Formation Linux Sécurité + Préparation LPI 303

Durée :	5 jours
Public :	Administrateurs Systèmes Linux confirmés
Pré-requis :	Avoir les connaissances Linux équivalentes au niveau LPI 202
Objectifs :	Maitriser la sécurité sous Linux - Comprendre la cryptographie et utiliser les certificats - Sécuriser les hôtes - Détecter les intrusions - Gérer les utilisateurs et les droits - Contrôler les accès - Gérer la sécurité Réseaux
Sanction :	Attestation de fin de stage mentionnant le résultat des acquis
Taux de retour à l'emploi:	Aucune donnée disponible
Référence:	LIN100012-F
Note de satisfaction des participants:	4,85 / 5

Sujet 325: Cryptographie

325.1 Certificats X.509 et les PKI

Comprendre les certificats X.509, leur cycle de vie, leurs champs et leurs extensions
Comprendre les chaînes de confiance et les PKI
Générer et gérer les clés publics et privées
Créer, gérer et sécuriser une autorité de certification
Demander, signer et gérer des certificats serveur et client
Révoquer des certificats et des autorités de certification

325.2 Certificats X.509 pour le chiffrement, la signature et l'authentification

Comprendre SSL, TLS et les versions de ces protocoles
Comprendre les menaces communes sur TLS, par exemple Man-in-the-Middle
Configurer Apache avec mod_ssl pour fournir du HTTPS, en incluant SNI et HSTS
Configurer Apache avec mod_ssl pour authentifier les utilisateurs utilisant des certificats
Configurer Apache avec mod_ssl pour fournir le chaînage OCSP
Utiliser OpenSSL pour les tests serveur et client pour SSL/TLS

325.3 Système de fichiers chiffré

Comprendre les périphériques de type bloc et le chiffrement de système de fichiers
Utiliser dm-crypt avec LUKS pour chiffrer les périphériques de type bloc
Utiliser eCryptfs pour chiffrer les systèmes de fichiers, en incluant les dossiers du home et l'intégration de PAM
Connaître dm-crypt et EncFS

325.4 DNS et cryptographie

Comprendre DNSSEC et DANE
Configurer et dépanner BIND comme serveur principal pour des zones sécurisé avec DNSSEC
Configurer BIND comme serveur récursif pour effectuer des validations DNSSEC et pour le compte de ses clients
Key Signing Key, Zone Signing Key, génération de clé TagKey, stockage, gestion et renouvellement des clés
Maintenance et re-signature de zones
Utiliser DANE pour publier des informations de certificats X.509 dans le DNS
Utiliser TSIG pour sécuriser la communication avec BIND

Atelier : QCM à commenter sur le sujet 325

Sujet 326: Sécurité des hôtes

326.1 Sécurisation des hôtes

Configurer la sécurité du BIOS et du boot loader (GRUB 2)
Désactiver les services et les logiciels inutiles
Utiliser sysctl pour la configuration de la sécurité relative au kernel, particulièrement la configuration d'ASLR, Exec-Shield et IP / ICMP
Configuration d'Exec-Shield et IP / ICMP
Limiter l'utilisation des ressources
Travailler avec des environnements chroot
Supprimer les fonctionnalités inutiles
Connaître les avantages sur la sécurité de la virtualisation

326.2 Détection d'intrusion

Utiliser et configurer les audits système Linux
Utiliser chkrootkit
Utiliser et configurer rkhunter, avec les mises à jour
Utiliser Linux Malware Detect
Automatiser l'analyse des hôtes avec cron
Configurer et utiliser AIDE, avec la gestion des règles
Connaître OpenSCAP

326.3 Gestion des utilisateurs et authentification

Comprendre et configurer NSS
Comprendre et configurer PAM
Renforcer les stratégies de complexité de mots de passe et de changement périodique
Verrouiller automatiquement les comptes suite à des tentatives échouées
Configurer et utiliser SSSD
Configurer NSS et PAM pour les utiliser avec SSSD
Configurer l'authentification SSSD avec Active Directory, IPA, LDAP, Kerberos et des domaines locaux
Obtenir et gérer les tickets Kerberos

326.4 Installation de FreeIPA et intégration de Samba

Comprendre FreeIPA, avec son architecture et ses composants
Comprendre les pré-requis système et de configuration pour installer FreeIPA
Installer et gérer un serveur et un domaine FreeIPA
Comprendre et configurer la réplication Active Directory et les approbations Kerberos inter-domaines
Connaître l'intégration de sudo, autofs, SSH et SELinux integration avec FreeIPA

Atelier : QCM à commenter sur le sujet 326

Sujet 327: Contrôle d'accès

327.1 Contrôle d'accès discrétionnaire

Comprendre et gérer les permissions et propriétaire fichier, SUID et SGID inclus
Comprendre et gérer les ACL
Comprendre et gérer les attributs étendus et les classes d'attribut

327.2 Contrôle d'accès impératif

Comprendre les concepts de TE, RBAC, MAC et DAC
Configurer, gérer et utiliser SELinux
Connaître AppArmor et Smack

327.3 NFS

Comprendre les problèmes et amélioration de la sécurité de NFSv4
Configurer les serveurs et clients NFSv4
Comprendre et configurer les mécanismes d'authentification de NFSv4 (LIPKEY, SPKM, Kerberos)
Comprendre et utiliser le pseudo système de fichier de NFSv4
Comprendre et utlisier les ACLs de NFSv4
Configurer les clients CIFS
Comprendre et utiliser les extensions Unix CIFS
Comprendre et configurer les modes de sécurité de CIFS (NTLM, Kerberos)
Comprendre et gérer le mappage et la manipulation de ACLs CIFS et SIDs dans un système Linux

Atelier : QCM à commenter sur le sujet 327

Sujet 328: Sécurité réseau

328.1 Renforcement du réseau

Configurer FreeRADIUS pour authentifier les nœuds réseau
Utiliser nmap pour scanner les réseaux et hôtes, avec différentes techniques de scans
Utiliser Wireshark pour analyser le trafic réseau, avec les filtres et les statistiques
Identifier et traiter les annonces de routeurs et messages DHCP indésirables

328.2 Détection d'intrusion réseau

Mettre en place la supervision de l'utilisation de bande passante
Configurer et utiliser Snort, avec la gestion des règles
Configurer et utiliser OpenVAS, avec NASL

328.3 Filtrage de paquets

Comprendre l'architecture de base d'un pare-feu, DMZ inclus
Comprendre et utiliser netfilter, iptables et ip6tables, avec les modules standard
Mettre en place le filtrage de paquet sur IPv4 et IPv6
Mettre en place le suivi de connexion et de la translation d'adresse NAT
Définir des ensembles d'IP et les utiliser dans les règles de netfilter
Avoir des connaissance basiques sur nftables et nft
Avoir des connaissance basiques sur ebtables
Connaître conntrackd

328.4 VPN

Configurer et gérer un serveur OpenVPN et des clients pour des réseaux VPN de type 2 (bridged) ou 3 (routed)
Configurer et gérer un serveur IPsec et des clients pour des réseaux VPN networks utilisant IPsec-Tools et racoon
Connaître L2TP

Atelier : QCM à commenter sur le sujet 328