Programme de cours
Détection d'intrusions

Durée :	4 jours soit 28 heures	Référence :	IF-DETINT

Public visé :

- Consultants en sécurité
- Techniciens
- Administrateurs systèmes / réseaux

Pré-requis :

- Bonnes connaissances des réseaux TCP/IP.
- Connaissances de base en sécurité informatique.

Objectifs pédagogiques :

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

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Modalités d'évaluation et suivi :

Avant
Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice) qui validera la base de connaissances nécessaires.
Pendant
Après chaque module théorique, un ou des ateliers pratiques permettent la validation de l'acquisition des connaissances. Un Quizz peut accompagner l'atelier pratique.
Après
Un examen de certification si le programme de formation le prévoit dans les conditions de l'éditeur ou du centre de test (TOSA, Pearson Vue, ENI, PeopleCert)
Enfin
Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation.

Description / Contenu

Module 1 : Le monde de la sécurité informatique
- 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.

Atelier : Navigation Underground. Savoir localiser les informations utiles.

Module 2 : TCP/IP pour firewalls et détection d'intrusions
- IP, TCP et UDP sous un autre angle.
- Zoom sur ARP et ICMP.
- Le routage forcé de paquets IP (source routing).
- La fragmentation IP et les règles de réassemblage.
- De l'utilité d'un filtrage sérieux.
- Sécuriser ses serveurs : un impératif.
- Les parades par technologies : du routeur filtrant au firewall stateful inspection ; du proxy au reverse proxy.
- Panorama rapide des solutions et des produits.

Atelier : Visualisation et analyse d'un trafic classique. Utilisation de différents sniffers.

Module 3 : Comprendre les attaques sur TCP/IP

- Le "Spoofing" IP.
- Attaques par déni de service.
- Prédiction des numéros de séquence TCP.
- Vol de session TCP : Hijacking (Hunt, Juggernaut).
- Attaques sur SNMP.
- Attaque par TCP Spoofing (Mitnick) : démystification.

Atelier : Injection de paquets fabriqués sur le réseau. Utilisation au choix des participants d'outils graphiques, de Perl, de C ou de scripts dédiés. Hijacking d'une connexion telnet.

Module 4 : Intelligence Gathering - l'art du camouflage

- Chercher les traces : interrogation des bases Whois, les serveurs DNS, les moteurs de recherche.
- Identification des serveurs.
- Comprendre le contexte : analyser les résultats, déterminer les règles de filtrage, cas spécifiques.

Atelier : Recherche par techniques non intrusives d'informations sur une cible potentielle (au choix des participants). Utilisation d'outils de scans de réseaux.

Module 5 : Protéger ses données

- Systèmes à mot de passe "en clair", par challenge, crypté.
- Le point sur l'authentification sous Windows.
- Rappels sur SSH et SSL (HTTPS).
- Sniffing d'un réseau switché : ARP poisonning.
- Attaques sur les données cryptées : "Man in the Middle" sur SSH et SSL, "Keystoke Analysis" sur SSH.
- Détection de sniffer : outils et méthodes avancées.
- Attaques sur mots de passe.

Atelier : Décryptage et vol de session SSH : attaque "Man in the Middle". Cassage de mots de passe avec LophtCrack (Windows) et John The Ripper (Unix).

Module 6 : Détecter les trojans et les backdoors

- Etat de l'art des backdoors sous Windows et Unix.
- Mise en place de backdoors et de trojans.
- Le téléchargement de scripts sur les clients, exploitation de bugs des navigateurs.
- Les "Covert Channels" : application client-serveur utilisant ICMP.
- Exemple de communication avec les agents de déni de service distribués.

Atelier : Analyse de Loki, client-serveur utilisant ICMP. Accéder à des informations privées avec son navigateur.

Module 7 : Défendre les services en ligne

- Prise de contrôle d'un serveur : recherche et exploitation de vulnérabilités.
- Exemples de mise en place de "backdoors" et suppression des traces.
- Comment contourner un firewall (netcat et rebonds) ?
- La recherche du déni de service.
- Les dénis de service distribués (DDoS).
- Les attaques par débordement (buffer overflow).
- Exploitation de failles dans le code source. Techniques similaires : "Format String", "Heap Overflow".
- Vulnérabilités dans les applications Web.
- Vol d'informations dans une base de données.
- Les RootKits.

Atelier : Exploitation du bug utilisé par le ver "Code Red". Obtention d'un Shell root par différents types de buffer overflow. Test d'un déni de service (Jolt2, Ssping). Utilisation de netcat pour contourner un firewall. Utilisation des techniques de "SQL Injection" pour casser une authentification Web.

Module 8 : Comment gérer un incident ?

- Les signes d'une intrusion réussie dans un SI.
- Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
- Comment réagir face à une intrusion réussie ?
- Quels serveurs sont concernés ?
- Savoir retrouver le point d'entrée et le combler.
- La boîte à outils Unix/Windows pour la recherche de preuves.
- Nettoyage et remise en production de serveurs compromis.

Module 9 : Conclusion : quel cadre juridique ?

- La réponse adéquate aux hackers.
- La loi française en matière de hacking.
- Le rôle de l'Etat, les organismes officiels.
- Qu'attendre de l'Office Central de Lutte contre la Criminalité (OCLCTIC) ?
- La recherche des preuves et des auteurs.
- Et dans un contexte international ?
- Le test intrusif ou le hacking domestiqué ?
- Rester dans un cadre légal, choisir le prestataire, être sûr du résultat