Sécurité des Systèmes d’Exploitatio – Résumé Académique Complet (Théorie + Labs)

Partie 1 : Fondamentaux de la Sécurité

Objectifs de la sécurité :

- **Protéger** : données, applications, systèmes, réseaux.
- **Prévenir** : menaces accidentelles et intentionnelles.
- **Garantir** :
  - **Authentification** : identifier l'utilisateur
  - **Confidentialité** : protéger les données
  - ✍ **Intégrité** : éviter les modifications non autorisées
  - **Non-répudiation** : ne pas nier une action
  - **Disponibilité** : accès aux services
  - **Traçabilité** : journalisation des actions

Vulnérabilités & Menaces :

| Terme | Définition | |-------|------------| | **Vulnérabilité** | Faiblesse du système (ex : mot de passe faible) | | **Menace** | Danger potentiel (pirate, feu, bug, utilisateur négligent) |

Types de menaces : - Naturelles : séisme, feu - ⚙ Techniques : pannes, bugs - Humaines : erreurs, piratage

Risques & Attaques :

| Terme | Explication | |-------|-------------| | Risque | Vulnérabilité + Menace | | Attaque | Risque intentionnel |

Objectifs d’une attaque : - Vol de données, contrôle, blocage (DoS), propagation (botnet)

Vecteur d’attaque : chemin utilisé
Surface d’attaque : ensemble des vecteurs

Attaques : Passive vs Active

- **Passive** : espionnage (écoute réseau)
- **Active** : modification/injection (ex : usurpation)

Logiciels Malveillants (Malware)

| Type | Fonction | |------|----------| | Virus | S'attache à un fichier | | Ver | Se propage seul | | Trojan | Logiciel déguisé | | Backdoor | Ouvre un accès caché | | Keylogger | Enregistre clavier | | Ransomware | Bloque accès | | Rootkit | Camouflage | | Botnet | Machine zombie | | Scareware | Fausse alerte |

Partie 2 : Défense et Mesures de Sécurité

StratégieDéfense en profondeur

- **Anticipation → Prévention → Détection → Réaction → Correction**

Protection de l’OS :

- Authentification obligatoire
- Droits d'accès (lecture, écriture, exécution)
- ACL (Access Control List)
- Sécurité au boot, BIOS, chargeur, verrouillage
- Politique de mots de passe (longueur, expiration)

Menaces sur l’OS :

- Accès physique non autorisé
- Clés USB contaminées
- Mauvaises configurations
- DoS/DDoS, usurpation (IP spoofing)
- Disque saturé, erreurs humaines

Bonnes pratiques :

| Type | Actions | |------|--------| | Physique | Contrôle accès, verrou BIOS | | Système | Mots de passe forts, comptes limités | | Réseau | Pare-feu, désactiver services inutiles | | Applicatif | Moindre privilège, sources officielles | | Intégrité | HIDS, surveillance fichiers système |

Partie 3 : Administration à Distance (SSH)

Objectif :

- Connexion sécurisée à distance : `ssh`
- Transfert sécurisé : `scp`, `sftp`
- Authentification forte avec clé publique/privée

Bonnes pratiques :

- Interdire `root` direct
- Changer le port 22
- Restreindre les IPs, groupes, utilisateurs

Commandes utiles :

```bash ssh-keygen -t rsa -b 4096 # Générer une clé ssh-copy-id user@serveur # Ajouter clé au serveur ```

Fichiers importants :

- `~/.ssh/authorized_keys`
- `/etc/ssh/sshd_config`

Partie 4 : Détection d’Intrusion (IDS/IPS)

| Type | Description | |------|-------------| | IDS | Détecte (ex : OSSEC) – passif | | IPS | Détecte + agit – actif |

Méthodes de détection : - Par **signature** (base connue) - Par **anomalie comportementale** - Par **état de protocole**
```

HIDS = OS local (ex : AIDE, OSSEC)
NIDS = Réseau (analyse trafic)

Honeypot = piège à pirates

Partie 5 : Intégrité des fichiers (AIDE)

AIDE (Advanced Intrusion Detection Environment)

- HIDS qui surveille les fichiers critiques

⚙ Commandes clés :

```bash yum install aide # Installation aide --init # Init base de données aide --check # Comparaison (détection) aide --update # Mise à jour base ```

LABS TECHNIQUES – Résumé par TP

LAB 1 – Certificats & PKI avec OpenSSL

Créer une autorité de certification (CA), générer et signer des certificats.

Commandes clés :

```bash openssl genrsa -out ca/fsb.key -des3 4096 openssl req -new -x509 -key ca/fsb.key -out ca/fsb.crt -config config/opensslca.cnf openssl genrsa -out certs/user.key -des3 2048 openssl req -new -key certs/user.key -out certs/user.req -config config/opensslmail.cnf openssl ca -config config/opensslmail.cnf -in certs/user.req -out certs/user.crt openssl pkcs12 -export -inkey certs/user.key -in certs/user.crt -out certs/user.p12 -certfile ca/fsb.crt openssl ca -revoke certs/user.crt -config config/opensslca.cnf ```

LAB 2 – Apache + mod_ssl (HTTPS)

Configurer Apache pour héberger un site sécurisé.

HTTPS + Authentification

```bash sudo yum install httpd modssl php openssl genrsa -out certs/server.key -des3 2048 openssl req -new -key certs/server.key -out certs/server.req -config config/opensslssl.cnf openssl ca -in certs/server.req -out certs/server.crt -config config/openssl_ssl.cnf sudo systemctl restart httpd ```

LAB 3 – Analyse TLS avec SSLyze

```bash pip install sslyze python -m sslyze www.demo.com ```

LAB 4 – VPN sécurisé avec OpenVPN

```bash sudo yum install openvpn openssl genrsa -out server.key -des3 2048 openssl req -new -key server.key -out server.req openssl ca -in server.req -out server.crt scp client.crt client.key fsb@IP:/home/fsb/ sudo yum install NetworkManager-openvpn ```

LAB 5 – S/MIME avec Thunderbird

Signer et chiffrer des e-mails avec certificat utilisateur.

Étapes :

1. Installer Thunderbird
2. Générer un certificat (`openssl_mail.cnf`)
3. Importer `.p12` dans Thunderbird
4. Activer la signature/chiffrement
5. Ajouter certificat destinataire

Déchiffrer avec OpenSSL :

```bash openssl smime -decrypt -in smime.p7m -inform DER -recip certs/user.crt -inkey certs/user.key -out clear.txt ```

Voir certificat Gmail :

```bash openssl sclient -connect imap.gmail.com:995 -showcerts openssl sclient -connect smtp.gmail.com:465 -showcerts ```
```