Sécurité des SI : types d’intrusions

Lien : https://innov-systems.com/formation/securite-des-si-types-dintrusions

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC30

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

OBJECTIFS DE LA FORMATION

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

- Mettre en pratique les techniques d'intrusion les plus récentes sur les principales technologies du marché

POUR QUI ?

- Experts en sécurité
- Auditeurs internes
- Administrateurs systèmes ou réseaux
- Chefs de projets

Innov Systems

Programme détaillé

1 / Introduction de la sécurité informatique

- Définitions : le hacker, le hacking
- La communauté des hackers dans le monde
- L'état d'esprit et la culture du hacker
- Les conférences et les sites majeurs de la sécurité

2 / Introduction aux tests d'intrusion

- Définition du test d'intrusion
- L'intérêt du test d'intrusion
- Les phases d'un test d'intrusion
- Reconnaissance
- Analyse des vulnérabilités
- Exploitation
- Gain et maintien d'accès
- Comptes rendus et fin des tests

3 / 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 : fragmentation, ICMP, OS Fingerprinting, DNS, dénis de service, etc
- 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

Innov Systems

4 / Les attaques sur TCP/IP

- Comment les pirates informatique mettent en oeuvre le "Spoofing" IP
- Les attaques par déni de service
- La technique de la prédiction des numéros de séquence TCP
- Vol de session TCP
- Comprendre comment les pirates arrivent à réaliser des attaques sur SNMP
- Attaque par TCP Spoofing (Mitnick)

5 / Intelligence Gathering

- Interrogation des bases Whois, les serveurs DNS, les moteurs de recherche
- Les techniques pour mettre en place l'identification des serveurs
- Analyse des résultats
- Les règles de filtrage

6 / Détection des trojans et des backdoors

- Vue d'ensemble des backdoors sous Windows et Unix
- Définition d'un backdoor
- Mettre en place des backdoors et des trojans
- Le téléchargement. Exploitation de bugs des navigateurs
- Les Covert Channels

7 / Intrusion sur les applications web

- Infrastructure Web
- Rappels HTTP
- Prise d'empreinte
- Présentation des webshells
- Injection de code SQL, de commande, inclusion de fichier
- XSS et CSRF

Inov Systems

8 / Découverte des mots de passe

- Généralités
- Génération des empreintes
- Méthodes et outils de cassage d'empreinte

9 / Utilisation de Metasploit

- Présentation du framework
- Méthodologie d'intrusion avec Metasploit
- Présentation de Meterpreter

10 / Intrusion sur les postes clients

- Évolution des menaces
- Prise d'empreintes des logiciels
- Attaques et prise de contrôle d'un poste client
- Pillage et rebond

11 / Intrusion sur les bases de données

- Introduction et rappels SQL
- Intrusion MySQL
- Intrusion SQL Server
- Intrusion Oracle

12 / Intrusion sur les systèmes Windows

- Identification des machines et des services
- Récupération d'information à distance / sessions nulles
- Récupération d'informations locales
- Authentification sous Windows et récupération des empreintes
- Attaque hors ligne

Inov Systems

- Élévation de privilèges

13 / Intrusion sur les systèmes Unix/Linux

- Sécurité sous Unix/Linux
- Sortir de la cage
- Attaque par le réseau
- Attaque locale

14 / Synthèse de la formation

- Validation des acquis : QCM de Certification

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

Prochaines dates programmées

01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca
13 au 17 Sep. 2027	Présentiel - Casablanca

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

Innov Systems

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