FORMATION EN PRESENTIEL ET/OU EN DISTANCIEL (SELON LE THEME)

PENTEST LES OUTILS D'AUDIT DE SÉCURITÉ

Dernière mise à jour le 17/10/2024.

OBJECTIF

Illustrer les méthodes pour éprouver les systèmes avec l'ensemble des attaques connues et identifier les vulnérabilités.

Tarif	**3290** € HT par participant
Réf.	**CYBOA**
Contact	0465260114 contact@univlearn.fr https://univlearn.fr/

COMPÉTENCES DÉVELOPPÉES

- Mettre en pratique les outils nécessaires pour rechercher les vulnérabilités
- Mettre en place une plateforme d'audit
- Identifier les vulnérabilités sur le périmètre du SI
- Mettre en place une politique de veilles de vulnérabilités
- Exploitation des vulnérabilités et filtrage des faux positifs
- Réalisation d'un rapport d'audit

PUBLIC CONCERNÉ

RSSI ou correspondants sécurité, DSI, chefs de projet, auditeurs, responsables techniques, administrateurs Systèmes

PRÉ-REQUIS

- Connaissance des systèmes Linux et Windows

MODALITÉS ET DÉLAIS D'ACCÈS

Vous pouvez vous inscrire pour suivre une de nos formations jusqu'à la veille de la date de démarrage si la formation est financée directement par votre entreprise ET si le nombre maximum de participants n'est pas atteint. Si la formation est financée via un OPCO, vous devez au préalable avoir obtenu un accord de ce dernier.

MÉTHODES ET MOYENS MOBILISÉS

Questionnaires de positionnement : un questionnaire de prérequis afin de s'assurer du niveau de l'apprenant et un questionnaire reprenant les attentes de l'apprenant en amont de la formation. Evaluation des acquis tout au long de la formation à travers des Tps, des Quizz; Evaluation de satisfaction de fin de formation; Attestation de fin de formation précisant les modules acquis et en cours d'acquisition; Support de cours remis en fin de session

MODALITÉS DE DÉROULEMENT DE L'ACTION DE FORMATION

Formation présentielle dispensée par un consultant formateur expert en cybersécurité. La formation alterne des exposés théoriques, des démonstrations et la mise en pratique au travers d'exercices et de cas concrets.

Niveau	Modalité	Effectif par session	Durée
Autres formations professionnelles continues	**Présentiel**	**2 mini > 6 maxi**	**35 heures / 5 jour(s)**

PROGRAMME

Aujourd'hui, pour affirmer avoir un niveau de protection suffisant sur l'ensemble de son infrastructure, il est nécessaire de réaliser des audits.
Le besoin en sécurité des systèmes d'information se fait à la fois ressentir de l'interne où les administrateurs et Expert SSI doivent disposer d'outils et de méthodologie pour évaluer la sécurité de leur système d'information en recherchant les vulnérabilités mais aussi de l'externe afin de former les auditeurs à intervenir sur les problématiques de sécurité sous forme d'audit de sécurité
Ce cours a pour objectif d'illustrer les méthodes pour éprouver les systèmes avec l'ensemble des attaques connues et identifier les vulnérabilités.
Mener un audit impose de connaitre des outils spécialisés et des méthodes.

Jour 1

Méthodologie de test d'intrusion

Externe
Interne
Footprinting et Reconnaissance
Analyse des vulnérabilités
Exploitation
Gain et maintien d'accès
La gestion des vulnérabilités

Vulnerability Assessment Concepts
La recherche de vulnérabilités
Classification des vulnérabilités
Vulnerability Management Life Cycle
Common Vulnerability Scoring System
Common Vulnerability and Exposure
Veille vulnérabilités
Vulnerability Assessment Tools
Plateforme d'audit

Mise en place de la plateforme d'audit
Installation et prise en main de Kali/Linux

Jour 2

Présentation du LABSSI

Services web vulnérables
OS Linux / Windows vulnérables
Réseaux vulnérables
Les outils de footprinting et de reconnaissance

Les attaques de mots de passe

Attaque par dictionnaires
Les outils sous Linux
Les outils sous Windows
Les rainbow tables
Port Scanning

NMAP host discovery
NMAP Scan de ports

NMAP Network cartography
NMAP NSE
Firewall evasion
SQL Mapping

Concept et outils de SQL Injection
Attaque du LABSSI

Jour 3

Les scanners de vulnérabilités

OpenVAS
Nikto / Vega
Nessus
Nexpose
Mise en pratique des scanners de vulnérabilité sur le LABSSI
Analyse des rapports

Jour 4

Les scanners de vulnérabilités WEB

Recherche vulnérabilités CMS, Wordpress
Burp Suite : prise en main et utilisation avancée du scanner / proxy

Jour 5

Exploitation

Proof of Concept et faux positifs
Découverte et mise en pratique de Metasploit
Le rapport d'audit

Structure d'un rapport d'audit
Détail vulnérabilités
Détail méthodologie
Synthèse des vulnérabilités

LES PLUS

C'est une formation pilotée par la pratique, les apprenants apprennent à mettre en place un environnement de test virtualisé et à installer tous les outils par eux-même. La pratique se fait ensuite sur des environnements de tests vulnérable, chaque partie théorique abordée est associée à de la mise pratique. Une étude ciblée sera réalisée à travers un LABSSI dédié pour la recherche, la découvertes et l'exploitation des vulnérabilités. Au final les méthodologies de rédaction d'un rapport d'audit seront détaillées - Formation certifiante éligible CPF - ICDL Module SECURITE DES TI / code 237556

INTERVENANT(S)	ÉVALUATION	ATTRIBUTION FINALE
Consultant formateur expert en cybersécurité	Chaque module de cours est concrétisé par un TP afin de permettre l'acquisition d'un vrai savoir-faire sur tous les points abordés, Evaluation de fin de formation afin d'évaluer l'atteinte des objectifs, Questions posées par le formateur tout au long de la formation à l'oral ou à travers un QCM	Attestation Individuelle de Formation