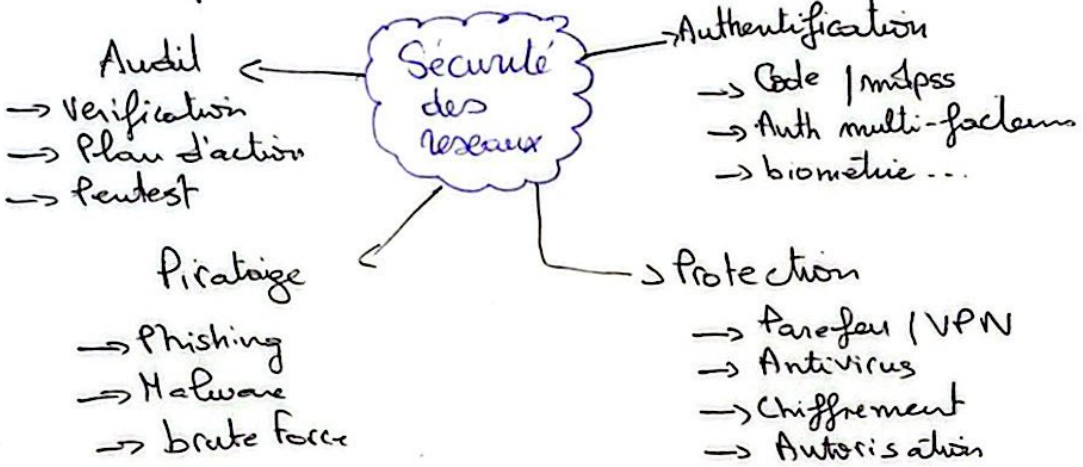
Chapitre 1

→ La sécurité des réseaux protège l'intégrité de l'infrastructure, des ressources et des informations afin d'empêcher les attaques et minimiser les répercussions financières et/ou opérationnelles.



La S.d.R peut être : Physique → Matériel, locaux
Informatique → logique et applicative
Communication → infrastructure réseau au niveau des protocole de comm
opérationnelle → Protéger les opération et les info échangées

Politique de Sécurité :

1) identifier ce qu'il faut protéger (les actifs)
2) Analyser et pondérer les risques.
3) évaluer les contraintes (budget, temps)
4) Choisir les moyens et opter pour un plan d'action
5) tester les mesures implémentés.

Cyberspace

→ Constitué de réseau et ressources informatiques, il s'agit d'un monde virtuel dans lequel les opérations s'effectuent de manière instantanée.
→ couche physique : infrast, matériels.
→ couche logique : services, logiciel ...
→ couche sémantique : les utilisateurs

Cyberattaque

→ tentative intentionnelle de voler, modifier, détruire des données par le biais de l'exploitation des vulnérabilité.
Prévention → Créer des politique de sécurité, app de surveillance.

Cybersecurity	VS	sécurité des réseaux
Protection contre Cybercrime		Protection contre les virus, les attaque
Sécurisé les S.I	≠	Sécurisés les données qui transitent
Sous ensemble de la Secu des SI		un sous ensemble de la Cybersecurity

Chapitre 2 :

Vulnerabilité :

→ Une Faiblesse qui pourrait être exploité par un acteur de menace.
comme → une faille materiel
→ " " humaine

Menace

→ exploitation d'une vulnérabilité par un acteur de menace.
comme vol d'information.

Risque

→ la probabilité qu'une faille de securité se produise et cause un impact sur les opérations de l'organisation.
comme, abus des droit d'auteur..

Analyse de vulnérabilité

il faut identifier les faiblesses dès le debut + surveiller en permanence les S.I
pour avoir une meilleure rentabilité il faut
→ Ameliorer la sécurité
→ Prioriser les risques
→ exiger la conformité

Gestion des Risques

→ C'est un processus permettant d'identifier les risques afin de selectionner les mesures de sécurité.

Identifier les actif → determiner l'objectif → Analyser les risques → définir les exigences → implementer les mesures

Politique → priorisation des risques → la gravité
→ criticité → frequence

Outils d'analyse des vulnérabilité

1 Openvas 2 NMAP 3 WireShark 4 Antivirus

1 → composé de plusieurs service et outils offrant l'analyse et la gestion des vulnerabilité

2) IP decouvre les hotes sur un reseau Tout en envoyant des paquets et en analysant leurs reponses

3) permet de voir tout le trafic qui transite sur une interface.

4) detection et le netoyage de virus
→ Scanne et analyse un support de Stockage
→ surveille le comportement en arriere plan

Bonne Pratique.

Analyse régulière, Gestion correcte, Priorisation des risques, integration avec les plans d'action.

Chapitre 4

Cryptologie ——> Cryptographie : méthode pour envoyer des données de manière confidentielle
└——> Cryptoanalyse : Retrouver le texte claire à partir des textes chiffrés en exploitant les failles des algo

Chiffrement ——> Substitution : Les lettres claires du text sont remplacées par d'autre lettres, chiffres, Symboles
└——> Transposition : l'ordre des lettres est modifié ——> permutation des lettres claires.

Ch.Symétrique : Avt : Simplicité, rapide, pas gourmand | Inc : le partage de la clé doit être securisé
text clair : + algorithme de ch = text chiffré
Clé serète : partagée entre 2 interlocuteurs ——> le text est chiffré et déchiffré avec la même clé
algorithme de dech : text chi + clé seciete ——> production du text original.

Ch. Asymétrique : Utilise une paire de clé distincte
clé privée : ne doit pas être partagée avec d'autres entités
clé publique : connue par toutes les entités qui veulent designer un destinataire spécifique.

Le partage de la clé publique n'induit pas l'identification de la clé privée ⚠
Une est utisée pour le chiffrement et l'autre pour le déchiffrement

Le chiffrement asymetrique est vulnérable à l'attaque MITM

Hachage : Appliquer une fonction mathématique à l'information en entrée et sa valeur de sortie s'appelle le hash
——> entrée de longueur variable et sortie de valeur fixe.
——> impossible de decouvrir le message à partir de la valeur de hash
——> Il d'avoir la même valeur de hash pour 2 messages differents

Avt : garantie d'integrité de données | Inc : il n'est pas tjrs possible de verifier l'identité de l'expéditeur

Signature électronique : l'envoie d'un message en le signant avec une clé privée

Pour se proteger contre l'attaque de MITM : il faut que chaque utilisateur confie sa clé public à CA
Chaque certificat a une periode de validité

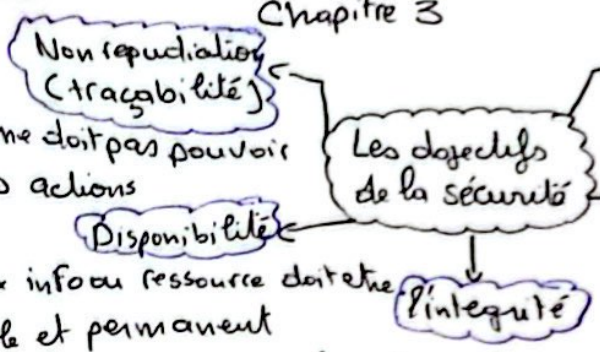
Pki : represente un système qui gere les clés public d'un S.I

Arch ——> Entité Finale : designe les utilisateurs finaux et consome les services fournies par PKI
——> CA : emetteur de certificat et des revocations
——> Autorité d'enregistrement : execute des fonctions facultatif du CA
——> Emetteur de CRL : publication de CRL.
——> Référentiel : designe toute methode de Stockage des Certif et CRL.

Mécanismes d'authentifications

——> CHAP ——> PPP
——> RADIUS ——> AAA
——> TACACS ——> AAA
——> KERBEROS

Chapitre 3



L'utilisateur ne doit pas pouvoir contester ses actions

Confidentialité : Seule la personne concernée peut connaître l'information

L'accès aux info ou ressource doit être disponible et permanent

l'authentification : Chaque personne faisant partie d'un échange est bien celui qui prétend de l'être.

les info ne doivent pas être altérées intentionnellement ou accidentellement

attaque → comportement → Active → modifier les actifs (Déni de service)
→ Passive → collecter les Info sans modifier les ressources
→ Position → interne → provient d'une entité à l'intérieur du périmètre
externe → " " de l'extérieur (SYN Flood) (Hameçonnage)

Attaques qui vise la CONFIDENTIALITÉ

Capture des paquet (Packet Sniffing) : l'attaquant peut capturer les paquet en cours de transmission et lire des données sensible comme les mdpss si le trafic n'est pas crypté

Balayage des ports : en scannant ces ports, l'attaquant peut exploiter le S.I

Balayage avec Ping : L'intrus envoie des paquet ping (ICMP) à une plage d'adresse pour voir laquelle elle répond → il identifie les utilisateurs du S.I.

Phishing et Pharming → 1 méthode de Piratage en envoyant des e-mail non sollicités
2 attaque réseau qui redirige le ~~site web~~ trafic vers un créer par l'attaquant
→ C + Authentification.

Keylogger : Programme qui s'exécute en A.Plan et enregistre les frapes de l'utilisateur → L'utilisateur saisie son mdps → celui-ci est enregistré dans un journal créé par le keylogger et envoyé à l'attaquant

attaque par mot de passe : L'attaquant cible les mot de passe.

ingénierie Sociale : il manipule les utilisateurs

→ Authentification :

USURPATION ARP : Permet de mapper une adresse IP à une adresse MAC

IP Spoofing : attaquant crée des paquet en cachant son identité ou en passant pour qlq d'autre

→ NON Répudiation :

Epuisement DHCP, ~~URD~~ USURPation DHCP

épuise les @ IP dispo dans le serveurs DHCP	déploie un serveur DHCP Pour envoyer des @IP aux clients

→ Disponibilité :

TCP SYN flood, Dos et DDos

→ intégrité :

Buffer overflow : se produit lorsque la qt de données dans la mémoire tampon dépasse le Stockage

XSS : injecte des données sur un site web pour affecter les utilisateurs.

SQL injection : il passe par des injections SQL afin de visualiser modifier ... les données