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

PENTEST GÉRER LES INCIDENTS DE SÉCURITÉ - DÉTECTION D'INTRUSIONS

Dernière mise à jour le 17/10/2024.

OBJECTIF

Apprendre à déclencher la riposte adaptée (filtrage d'anti-trojan, filtrage d'URL mal formée, détection de spam et détection d'intrusion en temps réel avec sonde IDS).

Tarif	2690 € HT par participant
Réf.	SecDet
Contact	0465260114 contact@univlearn.fr https://univlearn.fr/

COMPÉTENCES DÉVELOPPÉES

- Apprendre à gérer un incident d'intrusion
- Savoir identifier et comprendre les techniques d'analyse et de détection
- Acquérir les connaissances pour déployer différents outils de détection d'intrusion
- Connaître le cadre juridique
- Mettre en œuvre les solutions de prévention et de détection d'intrusions

PUBLIC CONCERNÉ

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

PRÉ-REQUIS

- Avoir de l'expérience en administration système Microsoft Windows ou Linux

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**	**28 heures / 4 jour(s)**

PROGRAMME

Module 1 : Le monde de la sécurité informatique – J1

Définitions "officielles" : le hacker, le hacking.
La communauté des hackers dans le monde, les "gurus", les "script kiddies".
L'état d'esprit et la culture du hacker.
Les conférences et les sites majeurs de la sécurité.
Déroulement d'une attaque
Test d'intrusion vs Audit
Atelier : Phase de reconnaissance : Que trouve-t 'on sur votre entreprise ?

Module 2 : TCP/IP pour firewalls et détection d'intrusions – J1 et J2

IP, TCP et UDP sous un autre angle.
Rappel sur ARP et ICMP.
Les parades par technologies : du routeur filtrant au firewall deep inspection ;
du proxy au reverse proxy, panorama rapide des solutions et des produits.
Panorama des différents sniffers réseau
Atelier : Visualisation et analyse d'un trafic classique. Utilisation de différents sniffers.

Module 3 : Comprendre les attaques sur TCP/IP – J2 et J3

Le "Spoofing" IP.
Sniffing d'un réseau switché : ARP poisonning.
Attaques par déni de service.
Prédiction des numéros de séquence TCP.
Vol de session TCP : Hijacking
Attaques sur SNMP.
Les scans
Détection de sniffer : outils et méthodes avancées.
IDS, IPS : l'importance de leur paramétrage
Le contournement des IDS avec la fragmentation IP et les règles de réassemblage.
Atelier : Injection de paquets fabriqués sur le réseau pour détecter un snffer. Analyse de PCAP pour détecter les différentes attaques. Détecter un scan avec un outil openSource (PortCentry, PSAD…). Détecter un ManInTheMiddle et un ARPSpoofing. Utilisation de SNORT et contournement d'un IDS.

Module 4 : Protéger ses données – J3

Rappel sur les bases du chiffrement
Rappels sur SSH et SSL (HTTPS).
Attaques sur les données chiffrées : "Man in the Middle" sur SSH et SSL
Attaques sur les mots de passe.
Atelier : Comment vérifier si vos mots de passe sont assez forts : cassage de mots de passe avec LophtCrack (Windows) et Hashcat (Unix).

Module 5 : Détecter les malveillants – J4

Vocabulaire : Ver, virus, rootkit
Etat de l'art des malveillants
Prise de contrôle d'un serveur : recherche et exploitation de vulnérabilités.
Les VDS, la veille, les CVS
Etat de l'art des anti-virus
Atelier : Les "Covert Channels" : application client-serveur utilisant ICMP.

Module 6 : Défendre les services en ligne – J4

Panorama des Vulnérabilités dans les applications Web.
l'OWASP
ISP, ISC et DevSecOps
Reverse-proxy et WAF
Atelier : Mise en place d'un reverse-proxy et d'un HIPS pour détecter et bloquer une attaque WEB

Module 7 : Comment gérer un incident ? – J4

Comment réagir face à une intrusion réussie ? Une cyber-crise ?
L'inforensic : la boîte à outils Unix/Windows pour la recherche de preuves.
Le rôle de l'Etat, les organismes officiels.
Le rôle du SIEM, sa mise en place et quelques solutions. Importance de la maîtrise de la gestion des LOG.

LES PLUS

Cette formation présente les techniques d'attaque les plus évoluées et montre comment y faire face

INTERVENANT(S)	ÉVALUATION	ATTRIBUTION FINALE
Consultant expert 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, Questions posées par le formateur tout au long de la formation à l'oral ou à travers un QCM	Attestation individuelle de formation