

Objectifs

Sécuriser une machine linux dans tous ses aspects, matériel et logiciel, poste autonome et serveur. Définir et appliquer une politique de sécurité aux ordinateurs de l'entreprise.

Participants

Administrateurs système et réseaux.

Prérequis

Avoir suivi les cours « LINUX Administration » et « Réseaux-TCP/IP » ou connaissances équivalentes.

Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en oeuvre les nouveaux outils présentés au cours de la session.

Profil de l'intervenant

Consultant-formateur expert sur cette thématique. Suivi des compétences techniques et pédagogiques assurée par nos services.

Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d'accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d'une documentation pédagogique papier ou numérique à échéance de la formation.

Méthodes d'évaluation des acquis

Exercices individuels et collectifs durant la formation. Évaluation des acquis et attestation de fin de stage adressés avec la facture.

Programme

Les attaques

Ingénierie sociale

Découverte des services (scan de ports)

Usurpation d'identité, d'adresse IP

Attaque force brute et attaque par dictionnaire

Virus, cheval de Troie, Déni de service

L'authentification, les comptes

Les comptes : utilisateur, groupe

Les bases de compte : locale, serveur (NIS, LDAP)

Sécurisation des mots de passe : formation des utilisateurs, la « SHADOW suite »

Les bibliothèques PAM

L'architecture du système PAM

Les fichiers de configuration

Intérêt de restreindre les ressources du système au niveau PAM

Paramétrage des règles PAM

Etude des principaux modules

Les droits des comptes

Permissions standards Linux. Les ACLs POSIX

Le danger de l'élévation de privilège associée aux fichiers (SUID, SGID)

L'élévation de privilège déclenchée : le sudo

Le chiffrement : base de la sécurité moderne

Les 2 types d'algorithmes cryptographiques : symétriques et asymétriques (à clé publique), les fonctions de hachage. La confidentialité. L'authentification et l'intégrité par la signature numérique. Les certificats, les autorités de certification et la PKI

Le service SSH : ouverture de session et copies sécurisées, le protocole et les commandes ssh

SSL : utilisation et certificats X-509

Chiffrement de fichiers (GnuPG) et de volume (LUKS)

Le filtrage réseau

Panorama des techniques: pare-feu, hôte-bastion, zone démilitarisée, proxy, nat (masquerading)

Le pare-feu noyau Netfilter: la commande Iptables

TCP wrappers : Limiter les hôtes ayant accès à un service

Mise en place d'un routeur filtrant, du masquerading et d'un bastion avec iptables

Le proxy SQUID

La sécurisation des applications

Principes généraux :

N'installer que le nécessaire

N'activer que le nécessaire

Sécurisation du Web (Apache), du mail (Sendmail, Postfix), du DNS (bind)