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

HACKING ET SÉCURITÉ NIVEAU 1

Dernière mise à jour le 02/10/2024.

OBJECTIF

Apprendre les techniques indispensables pour mesurer le niveau de sécurité de votre Système d'Information. A la suite de ces attaques, vous apprendrez à déclencher la riposte appropriée et à élever le niveau de sécurité de votre réseau.

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

COMPÉTENCES DÉVELOPPÉES

- Déterminer l'impact et l'étendue d'une vulnérabilité
- Évaluer le degré de sécurité de votre système d'information
- Appréhender les méthodes des hackers et être en mesure de déjouer leurs attaques.
- Effectuer un test de pénétration

PUBLIC CONCERNÉ

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.

PRÉ-REQUIS

- Avoir des connaissances en sécurité SI, réseaux et systèmes (en particulier Linux) et en programmation

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 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 formateur expérimenté. 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

Module 1 : Le Hacking et la sécurité
- Formes d'attaques, modes opératoires, acteurs, enjeux.
- Audits et tests d'intrusion, place dans un SMSI.

Module 2 : Sniffing, interception, analyse, injection réseau
- Anatomie d'un paquet, tcpdump, Wireshark, tshark.
- Détournement et interception de communications (Man-in-the-Middle, attaques de VLAN, les pots de miel).
- Paquets : Sniffing, lecture/analyse à partir d'un pcap, extraction des données utiles, représentations graphiques.
- Scapy : architecture, capacités, utilisation.

Travaux pratiques : Ecouter le réseau avec des sniffers. Réaliser un mini intercepteur de paquets en C. Utiliser scapy (ligne de commande, script python) : injections, interception, lecture de pcap, scan, DoS, MitM.

Module 3 : La reconnaissance, le scanning et l'énumération
- L'intelligence gathering, le hot reading, l'exploitation du darknet, l'Ingénierie Sociale.
- Reconnaissance de service, de système, de topologie et d'architectures.
- Types de scans, détection du filtrage, firewalking, fuzzing.
- Le camouflage par usurpation et par rebond, l'identification de chemins avec traceroute, le source routing.
- L'évasion d'IDS et d'IPS : fragmentations, covert channels.
- Nmap : scan et d'exportation des résultats, les options.
- Les autres scanners : Nessus, OpenVAS.

Travaux pratiques : Utilisation de l'outil nmap, écriture d'un script NSE en LUA. Détection du filtrage.

Module 4 : Les attaques Web
- OWASP : organisation, chapitres, Top10, manuels, outils.
- Découverte de l'infrastructure et des technologies associées, forces et faiblesses.
- Côté client : clickjacking, CSRF, vol de cookies, XSS, composants (flash, java). Nouveaux vecteurs.
- Côté serveur : authentification, vol de sessions, injections (SQL, LDAP, fichiers, commandes).
- Inclusion de fichiers locaux et distants, attaques et vecteurs cryptographiques.
- Évasion et contournement des protections : exemple des techniques de contournement de WAF.
- Outils Burp Suite, ZAP, Sqlmap

Travaux pratiques : Mise en œuvre de différentes attaques Web en conditions réelles côté serveur et côté client.

Module 5 : Les attaques applicatives et post-exploitation
- Attaque des authentifications Microsoft, PassTheHash.
- L'encodage de shellcodes, suppression des NULL bytes.
- Les Rootkits. Exploitations de processus : Buffer Overflow
- Metasploit : architecture, fonctionnalités, interfaces, workspaces, écriture d'exploit, génération de Shellcodes.

Travaux pratiques : Metasploit : exploitation, utilisation de la base de données. Msfvenom : génération de Shellcodes, piégeage de fichiers. Buffer overflow sous Windows ou Linux, exploitation avec shellcode Meterpreter

LES PLUS

C'est une formation pilotée par la pratique. A l'issue de la formation, l'apprenant sera en mesure de comprendre les techniques des pirates informatiques afin de pouvoir contrer leurs attaques. Il saura mesurer le niveau de sécurité de son système d'information. Il apprendra à réaliser un test de pénétration.

INTERVENANT(S)	ÉVALUATION	ATTRIBUTION FINALE
Consultant Formateur expert Cybersécurité Ethical Hacking	Chaque module de cours est concrétisé par un TP afin de permettre l'acquisition d'un vrai savoir-faire sur tous les points abordés, Questions posées par le formateur tout au long de la formation à l'oral ou à travers un QCM	Attestation justifiant les modules acquis et en cours d'acquisition