



ATELIER SI POUR ADMINISTRATEURS DE RÉSEAUX

Composantes d'un protocole sécurisé

A- Confidentialité

1. Cryptographie symétrique
 - 1.1 Concepts de la cryptographie par bloc (exemple détaillé : de DES à AES)
 - 1.2 Concepts de la cryptographie par flux (exemple détaillé : RC4)
 - 1.3 Problèmes de gestion des clés / solutions : Diffie-Hellman

2. Cryptographie asymétrique

- 2.1 Concepts de la cryptographie asymétrique
- 2.2 Algorithmes (exemple détaillé : RSA)

3. Cryptographie hybride

- 3.1 Concepts (exemple détaillé : PGP)

B- Authentification

1. Cryptographie

- 1.1 Concepts de certificats
- 1.2 Hachage cryptographique
- 1.3 Signature électronique

2. Protocoles d'authentification

- 2.1 Concepts (exemple détaillé : Needham-Schroeder et Kerberos)

Protocoles sécurisés

A- Exemple 1 : IPSec

B- Exemple 2 : SSL

C- Exemple 3 : WEP / WPA / WPA2

Mécanismes de protection courant

A- Coupe-feu

1. Niveaux de filtrage sans/avec états/applicatif
2. Bonnes pratiques pour une architecture sécurisée
3. Exemple détaillé : IPTables



B- Détecteurs d'intrusions

1. NIDS
 - 1.1 Capture de paquets
 - 1.1.1 Réception (ports de diffusion, taps, détournement, sans-fil)
 - 1.1.2 Analyse
 - 1.1.3 Exemple détaillé : Wireshark
 - 1.2 Signatures, heuristiques et comportementale
 - 1.3 Exemple détaillé : Snort
2. LIDS
 - 2.1 Journaux d'événements: formats, protocoles
 - 2.2 Exemple détaillé : Splunk
3. HIDS
 - 3.1 Qu'est-ce qui peut être monitoré?
 - 3.2 Exemple détaillé : OSSEC
4. Balayeurs de vulnérabilités
 - 4.1 Exemple détaillé : Nessus

Erreurs fréquentes

- A- Importance des mises-à-jour (exemple détaillé : Metasploit)
- B- Utilisation de protocoles sécurisés
- C- Limiter les accès au maximum (exemple détaillé : Shodan)
- D- Consoles Web et autres interfaces
- E- Mot de passe
- F- Divulgaration d'informations (exemple détaillé : NetBios et SNMP)

Portion théorique en matinée et pratique en après-midi.