Audit technique de sécurité

Programme *(Mis à jour le 12/02/2021)*

Introduction à l'audit de sécurité

- Pourquoi auditer la sécurité ?
- Le contexte juridique (ex : PCI-DSS)
- Les différents types d'audit : organisationnel, technique

L'audit technique de sécurité

- Les différentes façons de réaliser un audit technique : blackbox, whitebox, greybox
- Les limites d'un audit technique de sécurité
- Le planning typique d'un audit de sécurité technique

Les grandes phases de l'audit de sécurité technique :

- Collecte passive d'informations
- Collecte active d'informations
- Identification des vulnérabilités
- Exploitation des vulnérabilités
- Persistance et post-exploitation

Les principales failles de sécurité

- « systèmes » : buffer overflow, use-after-free, format string
- Web : failles PHP, injections SQL, XSS, XSRF, Clickjacking
- Réseau : déni de service, protocoles en clair, Man-In-The-Middle, Spoofing, Poisoning, Wifi

Le travail du Pentester :

- Collecter des informations en ligne afin de profiler une entreprise
- Scanner un réseau et identifier des vulnérabilités
- L'exploitation des failles sous Linux et Windows avec Metasploit
- Collecter et attaquer les mots de passe
- La post-Exploitation avec le meterpreter (bypasser un antivirus, élever ses privilèges, pivotage avec l'attaque pass-the-hash, pillage du système etc…)

Présenter les résultats de l'audit

- Le cours est accompagné de mises en pratique afin de permettre aux stagiaires de maîtriser les outils et les méthodes permettant d'auditer techniquement le niveau de sécurité d'un système d'information.
- Exemples d'outils que les stagiaires utiliseront : Metasploit, Netcat, Nmap et les scripts NSE, Open Vas, AirCrack-NG, John The Ripper, Medusa, Exiftool, TheHarvester, Maltego, Google GHDB, TCPDump, Nikto, Burp
  Proxy

Référence

THIS1939

Durée

3 jours / 21 heures

Prix HT / stagiaire

2550€

Objectifs pédagogiques

- Faire un audit technique de sécurité
- Définir les techniques de suivi de la sécurité informatique
- Montrer les résultats de l'audit de sécurité

Niveau requis

- Garantir avoir une connaissance de bases du modèle OSI, Windows, Unix, Réseau

Public concerné

- Responsables et Directeurs Informatiques, Qualité, Consultant et experts en Sécurité

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d'émargement (signature électronique privilégiée)
Evaluations formatives et des acquis sous forme de questions orales et/ou écrites (QCM) et/ou mises en situation
Questionnaires de satisfaction (enquête électronique privilégiée)