Formation « Sécurité Linux »

Réf : SECULIN

Linux est le socle des infrastructures de l'internet, de l'informatique en nuage, comme des systèmes embarqués. Son durcissement et son maintien en condition de sécurité sont au cœur de la réussite de sa politique de sécurité.

Objectifs

- Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux
- Réduire ou éliminer les risques sur les systèmes Linux
- Configurer les services courant pour qu'ils soient robustes avant 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

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

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

Pré-requis

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

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- 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

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECULIN par HS2.**

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)