Introduction à la cybersécurité

1 – Cybersécurité

La cybersécurité protège :

- Les systèmes informatiques
- Les réseaux
- Les données

contre les attaques et accès non autorisés

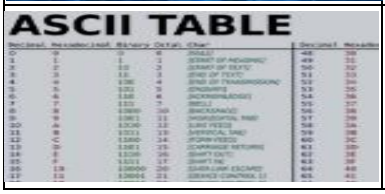
2 – Notions essentielles

Chiffrement

- Rend les données **illisibles sans clé** de chiffrement
- Types de clé :
  - Symétrique (AES)
  - Asymétrique (RSA)
- Objectif : **confidentialité des données**

Hachage :

- Transforme une donnée en empreinte unique (SHA)
- Non réversible
- Objectif : **intégrité des données**

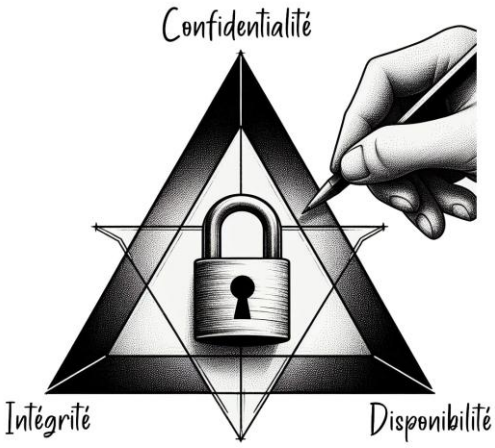


Codage

- Change le format (ex : Base64, codage ASCII)
- Réversible sans clé

❌ Ce n'est PAS de la sécurité

3 -Les piliers de la cybersécurité : CIA



CIA : **C**onfidentiality **I**ntegrity **A**vailability
CID : **C**onfidentialité **I**ntégrité **D**isponibilité

Confidentialité
Les informations sont accessibles qu'aux personnes autorisées.

Intégrité
L'intégrité assure que les données n'ont pas été modifiées (hachage).

Disponibilité
La disponibilité garantit que les informations et ressources sont accessibles aux utilisateurs quand cela est nécessaire.

4 – Vulnérabilités, menaces et actifs

En cybersécurité, votre mission est d'assurer la protection des **actifs** du réseau de l'entreprise en neutralisant toutes les vulnérabilités (faiblesses d'un système) pour éviter les menaces de personnes mal intentionnées.

Les actifs

- les données
- les serveurs (messagerie, fichier, …)
- les élément de l'infrastructures
- les périphériques finaux

Les vulnérabilités

- système désuet
- authentification faible (MdP = 123456, azerty, …)
- correctif logiciel absent
- infrastructure non conforme

Les menaces

- virus, rançongiciel
- piratage
- perte d'électricité, …

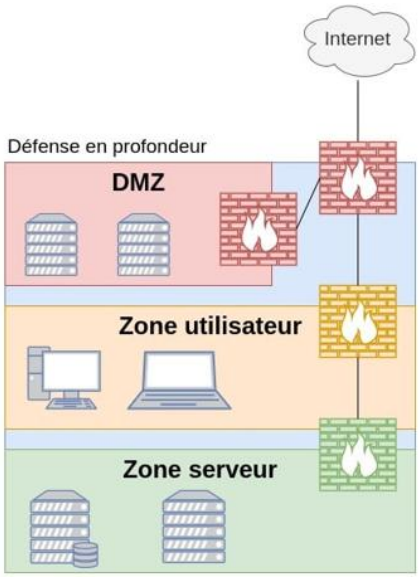
Exemples de vulnérabilités historiques et leurs implications modernes

Protocole ARP et IPv4 : ARP, crucial dans les réseaux IPv4, ne contient pas de mécanismes d'authentification, permettant des attaques de type ARP Poisoning. Avec l'adoption d'IPv6, ARP n'est plus utilisé, remplacé par NDP (Neighbor Discovery Protocol) qui intègre des fonctions de sécurité.

Protocole HTTP et le passage à HTTPS : Initialement, HTTP ne chiffrait pas les communications, exposant les données à des risques d'interception. La généralisation de HTTPS, intégrant SSL/TLS, marque une évolution vers des communications web sécurisées.

5 – La défense en profondeur

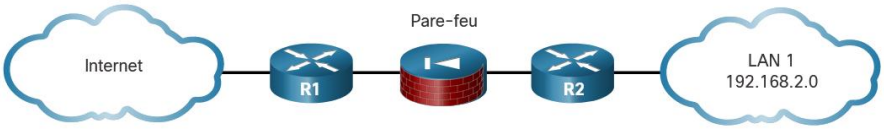
La défense en profondeur consiste à multiplier les protections de l'infrastructure d'une entreprise. L'idée, c'est de mettre en place plusieurs barrières pour décourager ou bloquer un hackeur (analogie : oignon / artichaut).



Exemples de barrières

- pare-feu
- DMZ (ou plusieurs DMZ)
- antivirus
- VPN
- segmentation réseau
- vérification des mises à jour
- sensibilisation des utilisateurs
- surveillance du trafic (sondes, IDS, IPS)
- Serveur AAA

Exemple de structure minimale



Routeur de périphérie : La première ligne de défense est appelée routeur de périphérie (R1). Le routeur dispose d'un ensemble de règles qui définissent le type de trafic autorisé ou refusé. Il transmet au pare-feu toutes les connexions destinées au réseau local interne.

Pare-feu : La deuxième ligne de défense est le pare-feu. Filtrage supplémentaire et suivi de l'état des connexions. Il empêche toute connexion entre les réseaux externes (non approuvés) et les réseaux internes (approuvés). Il peut également authentifier les utilisateurs pour permettre aux utilisateurs externes d'accéder aux ressources du réseau interne.

Routeur interne : Une autre ligne de défense est le routeur interne (R2). Il peut appliquer des règles de filtrage finales avant d'acheminer le trafic vers sa destination.

6 – Surveillance

Supervision des activités quotidiennes afin de maintenir un niveau élevé de sécurité dans toute l'entreprise.

- **Logs (journaux)** → Permet de voir ce qui s'est passé sur le réseau. Permet de déterminer comment une attaque s'est produite et quelles sont les défenses déployées qui ont réussi - et celles qui ont échoué.
- **Analyseur réseau** → surveiller le trafic, détection des tentatives d'intrusion, …
- **Configuration de référence** : Par exemple, tous les postes seront configurés de la même façon.

7 - La politique de sécurité

Les politiques de sécurité englobent diverses politiques : l'identification et l'authentification, les mots de passe, l'utilisation acceptable, l'accès à distance, la maintenance du réseau et la gestion des incidents.

8 – Les phases d'une attaque cyber

Attention !!!!

La phase de collecte en source ouvertes (passive) est légale. Si les scans sont actifs (interaction avec la cible) alors **c'est illégal** (sauf accord de la cible → Auditeur payé par l'entreprise).

Un scan de port sur une adresse IP dont on ne possède pas la propriété ou simplement le droit d'usage est illégal.

1 - Reconnaissance (Collecte d'infos)	**OSINT** – **O**pen **S**ource **INT**elligence - Utilisation de moteurs de recherche, réseaux sociaux et registres WHOIS pour obtenir des données publiques et identifier des vulnérabilités.
2 – Scan (Recherche de failles)	Identification des services ouverts, des systèmes d'exploitation et les applications. Recherche des vulnérabilités pour découvrir des failles exploitables. (Logiciel NMAP)
3 – Exploitation (attaque)	Exploitation de failles logicielles, ou utilisation de malwares pour obtenir un accès initial.
4 - Maintien de l'accès (Prise de contrôle)	Escalade des privilèges, création de backdoors, et pivotement pour exploiter d'autres systèmes internes afin d'obtenir un contrôle étendu sur les ressources de la cible.
5 – Exfiltration (Vol de données)	Extraction des données ou des ressources de valeur et effacement des traces pour éviter la détection.

```
# nmap -A -T4 scanme.nmap.org playground

Starting nmap ( https://nmap.org/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1002/tcp open  windows-icfw?
1025/tcp open  msrpc         Microsoft Windows RPC
1720/tcp open  H.323/Q.931   CompTek AquaGateKeeper
5800/tcp open  vnc-http      RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

Il faut systématiquement garder à l'esprit que l'ensembles des outils de scan et d'énumération actifs laissent des traces de leur passage.

Vous avez découvert dans les grandes lignes les principales phases d'une cyber-attaque, cette démarche est utilisée tant par les cybercriminels (Black Hat) que par les auditeurs/pentesters dans le cadre de leur métier (White Hat).

9 – Quelques exemples de métiers dans le domaine de la cybersécurité

— **Responsable de la Sécurité des Systèmes d'Information (RSSI)** : définit la politique de sécurité du SI.

— **Architecte (système, logiciel) sécurité** : structure les choix techniques, technologiques et méthodologiques.

— **Développeur de sécurité** : réalise des produits, des logiciels répondant à des exigences de sécurité.

— **Technicien ou Administrateur système et réseau** : assure ou est responsable de diverses activités de support, de gestion ou d'administration de la sécurité aux plans techniques ou organisationnel.

— **Auditeur** : contrôle les configurations des équipements et logiciels. Il est en mesure de tester les défenses d'un système d'information et d'identifier les divers chemins d'intrusions possibles et leurs conséquences. Il vérifie l'efficacité des mesures en place pour protéger le système.