CYBERSÉCURITÉ

Hacking et Sécurité - Niveau Expert

5 jours (35h00) | HS0023 | Num form : form-268 | Expertise

INFORMATIQUE / SÉCURITÉ IT / CYBERSÉCURITÉ

À l'issue de ce stage vous serez capable de :

- Savoir protéger son système d'information
- Comprendre comment sécuriser tous les aspects d'un SI : réseau, applicatifs et Web
- Acquérir les connaissances et compétences nécessaires pour détecter des failles et mettre en oeuvre des parades
- Savoir correctement réagir en cas d'attaque soudaine
- Être capable de mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle

Niveau requis :

- Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" ou disposer des compétences équivalentes

Public concerné :

- Développeurs
- Administrateurs systèmes / réseaux
- Ingénieur sécurité
- Consultant sécurité

Programme :

INTRODUCTION

- Définition du hacking

- Panorama 2018/2019
- Référentiel de sécurité (ANSSI, ENISA, CLUSIF, Cybermalvaillance.gouv etc...)
- Les différents types de hackers
- Les différents types d'attaques
- Les différents outils utilisés par le hacker
- Le cycle de l'attaquant

LE HACKING

- Scan de réseau/ports/versions
- Exploitation de CVE
- Élévation de privilège
- Mise en place d'une backdoor
- Récupération d'informations, création d'un dictionnaire + Bruteforce
- Payload msfvenom MITM
- Saut de VLAN (yersinia et/ou table overflow)

LES PILIERS DE LA SÉCURITÉ

- Confidentialité
- Intégrité
- Disponibilité
- Traçabilité

LES GRANDS PRINCIPES DE LA SÉCURITÉ

- IAAA
- Authentification
- Need to know
- Least Privilege
- Non répudiation
- Défense en profondeur

LA SÉCURITÉ PHYSIQUE

- Notion de sécurité physique
- Mise en correspondance des notions avec les principes précédents

SÉCURISER LE RÉSEAU

- La sécurité de la couche 2 : Port security, vLlan, Ssh, dhcp snooping, Defense contre arp MITM, Sécurité pour DTP,CDP,VTP,STP.
- La sécurité de la couche 3 : IPSec, routeur filtrant
- La sécurité de la couche 4 : Explication de la passerelle d'interconnexion de l'ANSSI, Travaux pratiques sur PFsense, explication des IDS/IPS , présentation de Snort, travaux

pratiques sur Snort
- La sécurité de la couche 5 : Le proxy

SÉCURISER LE SYSTÈME

- Hardenning sur Linux
- Hardenning sur Windows
- Mise en place d'HIDS

SUPERVISION DE LA SÉCURITÉ

- Présentation SOC
- Présentation SIEM
- Présentation de ELK et Splunk
- Mise en place de ELK ou Splunk pour analyser les Logs

RÉPONSE À INCIDENT

- Rejouer les attaques
- Analyser les logs
- Utiliser WireShark