G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Sécurité Linux

But de la formation

- Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux
- Réduire ou éliminer les risques sur les systèmes Linux
- Configurer les services courants pour qu'ils soient robustes avant leur mise en production (Apache, BIND, ...)
- S'assurer de l'intégrité des données sur les serveurs Linux
- Maîtriser les outils permettant de répondre aux incidents de sécurité
- Améliorer ses connaissances des procédures, bonnes pratiques et outils de sécurité du monde Unix

Pré-requis

- Avoir les bases en administration de systèmes Unix, idéalement 3 à 5 ans d'expérience

Type de public

- Professionnels de la sécurité,
- Administrateurs systèmes expérimentés,
- Auditeurs et gestionnaires d'incidents,
- Analystes en sécurité, auditeurs et membres de CSIRT (CERT)

Moyens pédagogiques

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Sanction de la formation

- Examen de certification HS2
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral avec travaux pratiques et échanges interactifs

Durée

35 heures (5 jours).

Programme

Introduction

- Panorama de l'histoire des problèmes de sécurité
    - Suivre l'actualité
    - Implication des utilisateurs
    - Discipline des administrateurs
        - Sudo

Cryptographie

- Rappels sur le vocabulaire, les principes et les algorithmes
- SSH
- GnuPG
- Certificats X.509 et infrastructures à clés publiques
    - openssl
- Certificats X.509 pour le chiffrement, la signature et l'authentification
    - application à Apache et nginx
    - application à Postfix
- Systèmes de fichiers chiffrés
    - dm-crypt
    - eCryptfs
- DNS et cryptographie
    - DNSSEC

Sécurité de l'hôte

- Durcissement de l'hôte
    - configuration de GRUB
    - configuration du système
    - bonnes pratiques de configuration des daemons
    - Détection d'intrusion sur l'hôte
    - Syslog
    - comptabilité système (accounting)
    - audit détection de rootkits
    - AIDE
- Gestion des utilisateurs et authentification
    - NSS
    - PAM

Contrôle d'accès

- Contrôle d'accès discrétionnaire
    - droits d'accès
    - ACL
- Contrôle d'accès obligatoire
    - SELinux

Sécurité réseau

- Durcissement du réseau
    - nmap
    - tcpdump
    - Wireshark
- Filtrage de paquets
    - concepts et vocabulaire
    - netfilter
    - TCP Wrapper
- Réseaux privés virtuels
    - OpenVPN

Examen de certification HS2 (QCM sur ordinateur)