Techniques de Hacking et Contre-mesures : niveau 1

Lien : https://innov-systems.com/formation/techniques-de-hacking-et-contre-mesures-niveau-1

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC42

CATÉGORIE
Test d'Intrusions, Techniques de Hacking, Contre Mesures et Audit

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Connaitre les différentes cibles d'un piratage
- Etre capable de lutter contre le hacking
- Assimiler le mécanisme des principales attaques

POUR QUI ?

- Administrateurs de systèmes
- Techniciens chargés du support
- Toutes personnes impliquées dans la sécurité du système d’information

Programme détaillé

1 / Evolution de la cybersécurité

- Nouveaux acteurs et nouvelles portées de la cybersécurité
- Sécurité et juridique
- CNIL ANSSI
- ENISA
- Les normes

2 / Principes généraux de la sécurité informatique

- Pourquoi la sécurité informatique ?
- Les piliers de la sécurité informatique : confidentialité, intégrité, disponibilité...
- Les composants de la cybersécurité : Que veut-on protéger ? Pourquoi ?
- Défense en profondeur et politique de sécurité
- Méthodes et normes pour l'analyse des risques

3 / Introduction à la cybercriminalité

- L'évolution de la cybercriminalité. Son impact
- Les types d'attaquants (White hat...)
- Qu'est-ce que le hacking ?
- Les principaux groupes de hackers
- Les types d'attaques (Malware, MITM, SE...)
- Les différentes phases d'une attaque (Cyber Kill Chain)
- Sophistication des techniques d'attaques
- Les différentes lois et référentiels

4 / Reconnaissance passive et active

Innov Systems

- Utiliser les outils publics pour obtenir des informations sur une cible
- Les outils de reconnaissance active (Nmap, Hping3) et leur signature (Wireshark)
- Banner grabbing : description des services d'une cible
- Les outils d'analyse (NmapSE et Metasploit)
- Analyse de vulnérabilités

5 / Bien comprendre les protocoles réseaux

- D’autres aspects des protocoles IP, TCP et UDP
- Focus sur ARP et ICMP
- Le routage forcé de paquets IP
- Problèmes de sécurité de TCP/IP
- Filtrage sérieux : l'utilité
- Sécurisation des serveurs : un impératif
- Routeur filtrant au firewall stateful inspection
- Bref présentation des solutions et des produits

6 / Connaitre les attaques sur réseau

- Liste des protocoles les plus vulnérables
- Compréhension et utilisation des techniques de "l'homme du milieu" (MITM)
- Attaques sur les protocoles réseaux
- IDLE Scan
- LLMNR (Link-Local Multicast Name Resolution)
- WPAD (Web Proxy Auto Discovery)
- DoS
- ARP (Address Resolution Protocol)
- Usurpation d'IP et MAC
- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name System)
- Description des Protocoles 802.11 et attaques associées

Innov Systems

7 / Les vulnérabilités des applications web

- Top 10 OWASP
- Comprendre les attaquse par injection
- Les failles XSS (Cross-Site Scripting)
- Les mauvaises configurations de sécurité
- Reconnaissance et utilisation des références directes non sécurisées à un objet
- Cross-Site Resquest Forgery (CSRF)
- Cookie poisonning, session hijacking...
- Exploitation de vulnérabilités connues

8 / Exploitation

- Les frameworks offensifs (Metasploit, Empire)
- Recherche et obtention d'accès via une vulnérabilité identifiée

9 / Post-exploitation

- Objectifs de la phase de post-exploitation
- Identification des modules de post-exploitation

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Innov Systems

Prochaines dates programmées

08 au 12 Fév. 2027	Présentiel - Casablanca
05 au 09 Avr. 2027	Présentiel - Casablanca
31 Mai au 04 Juin 2027	Présentiel - Casablanca
26 au 30 Juil. 2027	Présentiel - Casablanca
20 au 24 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés

Innov Systems