Sécuriser un système linux

PRÉSENTIEL | CERTIFIANT

VUE D'ENSEMBLE
Contexte
Les risques

INTRUSION D'UTILISATEUR
Ingénierie sociale
Découverte des services (scan de ports)
Utilisation de services non protégés ou peu protégés
Usurpation d'identité d'utilisateur
Usurpation d'adresse IP (IP spoofing)

INTRUSION DE PROGRAMME
Pgm destructeur : virus
Pgm cassant la sécurité : cheval de Troie
Exploitation d'une « backdoor »

DÉNI DE SERVICE
Ping Mortel
Finger récursif
Inondation de SYN

SÉCURISER LA MISE EN PLACE
Sécurisation physique
Sécurisation de l'amorçage
Sécuriser l'installation du système

SÉCURISER LES COMPTES
Utiliser la PAM
Renforcer les mots de passe
Limiter su avec wheel
Restreindre les shells

SÉCURISER LES DISQUES
Permissions
Attributs étendus
Contrôler les programmes en setuid et setgid
Cryptage GPG et effacement de sécurité

PARTITIONNEMENT SÉCURISÉ

SÉCURISER LES SERVICES
N'installer que le nécessaire
N'activer que le nécessaire
TCP wrappers : Limiter les hôtes ayant accès à un service
Crypter les accès aux services avec SSL ou SSH
Auditer

LE PARE-FEU NETFILTER
Les hooks
Le NAT
Fonctionnement
Syntaxe : iptables
Outils d'administration

Référents pédagogiques

Nos intervenants sont des spécialistes du logiciel proposé et sont sélectionnés selon un processus de qualification très rigoureux permettant d'évaluer notamment : leur connaissance de l'outil, leurs compétences pédagogiques et leur capacité à faire travailler les apprenants en format « atelier ».

OBJECTIFS
Sécuriser une machine linux dans tous ses aspects, matériel et logiciel, poste autonome et serveur. Savoir paramétrer le pare-feu des noyaux linux récents

PRÉ-REQUIS
Avoir suivi les cours « LINUX Administration » et « Réseaux-TCP/IP»

PUBLIC
Administrateurs réseaux, RSI

MÉTHODES PÉDAGOGIQUES
Un poste de travail par personne / Points théoriques apportés par le formateur / Mise en application aux travers d'exercices / Échanges participants-formateur

RESSOURCES PÉDAGOGIQUES
1 ordinateur par participant
Support de cours, cas pratiques

ÉVALUATION

Évaluation préalable
Recueil des attentes (QCM)
Évaluation des compétences
Cas pratiques
Évaluation de la formation
Questionnaire de satisfaction stagiaire
Synthèse fin de stage du formateur

VALIDATION
Attestation de fin de formation
Attestation de présence

MODALITÉS DE SUIVI D'EXÉCUTION DE LA FORMATION
Le contrôle de l'exécution de la formation est assuré par le formateur

DATES
Cf planning

OPTION CERTIFICATION
100 € HT / pers.
ENI | **Code CPF : 237547**