HACKING ET SÉCURITÉ - PERFECTIONNEMENT_1097

3250 € HT (tarif inter) | REF : -RÉS607
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

5 JOURS | **35** HEURES

Description

PROGRAMME

LA SENSIBILISATION A LA SÉCURITÉ INFORMATIQUE | PREMIÈRE PARTIE

- L'apparition des cyberattaques.
- Les caractéristiques juridiques.
- La cyber sécurité autrement.
- La veille technologique, dans le domaine de la sécurité.

LA SENSIBILISATION A LA SÉCURITÉ INFORMATIQUE | DEUXIÈME PARTIE

- La méthodologie d'OSINT.
- La reconnaissance passive (WHOIS, SHODAN…).
- La reconnaissance active (Scan de ports…).
- Les techniques d'ingénierie sociales.
- Les mesures contre la cybercriminalité.

LES ATTAQUES POSSIBLES

- Les fondements des réseaux.
- Les différentes attaques sur les réseaux.
- Analyser le trafic réseau en temps réel (Wireshark).
- L'exploitation d'une faille de sécurité avec Metasploit.

LES SOLUTIONS POUR OPTIMISER LA SÉCURITÉ DU RÉSEAU : (FW/IDS/IPS)

- La présentation.
- Les firewall (iptables…).
- Le concept de supervision réseau et sa nécessité (Nagios) - Les IDS/IPS (Suricata, OSSEC…).
- La détection, pertinence et amplification des signaux faibles.

LES PRINCIPES DE BASE DE LA CRYPTOGRAPHIE

- L'histoire de la machine (Enigma).
- L'encodage base 64.
- Les différentes fonctions de hachage cryptographique.
- Le cryptage symétrique et asymétrique.
- La sécurisation des emails (PGP) et la dissimulation des données.

LA SÉCURISATION DES APPLICATIONS WEB AVEC L'OWASP L'OWASP : LES 10 RISQUES LES PLUS CRITIQUES POUR LA SÉCURITÉ DES APPLICATIONS

- L'opération des outils (BurpSuite, ZAP Proxy…).
- Les scanners de vulnérabilités Web.

L'ANALYSE DE MALWARE ET LA PRATIQUE DE L'INVESTIGATION NUMÉRIQUE

- L'analyse statique de base d'un malware et l'analyse dynamique de base d'un malware.
- Les différentes techniques de détection des virus et malwares.

LA RÉALISATION D'UN AUDIT TECHNIQUE

- Les procédés d'audit.
- Les différents types d'audits et les cas particuliers.

OBJECTIFS

Identifier les faiblesses des éléments des prises d'empreintes Avoir des compétences techniques pour comprendre les attaques Comprendre comment organiser la sécurité informatique Savoir rechercher des informations fiables

PUBLIC | PRÉREQUIS

PUBLIC
Techniciens informatique, gestionnaires de parc, techniciens d'exploitation, techniciens de maintenance…
PRÉREQUIS
Connaissance de la structure matérielle et architecturale d'un ordinateur

INFOS PRATIQUES

HORAIRES DE LA FORMATION
de 9 h 00 à 12 h 30 et de 13 h 30 à 17 h 00
MÉTHODOLOGIE PÉDAGOGIQUE
Théorie | Cas pratiques | Synthèse
MODALITÉS D'ÉVALUATION
Évaluation qualitative des acquis tout au long de la formation et appréciation des résultats

DATES ET LIEUX

Aucune session ouverte