

SECURE TEST

Mettez en oeuvre des tests d'intrusion (pentests)
pour détecter les vulnérabilités dans un systèmes d'informations



Objectif

Initier une démarche méthodologique de tests de sécurité et comprendre les vulnérabilités les plus courantes, savoir les exploiter et les corriger.
Connaître des outils utilisables pour tester la présence de vulnérabilités dans son système d'information.



Destinataires

Informaticiens intéressés par les techniques d'attaques informatiques et les mesures de protection ad-hoc.



Formateurs

Consultants-Formateurs spécialistes de la sécurité informatique.



Prérequis

Bonnes notions dans le fonctionnement des systèmes d'exploitation et des réseaux.



Méthode pédagogique

Acquisition des compétences de manière immersive en s'appuyant sur des exemples réels et sur des ateliers de réflexion.

Apports théoriques et mise en oeuvre pratique grâce à un système vulnérable fourni par SECURESPHERE (sans danger pour votre système).



Compétences acquises

- Être en mesure d'appréhender les mécanismes permettant de se mettre en position d'interception réseau (man-in-the-middle)

- Comprendre les interactions entre les différents réseaux locaux d'entreprise.
- Savoir découvrir et exploiter des services vulnérables sur un réseau
- Être capable d'élever ses privilèges sur un système
- Savoir utiliser et comprendre le fonctionnement des outils permettant d'automatiser ces attaques ad-hoc.



PRÉREQUIS MATÉRIEL

SECURESPHERE met à la disposition des stagiaires un ordinateur portable pour la formation.

En cas d'indisponibilité de notre matériel, il vous sera demandé de fournir vous-même un ordinateur portable sans contrainte sur le système d'exploitation (Windows, Linux ou Mac OS X) sur lequel vous devrez pouvoir exécuter une machine virtuelle (fichier OVA) sans danger pour votre système.



DURÉE

3 jours - 21 heures



TARIF INTER

2 250 € HT
par stagiaire

TARIF INTRA

11 500 € HT
par stagiaire
(pour 10
personnes
maximum)



LIEU

Campus Cyber
Tour Eria,
5 rue Bellini
92800 Puteaux
ou dans vos
locaux



ACCESSIBILITÉ

Cette formation est accessible aux personnes en situation de handicap.



SECURESPHERE

est détenteur de la certification Qualiopi au titre de la catégorie d'actions de formation.

PROGRAMME

PRÉPARATIFS

Introduction

- Définitions et rappels
- Préparer un test d'intrusion (engagements, périmètre, contacts, convention)
- Méthodologie

Poste de l'auditeur

- Sécuriser un poste de travail d'auditeur
- Présentation de Kali Linux

DÉCOUVERTE RÉSEAU

Les équipements réseau

- Tour d'horizon
- Principales vulnérabilités

Découverte réseau

- Méthodologie de scans réseau
- Établir une topologie réseau

Les réseaux TCP/IP

- Rappels fonctionnels
- MAC spoofing
- Empoisonnement de cache ARP
- Attaques sur DHCP
- IP spoofing
- Sauts de VLAN

EXPLOITATION DE SERVICES

Tests sur les services accessibles par le réseau

- Interfaces d'administration
- Techniques de brute force en ligne

Exploitation de vulnérabilités web

- Injections SQL
- Commandes système
- Arguments de commandes
- Code interprété
- Upload arbitraires de fichiers

Exploitation de SGBD

- Comptes par défaut
- Exploitation de vulnérabilités
- Rebonds vers le système d'exploitation

EXPLOITATION DES SYSTÈMES

Linux

- Prise de contrôle de la machine (accès physique)
- Exploitation de programmes SUID
- Exploitation de services
- Comptes locaux

Windows

- Initiation à des frameworks post-exploitation (Metasploit, Covenant, etc.)
- Initiation à Mimikatz
- Méthodes pour élever ses privilèges
- Récupération des secrets (hash, cassage de mot de passe, tickets)

POST EXPLOITATION

- Nettoyage d'un système
- Rédaction d'un rapport



ÉVALUATION

La validation des compétences sera réalisée sous la forme de cas pratiques et de mises en situation.



ATTESTATION DE RÉUSSITE

Une AACE, Attestation d'Acquisition des Compétences de l'EPITA, est délivrée aux stagiaires ayant validé l'ensemble des compétences visées par le stage.

APPELEZ-NOUS : 01 84 07 16 87

Référent handicap : marie.moin@epita.fr

Siège Social : 14-16 rue Voltaire 94270 le Kremlin Bicêtre - Campus EPITA
RCS Créteil 809 748 635 - Déclaration d'activité N° 11 94 08975 94