FORMATION HACKING ET SECURITE LES BASES

La formation Hacking et Sécurité les bases sur 2 jours va vous permettre de protéger votre système d'information afin de contrer les attaques les plus courantes. Vous obtiendrez ainsi une vue d'ensemble des principaux risques existants sur les réseaux, serveurs Web et données. À terme, vous serez aptes à anticiper les failles de votre système et à en mesurer les risques dans le but d'y appliquer la meilleure protection possible

PROGRAMME

1/ Introduction générale
- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test

2/ Prise d'information
- Objectifs
- Prise d'information passive (WHOIS, réseaux sociaux, Google Hacking, Shodan, etc.)
- Prise d'information active (traceroute, social engineering, etc.)
- Bases de vulnérabilités et d'exploits

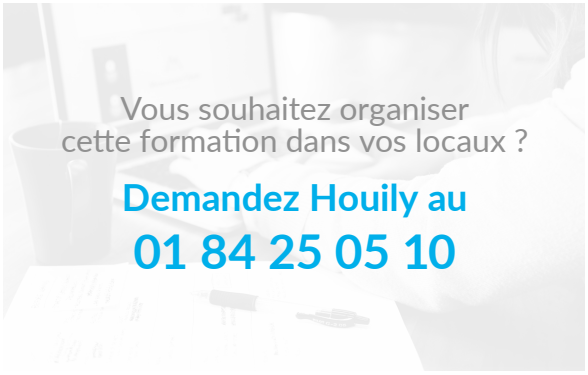
3/ Réseau
- Rappels modèles OSI et TCP/IP
- Vocabulaire
- Protocoles ARP, IP, TCP et UDP
- NAT
- Scan de ports
- Sniffing
- ARP Cache Poisoning
- DoS / DDoS

4/ Attaques locales
- Cassage de mots de passe
- Elévation de privilèges
- Attaque du GRUB

5/ Ingénierie sociale
- Utilisation de faiblesses humaines afin de récupérer des informations sensibles et/ou compromettre des systèmes
- Phishing
- Outils de contrôle à distance
- Attaque à distance
- Introduction à Metasploit Framework

PRIX (INTER-ENTREPRISE) : 1300 euros

14h jours | **SEH01**



OBJECTIFS

- Évaluer les risques et en mesurer leur portée
- Connaître les termes techniques
- Savoir mener un test d'intrusion
- Adopter les bonnes pratiques de sécurité
- Être capable de repérer les failles et techniques de hacking
- Connaître les différentes mesures préventives et correctives à adopter
- Être capable de contrer les attaques courantes

PRE-REQUIS

- Avoir des notions de sécurité informatique
- Connaître les invités de commandes Windows et Linux
- Connaissances sur le fonctionnement des applications Web

PUBLIC CONCERNE

- Responsables de l'informatique
- Responsables de la sécurité
- Administrateurs réseaux
- Techniciens
- Webmasters

DATES INTER-ENTREPRISES

Delais d entree : sans
Paris et à distance
06/03/2023, 03/04/2023, 09/05/2023, 12/06/2023, 03/07/2023, 07/09/2023, 12/10/2023, 09/11/2023, 04/12/2023,

Si vous souhaitez organiser cette formation a une autre date contactez-nous

NOUS CONTACTER

Openska
21 rue Louise Weiss
75013 Paris

Tel : 01 84 25 05 10
Tel : 01 84 17 44 76
www.openska.com

6/ Scanner de vulnérabilités
- Attaque d’un poste client
- Attaque d’un serveur
- Introduction aux vulnérabilités Web

7/ Se sécuriser
- Les mises à jour
- Configurations par défaut et bonnes pratiques
- Présentation de la stéganographie
- Anonymat (TOR)

ELEMENTS COMPLÉMENTAIRES À TRANSMETTRE IMPÉRATIVEMENT À VOTRE OPCO POUR VOTRE DEMANDE DE PRISE EN CHARGE

HORAIRES
- 9h30-13h
- 14h-17h30

ACCÈS HANDICAP
Oui, Consultez notre référent interne.

MODALITÉS D'ÉVALUATION
L'évaluation des acquis se fait tout au long de la formation au travers de multiples exercices et mise en situation

MODALITÉS DE SUIVI DE L'EXÉCUTION
- Contrôle systématique des présences par demi-journée
- Attestation de présence remis à chaque participant

COMPÉTENCES DU FORMATEUR
Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque formation qu'ils animent. Ils ont majoritairement cinq à dix années d'expérience dans leur domaine de compétences et ont une grande pratique en entreprise

MOYENS PÉDAGOGIQUES
Les supports pédagogiques sont imprimés par nos soins et transmis à chacun des stagiaires.Les supports sont aussi remis au format électronique aux participants. Ce support est projeté via un vidéo projecteur afin d'animer la formation.Des exercices d'application ou études de cas sont prévus afin de valider les acquis des stagiaires.

MOYENS D'ACCOMPAGNEMENT
8 personnes maximum, formation animée par un formateur expert sur le sujet.
Mise en situation : Pédagogie active et participative.
Apport théorique et méthodologique.
Etude de cas. Atelier pratique.

NATURE DES TRAVAUX DEMANDÉS AU STAGIAIRE
Un exercice est réalisé par le participant à la fin de chaque chapitre. Le participant dispose de 20 min avant de passer à la correction avec le formateur.

MODALITÉS TECHNIQUES EN CAS DE PROBLÈMES
Les connexions et installations d'outil peuvent être testées en amont de la formation avec le formateur et les stagiaires ou le donneur d'ordre.
Ce test permet d'éviter tout accident technique lié aux outils de connexion à distance.
Le formateur prend la main sur le poste du participant en cas de difficulté durant la formation.

ORGANISME DE FORMATION RÉFÉRENCÉ SOUS LE NUMÉRO : 117 555 432 75