I. Protection dans les réseaux

1. Les types d'attaques

a. Man in the middle

- L'attaquant se place entre deux victimes et intercepte les connexions. Il peut lire et modifier les messages.
- Les victimes croient parler entre elles.

b. DHCP snooping

- Fonctionnement :
  - DHCP Discovery (boadcast) : découverte du serveur DHCP
  - DHCP Offer : envoie des paramètres du seveur
  - DHCP Request :
  - DHCP xxx :
- Attaque :
  - Envoyer un DHCP Offer depuis un serveur DHCP pirate
- Solution :
  - Sur les switch, autoriser uniquement certains ports à émettre des requêtes DHCP.

c. Spoofing

- IP Spoofing :
  - Usurpation d'adresse IP
  - Utilité : falsifier la source d'une attaque pour ne pas être localisé
  - Utilité : profiter d'une relation de confiance entre machines
- ARP Spoofing :
  - Usurpation d'adresse MAC
  - Corromp le cache de la machine victime
  - Envoyer régulièrement des ARP REPLY en broadcast
  - Solution :
    - Controler les couples IP/MAC
    - Tables ARP statiques
- DNS Spoofing :
  - Rediriger la machine vers un faux service
  - DNS ID Spoofing
    - Modifier une demande entre PC et serveur DNS
  - DNS Cache Poisoning
    - Compromettre le cache du serveur DNS

d. Sniffing

- Collecter des infos en écoutant le réseau

e. DoS

Denial of service :

- Inonder une machine à faire tomber
- Mené à plusieurs (Distributed DoS)

- Solution : (Lourd à mettre en place / difficile à éviter)
    - Monitorer le trafic
    - Etablir des scénarios type

Buffer overflow :

- Exploite une faille programme pour écrire ailleurs que dans la zone mémoire.
- Solution :
    - Code propre / Appliquer les patchs de l'éditeur / Audit du code

Ping of death :

- Envoi de ping de taille supérieure à la normale => envoi fragmenté => la cible doit le reconstruire => blocage système.

SYN flood :

- Noyer la cible sous des demandes TCP SYN sans répondre au ACK du serveur.
- Solution : Limiter le nombre de connexion.

2. Protocoles

a. VLAN-ACP

- Réduction du domaine de broadcast
- Permet la mise en œuvre d'Access Control List (ACL) (Source, Destination, Port)

b. 802.1x

- Permet l'authentification dès l'accès physique au réseau
- Avant tout autre mécanisme (ex : DHCP)

c. QoS : Quality of Service

- Mettre des priorités sur les flux de donnée afin de garantir la performance.
- Ex : ToIP, VoIP, Téléconférence, streaming

d. VPN (Virtual Private Network)

- Infrastructure privée dans une infra publique
- Permet de relier à distance des réseaux de façon confidentielle (cryptage, tunneling).
- SSL (Secure Shell Layer) : canal entre applis. Utilise un navigateur comme client.
- PPTP, L2TP / GRE

3. Elements d'architecure

a. Pare-feu / UTM (Unifed Threat Management)

- Bloquer les accès non autorisés.
- Protéger le LAN d'internet.
- Définition de zones DMZ (Demilitarized Zones) : zones ou le pare-feu est moins actif (utile au niveau des serveurs qui vont sur internet).
- Pare-feu stateful : [AF]

b. Serveur radius (Remote Authentification Dial In User Service)

- AAA : Authentification / Authorization / Accounting
- Authentification des utilisateurs

II. Internet

1. Risques

- **Hoax :** Rumeur / pas de dégâts
- **Spam :** Pub non sollicité / pas de dégâts
- **Phishing :** Récupération de données perso
- **Virus :** Auto duplication / dégâts
- **Worm :** Auto duplication / pas de dégâts
- **Trojan Horse :** Ne se duplique pas / facilite l'accès à une machine
- **Spyware :** Collecte des infos perso

2. Eléments d'architecture

- **Proxy :** Transparent et authentifié. Intermédiaire. (Fourni cache, blacklist, etc.)
- **Reverse-proxy :** Récupère les connexions externes et les redirige vers l'intérieur
- **Serveur anti-virus :** centralise la gestion d'un anti-virus

III. Systèmes d'exploitation : solutions, possibilité, recommandations

- Materiel :
  - RAID, Cluster, Alim redondante
- Logiciel :
  - Privilèges : Pas de droit root aux utilisateurs
  - Firewall
  - Externaliser les logs, etc.

IV. Audit de sécurité

Supervision du réseau et supervision système. Détection d'intrusion.

V. Services de base de la sécurité

- Identification
- Authentification
  - Vérifier l'identité
  - Login + pass, carte à puce, biométrie
  - Méthode simple (auth d'un côté) / mutuelle (auth des deux côtés)
- Confidentialité (chiffrement)
  - Chiffrement symétrique (AES) / asymétrique (RSA)
- Intégrité des données (données non modifiées)
  - Chiffrement ou hash
- Non-répudiation
  - Preuve d'envoi et de réception (certificats (chiffré avec la clé privée, vérifié avec la clé publique))