. Maintien de l'accès
V. Couvrir les traces

A qui s'adresse ce cours ?

- Pirates informatiques,
- Administrateurs de systèmes,
- administrateurs et ingénieurs de réseaux,
- gestionnaires de sites web,
- auditeurs,
- Professionnels de la sécurité en général

Contenu du stage

Jour 1

1. **Introduction au piratage éthique**

   Couvrir les fondamentaux des questions clés dans le monde de la sécurité de l'information, y compris les bases du piratage éthique, les contrôles de la sécurité de l'information, les lois pertinentes et les procédures standard.

2. **Empreinte et reconnaissance**

   Apprendre à utiliser les techniques et les outils les plus récents pour réaliser des impressions et des reconnaissances, une phase critique de pré-attaque éthique. reconnaissance, une phase critique de pré-attaque du processus de piratage éthique. du processus de piratage éthique.

3. **Analyse des réseaux**

   Apprendre les différentes techniques d'analyse de réseau et les contre-mesures.

4. **Enumération**

Apprendre diverses techniques d'énumération, telles que le protocole Border Gateway Border Gateway Protocol (BGP) et Network File Sharing (NFS), et les contre-mesures associées. contre-mesures associées

Jour 2

5. **Analyse des vulnérabilités**

Apprendre à identifier les failles de sécurité dans le réseau, l'infrastructure de communication et les systèmes finaux d'une organisation cible réseau, l'infrastructure de communication et les systèmes finaux d'une organisation cible. Différents types d'évaluation des vulnérabilités et d'outils d'évaluation des vulnérabilités.

6. **Piratage de système**

Découvrir les différentes méthodologies de piratage de systèmes, y compris la stéganographie, les attaques par stéganalyse et la dissimulation de traces, utilisées pour découvrir les secrets d'un système,
stéganographie, les attaques par stéganalyse et la dissimulation de traces - utilisées pour découvrir les vulnérabilités du système et du réseau pour découvrir les vulnérabilités des systèmes et des réseaux.

7. **Menaces liées aux logiciels malveillants**

Apprendre les différents types de logiciels malveillants (chevaux de Troie, virus, vers, etc.), APT et les logiciels malveillants sans fichier, la procédure d'analyse des logiciels malveillants et les contre-mesures.

8. **Reniflage**

Apprendre les techniques de reniflage de paquets et comment les utiliser pour découvrir les vulnérabilités du réseau, ainsi que les contre-mesures pour s'en protéger. découvrir les vulnérabilités du réseau, ainsi que les contre-mesures pour se défendre contre les contre les attaques de reniflage.

Jour 3

9. **Ingénierie sociale**

Apprendre les concepts et les techniques de l'ingénierie sociale, y compris comment d'identifier les tentatives de vol, d'auditer les vulnérabilités humaines et de suggérer des contre-mesures d'ingénierie sociale.

10. **Déni de service**

Découvrir les différentes techniques d'attaque par déni de service (DoS) et par déni de service distribué (DDoS), ainsi que les outils permettant d'auditer une cible et de la protéger. (DDoS), ainsi que les outils utilisés pour auditer une cible et concevoir des contre-mesures et des protections DoS et DDoS. d'auditer une cible et de concevoir des contre-mesures et des protections DoS et DDoS.

11. **Détournement de session**

Apprendre diverses techniques d'énumération, telles que le protocole Border Gateway Border Gateway Protocol (BGP) et Network File Sharing (NFS), et les contre-mesures associées. contre-mesures associées

12. **Déjouer les IDS, les pare-feu et les pots de miel**

Introduction aux techniques de contournement des pare-feux, des systèmes de détection d'intrusion (IDS) et des pots de miel ; les outils utilisés pour auditer le réseau. de détection d'intrusion (IDS) et des pots de miel ; les outils utilisés pour réseau pour détecter les faiblesses et les contre-mesures.

Jour 4

13. **Piratage des serveurs web**

Apprendre les attaques de serveurs web, y compris une méthodologie d'attaque complète méthodologie d'attaque complète utilisée pour auditer les vulnérabilités des infrastructures de serveurs web et les contre-mesures.

14. **Piratage des applications web**

Apprendre les attaques d'applications web, y compris une méthodologie complète de piratage d'applications web méthodologie de piratage d'applications web utilisée pour auditer les vulnérabilités des applications web et les contre-mesures

15. **Injection SQL**

Découvrir les attaques par injection SQL, les techniques d'évasion et les contre-mesures à l'injection SQL et les contre-mesures à l'injection SQL.

16. **Piratage des réseaux sans fil**

Comprendre les différents types de technologies sans fil, y compris cryptage, les menaces, les méthodes de piratage, les outils de piratage, les outils de sécurité Wi-Fi et les contre-mesures et les contre-mesures.

Jour 5

17. **Piratage de plateformes mobiles**

Apprendre les vecteurs d'attaque des plateformes mobiles, le piratage d'Android et d'iOS, la gestion des appareils mobiles, les directives de sécurité mobile et les outils de sécurité. la gestion des appareils mobiles, les directives de sécurité mobile et les outils de sécurité.

18. **Piratage IoT et OT**

Apprendre les différents types d'attaques IoT et OT, la méthodologie de piratage, les outils de piratage et les contre-mesures, outils de piratage et contre-mesures

19. **Cloud Computing (l'informatique en nuage)**

    Apprendre les différents concepts de l'informatique en nuage, tels que les technologies de conteneurs et l'informatique sans serveur, les différentes menaces liées à l'informatique en nuage, les attaques, la méthodologie de piratage et les techniques et outils de sécurité en nuage, méthodologie de piratage, ainsi que les techniques et outils de sécurité du cloud computing.

20. **Cryptographie**

    Découvrir les algorithmes de cryptage, les outils de cryptographie, l'infrastructure à clé publique (PKI), le cryptage des courriels, le cryptage des disques, les attaques et les outils de cryptanalyse.

Prérequis

Test de prérequis

Mode d'évaluation des acquis

L'examen à la fin de la formation. Bon d'examen est fourni par EC-Council. Auto-évaluation chaque jour formalisée sur le Moodle.