DÉTECTION D'INTRUSIONS

Public	Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.
Durée	4 jours - 28 heures
Pré-requis	Bonnes connaissances des réseaux TCP/IP. Connaissances de base en sécurité informatique.
Objectifs	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
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Planning	Du 10/06/2024 au 13/06/2024 Du 14/10/2024 au 17/10/2024 Du 09/12/2024 au 12/12/2024
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

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.

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.

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.

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.

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.

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.

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.

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.

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.

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation