Syllabus

Test de Pénétration

CYBERIUM ARENA

— SIMULATOR —

Description
Les testeurs de pénétration font face à une combinaison de systèmes de détection d'intrusion, de protection basée sur l'hôte, de systèmes renforcés et d'analystes qui déversent les données collectées par leurs systèmes de gestion des informations de sécurité.
Les tests de pénétration aident à trouver des failles dans le système pour prendre les contre-mesures appropriées pour protéger les données et maintenir la fonctionnalité. Cette formation fournira à l'étudiant un tremplin pour exécuter des tests de pénétration dans la pratique et entreprendre la tâche complexe de cibler et de planifier efficacement une attaque de pénétration sur un environnement traditionnellement sécurisé.
Ce cours aide à préparer les examens de certification CEH (EC | Council), PenTest + (CompTIA) et GPEN (SANS).

Public cible
Ce cours s'adresse aux personnes du monde informatique qui souhaitent améliorer leur carrière et maîtriser l'art des tests d'intrusion.

Conditions préalables
Linux
Réseautique de base

Objectifs
• Contourner la sécurité et attaquer le réseau
• Se familiariser avec la pénétration
• Tester les faiblesses de sécurité existantes

Module 1: Planification et collecte d'informations

Avant que l'équipe de test d'intrusion puisse analyser et mener une série de tests et d'attaques, l'équipe doit collecter des données pour élaborer un meilleur plan d'action. Dans ce module, l'étudiant passera par les bases de la collecte d'informations et de la reconnaissance.

Collecte passive d'informations
- Le cadre OSINT
- Surveillance des blogs personnels et d'entreprise
- Collecter des informations personnelles sur les employés
- Récolte des courriels de l'organisation

Collecte d'informations active
- Analyse NMAP
- Versions des services
- Énumération DNS

Identifier les vulnérabilités et les exploits
- Script NSE
- Méthodes de détection des vulnérabilités
- Moteur de recherche Shodan
- Trouver des exploits
- Automatiser l'analyse

Module 2: Accès et post-exploitation

Dans ce module, les étudiants apprendront à utiliser leurs connaissances dans les deux premières phases pour accéder, soit en utilisant un exploit existant, soit en les forçant brutalement dans le réseau. Après avoir pris le contrôle de la cible, les étudiants apprendront à abuser des services existants pour élever leurs autorisations.

Trouver un moyen d'entrer
- Ingénierie sociale
- Services de forçage brutal
- Metasploit

Obtenir un accès via Wi-Fi
- Bases du Wi-Fi
- Modes de gestion et de surveillance
- Accéder au réseau

Post-exploitation et collecte de preuves
- Escalade des privilèges de base
- Utilisation des modules Meterpreter
- Principes de base de Windows et Linux Privesc
- Pivotement du réseau

Module 3: Menaces internes

Trouver des vulnérabilités sur le réseau à l'aide de différentes méthodes de détection est très important et peut révéler les vulnérabilités et les faiblesses de l'organisation. Dans ce module, les étudiants utiliseront.

Reniflage et attaques

- Attaques MAC
- Attaques DHCP
- Empoisonnement ARP
- Attaques d'usurpation d'identité
- Empoisonnement DNS
- Outils de reniflement
- Techniques de détection de reniflement
- Attaques Kerberos
- Billets Silver pour la persistance
- Cartographie et exploitation de domaine
- Escalade efficace des privilèges de domaine
- Exploits SMB
- Exploits SNMP
- Exploits SMTP
- Exploits FTP
- Passe-le-hachage

Module 4: Introduction à la sécurité des applications Web

Dans ce module, les étudiants apprendront l'importance de l'analyse de la sécurité des applications Web. De nombreuses organisations ont été piratées à l'aide de vulnérabilités dans la couche application.

Piratage de serveurs Web

- Injection SQL
- Vulnérabilité de téléchargement « upload » de fichier
- Inclusion de fichiers locaux
- Inclusion de fichiers à distance
- XSS
- BeEF
- Attaques par mot de passe