Détection d'intrusions comment gérer les incidents de sécurité

-Réference: **PL-53** -Durée: **4 Jours (28 Heures)**

Les objectifs de la formation

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

A qui s'adesse cette formation ?

POUR QUI :

- Responsable, architecte sécurité. Techniciens et administrateurs systèmes et réseaux.

Programme

- **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.
  - Travaux pratiques Navigation Underground.
  - Savoir localiser les informations utiles.
- **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.

Programme

- Panorama rapide des solutions et des produits.
- Travaux pratiques Visualisation et analyse d'un trafic classique.
- Utilisation de différents sniffers.

- **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.
  - Travaux pratiques 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.

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

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

Programme

- **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.
  - Travaux pratiques Analyse de Loki, client-serveur utilisant ICMP.
  - Accéder à des informations privées avec son navigateur.
- **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.
  - Travaux pratiques 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.
- **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.
- **Conclusion : quel cadre juridique ?**

Programme

- 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.


(+212) 5 22 27 99 01


(+212) 6 60 10 42 56


Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc