Collection Certifications

Préparation à la Certification **LPIC-3**

# LINUX

2ième édition

**EXAMEN LPI 300**

30 Travaux pratiques
168 Questions-réponses

**OFFERT :**
**UN EXAMEN BLANC en ligne**
avec réponses commentées et détaillées

eni éditions


**Issam MEJRIR**

Les éléments à télécharger sont disponibles à l'adresse suivante :
http://www.editions-eni.fr
Saisissez la référence ENI du livre CE2C3LIN dans la zone de recherche et validez.
Cliquez sur le titre du livre puis sur le bouton de téléchargement.

**Chapitre 3 Gestion des données et exploitation de l'annuaire**

**Chapitre 10 Samba et environnements hétérogènes**



**Chapitre 11 Installation et configuration de Samba**

# Chapitre 5

## Pré-requis

☒Connaissances de base sur la sécurité informatique.

☒Notions de base sur le chiffrement SSL.

☒Connaissances élémentaires sur le protocole Kerberos.

## Objectifs

À la fin de ce chapitre, vous serez en mesure de :

☒Sécuriser l'accès à l'annuaire à l'aide des certificats électroniques.

☒Configurer l'authentification SASL.

☒Maîtriser l'authentification Kerberos.

☒Mettre en place des ACL avancées.

☒Restreindre l'accès aux mots de passe au sein de l'annuaire.

☒Implémenter une politique de sécurité pour les mots de passe des utilisateurs de l'annuaire LDAP.

## A. Généralités sur la sécurité informatique

### 1. Objectifs de la sécurité

La sécurité des systèmes d'information est l'un des enjeux majeurs dans la vie de l'entreprise ainsi que dans sa résistance aux différents problèmes qu'elle peut rencontrer, tels que les attaques de l'extérieur, surtout lorsqu'une partie de son système d'information est relié à un réseau hostile comme Internet.

L'entreprise doit assurer aussi la confidentialité des informations et la documentation interne liée à ses employés ou à ses transactions avec le monde extérieur.

Une entreprise qui offre des services à travers le réseau doit faire face à toute cause d'indisponibilité de son système d'information.

Dans le contexte d'un service critique (serveur Web, serveur LDAP, mail, base de données), une panne occasionnant un arrêt du service peut causer un tort considérable entraînant une perte de productivité, voire une perte de confiance du client.

Les solutions de sécurité qui seront mises en place doivent contribuer à satisfaire les critères suivants :

- La disponibilité.
- L'intégrité.
- La confidentialité.

Ce sont les critères DIC.

Un autre critère important doit aussi être pris en compte dans les communications entre un client et un serveur, l'authentification.

## 2. La disponibilité

La disponibilité d'une ressource signifie que celle-ci doit être accessible à tout instant, et doit également être utilisable avec des temps de réponse acceptables.

La disponibilité des services système et données est réalisée en assurant un dimensionnement approprié et une certaine redondance et par une gestion opérationnelle efficace des infrastructures, ressources et services.

Dans une entreprise, des solutions comme les tests de montée en charge sont généralement effectués pour évaluer le comportement des systèmes sous certaines conditions extrêmes et contribuer ainsi à mieux définir leur dimensionnement.

Il faut néanmoins mettre en place une politique de sauvegarde permettant de restituer des données en cas de défaillance matérielle ou logicielle.

Des solutions de haute disponibilité existent pour assurer la continuité de service. L'étude détaillée de ces solutions dépasse les objectifs de cet ouvrage.

## 3. La confidentialité

La confidentialité est le maintien du secret des informations. La confidentialité peut être vue comme la protection des données contre une divulgation non autorisée.

Deux opérations permettent d'assurer la confidentialité des données :

- Limiter leur accès par un mécanisme de contrôle d'accès (ACL).
- Transformer les données par des procédures de chiffrement afin qu'elles deviennent inintelligibles aux personnes ne possédant pas les moyens de les déchiffrer.

  Le chiffrement contribue à assurer la confidentialité des données et à en augmenter la sécurité lors de leur transmission ou de leur stockage.

## 4. L'authentification

L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame.

Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a dotée.

Pour cela, l'identité devra produire une information spécifique telle que par exemple un mot de passe, un code ou une empreinte biométrique.

## 5. L'intégrité des données

Assurer l'intégrité de l'information est relatif au fait que des ressources de données, traitements, transactions ou services n'ont pas été modifiés, altérés ou détruits, tant de façon intentionnelle qu'accidentelle.

Lors de leur transfert, les données ne devraient pas être altérées par les protocoles de communication qui les véhiculent.

L'intégrité des données ne sera garantie que si elles sont protégées des écoutes actives qui peuvent modifier les données interceptées.

# B. Le chiffrement SSL/TLS - StartTLS

## 1. La cryptographie

La cryptographie a pour but d'assurer la confidentialité et l'intégrité des données.

La confidentialité est garantie par des algorithmes de chiffrement.

Le chiffrement est l'opération par laquelle on chiffre un message. C'est une opération de codage. Chiffrer ou crypter une information permet de la rendre incompréhensible en l'absence d'un décodeur particulier.

## 2. Les algorithmes de chiffrement

Les algorithmes de chiffrement sont divisés en deux grandes catégories :

- Le chiffrement symétrique.
- Le chiffrement asymétrique, dit à clé publique.

### a. Le chiffrement symétrique

Dans le chiffrement symétrique, une seule clé, qui sert pour le chiffrement et le déchiffrement, est partagée entre toutes les personnes participant à un échange.

Pour chiffre ou déchiffrer un texte, il faut définir une clé et un algorithme de chiffrement.

Chaque entité doit posséder autant de clés secrètes qu'elle a d'interlocuteur. Il faut donc disposer d'autant de paires différentes de clés qu'il y a de paires de correspondants.

Le tableau suivant liste quelques algorithmes de chiffrement symétriques :

| Algorithme | Taille de clé (en bits) | Taille de bloc |
|---|---|---|
| 3-DES | 112,168 | 64 |
| RC5 | 32, 64, 128 | Jusqu'au 2048 |
| AES | 128, 192, 256 | 128 |
| RC6 | Jusqu'à 2048 | 128 |
| Camelia | 128, 192, 256 | 128 |
| Serpent | 128, 192, 256 | 128 |

- DES (*Data Encryption Standard*) : avec cet algorithme les données sont chiffrées par bloc de 64 bits avec une clé de 56 bits.
- 3DES (*Triple DES*) : on réalise trois niveaux de chiffrement ce qui donne une clé effective de chiffrement de 168 bits.
- RC5 est un algorithme propriétaire à clé symétrique développé par Ronald Rivest et diffusé par la société RSA Security Inc. Il utilise des clés de longueur variable pouvant aller jusqu'au 2048 bits.
- Camelia est un algorithme de chiffrement symétrique par bloc de 128 bits, conçu pour fonctionner avec des clés de 128, 192 et 256 bits. Il a été développé conjointement par la Nippon Telegraph And Telephone corporation et Mitsubishi Electric Corporation en 2000.

Depuis 2006, le code source de Camelia est disponible sous plusieurs licences libres telles que GPL, BSD, MPL et la licence OpenSSL.

- Serpent : est un algorithme de chiffrement par bloc, serpent a une taille de bloc de 128 bits et supporte des clés de 128, 192 ou 256 bits.

  Serpent est souvent considéré comme l'un des systèmes de chiffrement les plus sûrs actuellement disponibles.

### b. Le chiffrement asymétrique

Dans le chiffrement asymétrique, il existe deux clés, une clé publique et une clé privée. Ces deux clés sont générées ensemble par un logiciel (exemple OpenSSL, GNUTLS) et elles dépendent mathématiquement l'une de l'autre.

La clé publique peut être publiée sans risque, mais la clé privée doit être soigneusement gardée secrète par son propriétaire.

La clé publique sert habituellement à crypter un message et la clé privée à le décrypter, mais l'inverse est également possible.

La cryptographie à clés publiques présente plusieurs avantages :

- Elle diminue le nombre de clés nécessaire à la communication entre un nombre important de personnes.
- Elle permet la signature d'un document numérique.
- Elle permet l'authentification mutuelle de deux composants.
- Les principaux algorithmes de chiffrement à clé publique, dont le nom est celui de leur inventeur, utilisent le plus souvent des clés de longueur variant de 512 à 1024 bits, citons par exemple :
  - RSA (*Rivest, Shamir, Adelman*) qui est basé sur la factorisation des nombres premiers.
  - El Gamal, basé sur la difficulté de résoudre le problème de logarithme discret.

☞*La sécurité du processus de chiffrement repose en grande partie sur la sécurité et la confidentialité des clés utilisées, sur la robustesse des algorithmes et sur la sécurité des plates-formes matérielles et logicielles qui les supportent.*

## 3. Le chiffrement SSL-TLS

Le protocole cryptographique SSL (*Secure Sockets Layers*) a été créé par la société Netscape en collaboration avec d'autres acteurs dont MasterCard et Bank of America pour prendre en charge des échanges sécurisés et authentifiés entre un client et un serveur. SSL peut être utilisé pour toute application reposant sur TCP, à l'instar de LDAP.

TLS (*Transport Layer Security*), le véritable nom pour SSLv3.1 décrit dans la RFC 2246, est la couche cryptographique qui se glisse entre TCP et LDAP pour sécuriser des échanges sur un lien non sûr.

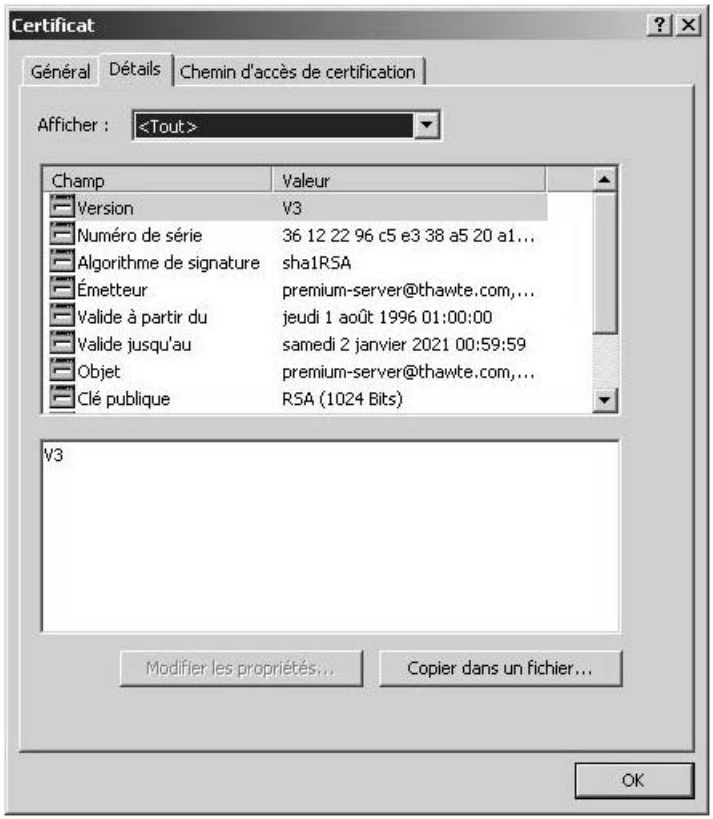
SSL permet de chiffrer les communications entre deux machines et d'assurer la confidentialité des données, l'authentification de l'utilisateur et du serveur, ainsi que l'intégrité des données par signatures électroniques à travers les certificats numériques et la mise en œuvre du chiffrement asymétrique.

Dans ce chapitre on s'intéresse particulièrement à la sécurisation du protocole LDAP et la configuration d'OpenLDAP à l'aide des certificats.

### a. Qu'est-ce qu'un certificat numérique ?

Un certificat numérique ou certificat électronique constitue la carte d'identité numérique d'une entité (personne morale ou physique) ou d'une ressource informatique à laquelle il appartient. Il contient entre autres l'identification de son propriétaire, la clé publique qui lui est attribuée ainsi que l'identification de l'organisme qui l'a délivrée.

Propriétés d'un certificat dans Internet Explorer :




### b. Mise en place de chiffrement par SSL dans LDAP

Pour mettre en place le chiffrement des échanges avec LDAP, il faut générer un certificat pour le serveur.

Pour créer ce certificat, il existe plusieurs façons :

- Créer un certificat auto-signé : ce type de certificat ne garantira pas l'identité de la source, mais permettra le chiffrement des échanges.