réf. sc13

TECHNIQUES DE HACKING ET DE CONTRE-MESURES

INFORMATIONS

CONTACT
03 88 47 10 96
mfo@metaformose.org

A QUI S'ADRESSE LA FORMATION ?
- Responsable réseau
- Toute personne en charge de la sécurité
- Cette formation ne convient pas aux développeurs

MÉTHODES ET OUTILS PÉDAGOGIQUES
- Formation en présentiel, interactive axées ur la pratique pour une meilleure compréhension et application
- Supports vidéo et exercices
- Documents informatiques et papiers

PREREQUIS
- Avoir suivi les formations «Mettre en œuvre la sécurité réseaux» ou «Concevoir et mettre en œuvre la sécurité du système d'information

NOMBRE DE PARTICIPANTS
2 à 8 personnes

DURÉE DE L'INTERVENTION
5 journées soit 35 heures
9h-12h30 et 13h30h-17h

EVALUATION
- Contrôle des connaissances en cours de formation, tests, questionnaires
- Fiche d'évaluation et de satisfaction stagiaire
- Attestation individuelle de formation

INTERVENANTS
- Formateurs seniors experts en sécurité et cloud

LES OBJECTIFS DE LA FORMATION

» Comprendre les risques, évaluer leur portée
» Savoir identifier les techniques d'hacking et repérer les failles
» Connaître les mesures à adopter et savoir engager des actions préventives et correctives
» Définir les priorités d'investissement en termes de sécurité

LE PROGRAMME DE LA FORMATION

1. Introduction et définition
- La sécurité informatique, pour quoi, pour qui ?
- L'hacking se veut éthique
- Connaître son ennemi pour s'en défendre

2. Méthodologie d'une attaque
- Préambule
- Cibler ma victime
- L'attaque
- Introduire le système et assurer son succès
- Bilan de l'intrusion et sécurisation

3. Social Engineering
- Brève histoire d'une technique vieille comme le monde
- Ingénierie sociale : pourquoi ?
- Solution de protection
- Pour aller plus loin

4. Les failles physiques
- Généralités
- Accès direct à l'ordinateur : accès à un ordinateur éteint (BIOS protégé et non protégé) et accès à un ordinateur allumé

5. Les prises d'empreinte
- Le hacking éthique
- Collecte d'informations : le footprinting, le fingerprinting, découverte de failles potentielles, le reporting, sites internet

6. Les failles réseaux
- Généralités
- Rappel sur les réseaux TCP/IP
- Outils pratiques
- Dos et DDos
- Sniffing
- Man in the middle (avec petit TP)
- Vol de session TCP HIJACKING
- Failles Wifi
- IP over DNS
- La téléphonie sur IP

7. Les failles systèmes
- Généralités
- Les mots de passe
- Utilisateurs, groupes et permissions sur le système
- Élévations des privilèges
- Le processus
- Le démarrage
- L'hibernation
- Les appels de procédures distantes
- La virtualisation
- Les logs, les mises à jour et la sauvegarde
- Bilan

8. Risques juridiques et solutions
- Préambule
- Atteintes à un système d'information
- Atteintes aux traitements de données à caractère personnel
- Infractions classiques applicables à l'informatique
- Solutions et préconisations