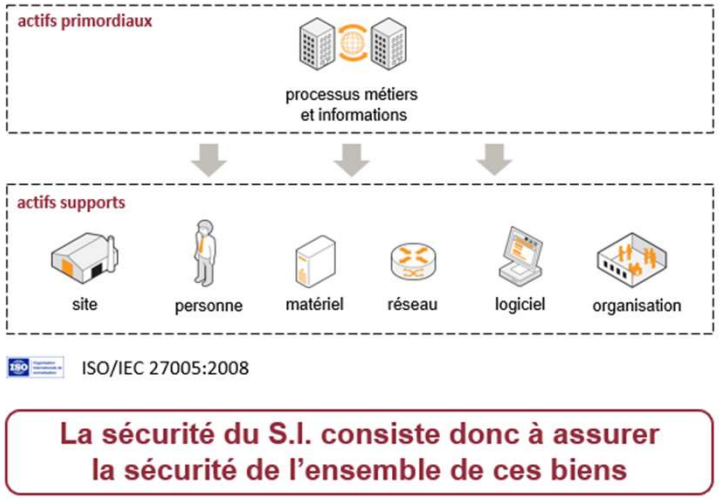
S'INITIER À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Introduction

- Un système d'information est une organisation d'activités consistant à acquérir, stocker, traiter, et diffuser les informations. Un des moyens techniques pour faire fonctionner un système d'information est d'utiliser des systèmes informatiques.
- Assurer la sécurité de l'information implique ainsi d'assurer la sécurité des systèmes informatiques.
- Le problème de la protection des informations sur les ordinateurs est devenu encore plus critique et difficile depuis l'adoption de l'Internet. L'Internet est devenu la route principale à la pénétration aux systèmes par des utilisateurs non autorisés qui peuvent effectuer des actions malveillantes.
- Il est donc essentiel de connaître les ressources du système à protéger et mettre en œuvre des mécanismes de protection.

- Le système d'information d'une organisation contient un ensemble d'actifs :



ISO/IEC 27005:2008

La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

Sécurité informatique : Introduction à la sécurité

1. Définitions

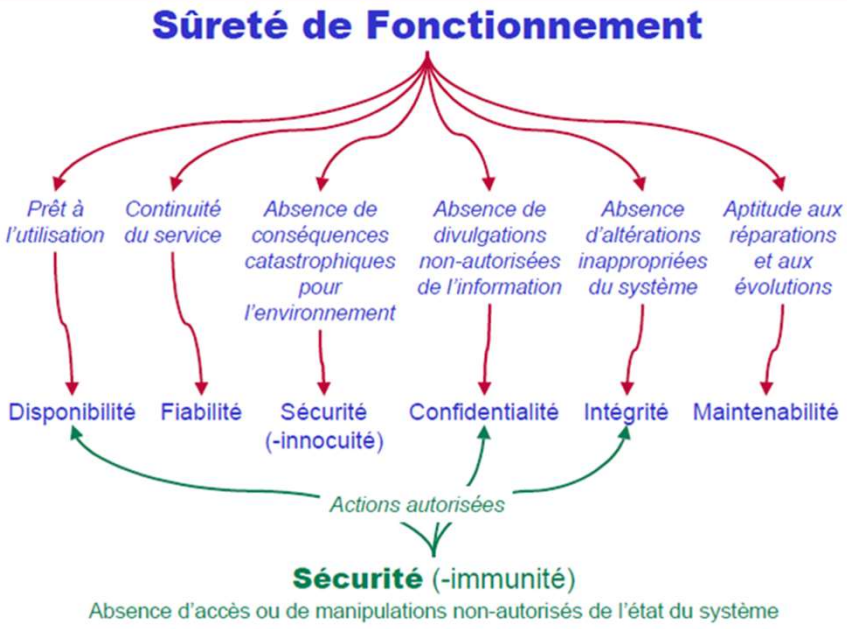
a) Sécurité informatique

C'est l'ensemble des moyens techniques, organisationnels, juridiques et humains mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

b) Sécurité et sûreté

La sécurité informatique concerne deux domaines :

- **« Sûreté = Safety (en anglais) » :** protection de systèmes informatiques contre les accidents dus à l'environnement et les défauts du système.
- **« Sécurité = Security (en anglais) »** : protection des systèmes informatiques contre des actions malveillantes intentionnelles.

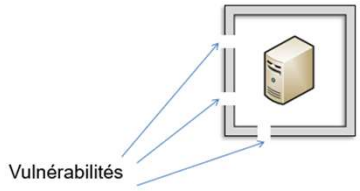


Sécurité informatique : Introduction à la sécurité

2. Principaux concepts de sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini. Afin de bien comprendre ces malveillances informatiques, il est nécessaire de définir certains termes :

• **Vulnérabilité :** une vulnérabilité (en anglais « vulnerability », appelée parfois faille ou brèche) est un point où un système est sensible à une attaque malveillante. Il s'agit d'une faiblesse de sécurité de nature logique ou physique pouvant être exploitée pour causer des pertes ou des dommages.



Vulnérabilité : Exemples

- Mots de passe et logins mal utilisés : mots de passe communs à plusieurs utilisateurs, transmission des mots de passe par email, mots de passe trop simple et trop peu renouvelés, etc;
- Logiciels ou systèmes d'exploitation : absence de mises à jour régulières;
- Télétravail et l'utilisation de matériel personnel : les équipements personnels ne disposent pas du même degré de sécurité que votre infrastructure d'entreprise;

2. Principaux concepts de sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini. Afin de bien comprendre ces malveillances informatiques, il est nécessaire de définir certains termes :

• **Menace :** une menace (en anglais « threat ») représente le type d'action malveillante susceptible de nuire à un système informatique en exploitant ses vulnérabilités (ses faiblesses) de sécurité. Une menace est un danger possible pour le système.

Menace : Exemples

- Logiciels malveillants : Le Trojan ou cheval de Troie, Les spywares, Les worms ou vers informatiques, etc;
- Piratage : pirates et hackers;
- Nature : Séisme, inondation, coupure d'électricité, incendie, etc;
- Pannes techniques.

2. Principaux concepts de sécurité informatique

• **Risque :** Il signifie la probabilité qu'une menace exploitera une vulnérabilité du système. La définition du risque dépend de la notion de menace associée ou non à des vulnérabilités. On peut formaliser le risque comme suit:

$$Risque = \frac{Menace \times Vulnérabilité}{Contre\ mesure}$$

Risque : Exemples

- **Risques humains : sont les plus importants et ils concernent les utilisateurs (souvent ignorés ou minimisés) :**
  - **L'accès illégitime ;**
  - **Le détournement de mot de passe;**
  - **Le vol de matériels.**
- **Risques techniques : sont liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels :**
  - **Incidents liés au matériel;**
  - **Incidents liés au logiciel;**
  - **Incidents liés à l'environnement.**
- **Risques juridiques :**
  - **Le non-respect de la législation relative à la signature numérique ;**
  - **Les risques concernant la protection du patrimoine informationnel;**
  - **Le non-respect de la législation relative à la vie privée;**

Sécurité informatique : Introduction à la sécurité

2. Principaux concepts de sécurité informatique

• **Contre-mesure :** c'est l'ensemble des actions mises en œuvre en prévention de la menace.

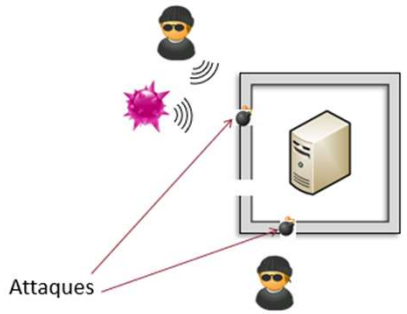
Contre-mesure : Exemples

- **Routeurs: masquer les adresses IP (Internet Protocol);**
- **Antivirus et anti-spyware: protection contre les logiciels malveillants (malware);**
- **Techniques comportementales: appliquées par les utilisateurs pour dissuader les menaces, telles que les pièces jointes suspectes;**
- **Pare-feu;**
- **Systèmes de détection et de prévention d'intrusion (IDS & IPS);**
- **VPN, ACLs, etc;**

2. Principaux concepts de sécurité informatique

• **Attaques :** Une attaque est une tentative volontaire de violer une ou plusieurs propriétés de sécurité.

• **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente **la concrétisation d'une menace**, et nécessite **l'exploitation** d'une **vulnérabilité**.



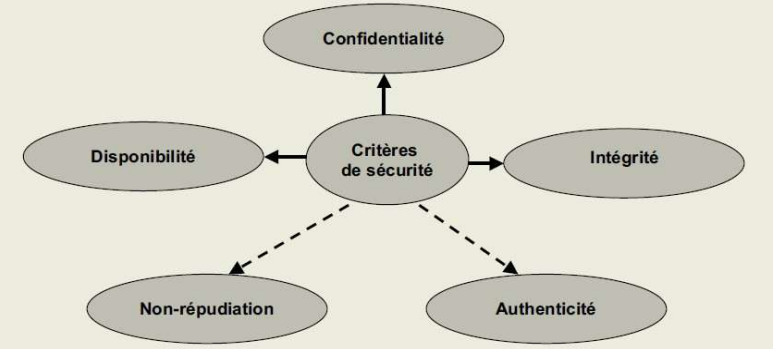
Les objectifs de la sécurité informatique

Les objectifs de la sécurité informatique correspondent aux attentes des utilisateurs en matière de protection des systèmes et des données. Ils définissent ce que la sécurité doit garantir dans un système informatique.

3. Objectifs de la sécurité informatique

Les objectifs (propriétés, exigences, services,, …) de la sécurité informatique caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité.

Cinq principaux objectifs à garantir :



1. Confidentialité

C'est la propriété qui assure que seuls les utilisateurs autorisés, dans des conditions prédéfinies, ont accès aux informations. C'est-à-dire garder les informations secrètes sauf pour les personnes auxquels elles sont destinées. L'un des moyens pour garantir la confidentialité des données est le chiffrement des données et la cryptographie.

2. Authentification

C'est la propriété qui assure la vérification et la confirmation de l'identité des entités qui s'échangent des informations, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Parmi les moyens utilisés pour garantir l'authentification sont les login/mot de passe, certificats numériques, etc.

Sécurité informatique : Introduction à la sécurité

3. Intégrité

C'est la propriété qui assure que les données ne sont pas corrompues ni modifiées de façon non autorisée. L'un des moyen pour assurer l'intégrité est l'utilisation des empreintes digitales.

4. Disponibilité

C'est la propriété qui assure que les données ou les services d'un système sont accessibles au moment voulu par les utilisateurs autorisés.

5. Non répudiation

C'est la propriété qui assure que l'auteur d'un acte ne peut ensuite nier l'avoir fait, il en assume la responsabilité. Par exemple empêcher l'émetteur ou le récepteur de nier la transmission ou la réception d'un message.

Le Cube de McCumber

Le cube de McCumber (également appelé cube de la sécurité informatique) est un outil développé par John McCumber afin d'aider à gérer la protection SI;

Ce cube a trois dimensions (3 façades);

Il répond aux trois questions suivantes :

Quels sont les objectifs de la SI ?

Quand les vérifier ?

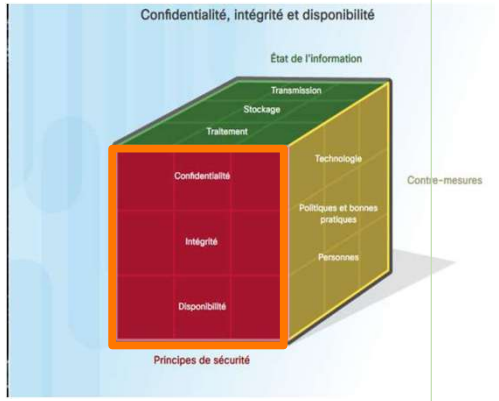
Comment les assurer ?

John McCumber
UCLA European Languages & Transcultural Studies

8

Les principes de la sécurité

La première dimension du cube de la cybersécurité identifie les objectifs identifiés précédemment et qui sont les principes fondamentaux de la triade de la **CID**. Notamment **la confidentialité, l'intégrité et la disponibilité.**



Le Cube de McCumber est conçu pour répondre à la sécurité informatique.
Le contour orange entour la face des **principes de la sécurité**

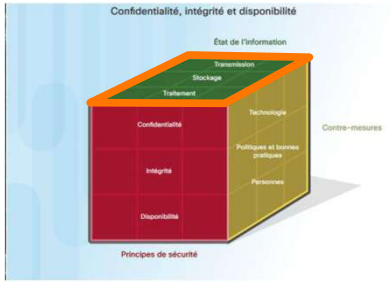
Les états de l'information

La deuxième dimension du Cube de la sécurité informatique traite le problème de la protection des données durant ces différentes états possibles :

Transmission : transfert de données entre systèmes d'information - également appelé données en transit

Stockage : Données au repos , telles que celles stockées en mémoire ou sur un disque dure.

Traitement : réalisation d'opérations sur des données afin d'atteindre un objectif souhaité.



états de l'information

Copyright - Tout droit réservé - OFPPT

Le Cube de McCumber est conçu pour répondre à la sécurité informatique.
Le contour orange entour la face des

Les états de l'information

État	Description	Exemples
DAR (Data at Rest)	Données stockées (inactives).	Fichiers sur un disque dur, base de données, sauvegarde.
DIA (Data in Action)	Données en cours de **traitement** (utilisation active).	Données dans la RAM pendant un calcul, CPU qui exécute un algorithme.
DIT (Data in Transit)	Données en **transmission** (déplacement).	E-mail envoyé, flux réseau (HTTP, FTP), VPN.

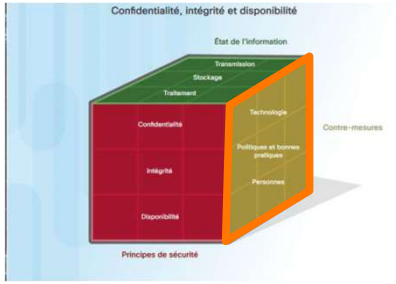
Pourquoi ces états sont-ils importants ?

Mesures de protection de la cybersécurité (Contre-mesures)

La troisième dimension du cube de McCumber définit les compétences et les disciplines auxquelles un professionnel de la sécurité informatique peut faire appel. Tout en veillant toujours de rester du "bon côté" de la loi.

Ces compétences et disciplines sont :

- **Politiques et bonnes pratiques** : contrôles administratifs, tels que les directives de gestion, qui fournissent une base pour la mise en de l' assurance de l'information au sein d'une organisation. (exemples : politiques d'utilisation acceptable ou procédures de réponse aux incidents) - également appelées opérations .
- **Personnes** : s'assurer que les utilisateurs des systèmes d'information sont conscients de leurs rôles et responsabilités en matière de protection des systèmes d'information et sont capables de suivre les normes.
- **Technologie** : solutions logicielles et matérielles conçues pour protéger les systèmes d'information (exemples : antivirus, pare-feu, systèmes de détection d'intrusion, etc.)



*Le Cube de McCumber est conçu pour répondre à la sécurité informatique. Le contour orange entour la face des **Contre-mesures***

Tous droit réservé - OFPPT

Les Mesures de Protection (3 Catégories)

Pour atteindre les objectifs CID, on combine 3 types de mesures :

Catégorie	Description	Exemples
Technologiques	Solutions logicielles/matérielles.	Firewalls, antivirus, IDS/IPS, chiffrement, biométrie.
Politiques	Règles et procédures formelles.	Politiques de mot de passe, audits, normes (ISO 27001, RGPD).
Humaines	Formation et sensibilisation des utilisateurs.	Anti-phishing, bonnes pratiques, gestion des accès (principe du moindre privilège).

4. Classification des menaces

Avant de pouvoir mettre en œuvre une solution de sécurité, il faut d'abord commencer par connaître les différents dangers et leurs motivations afin de prévoir la façon de les protéger et limiter les risques.

Les différentes menaces qui existent peuvent être classifiées selon plusieurs classes :

- **selon la technologie,**
- **selon l'intention,**
- **selon le comportement,**
- **selon l'action.**

1. La classification selon la technologie

1. Menace non Informatique

• **Risques matériels accidentels :**

Incendie, explosion, inondation, tempête, foudre.

• **Vol et sabotage de matériels :**

Vol d'équipements matériels, destruction d'équipements, destruction de supports de sauvegarde.

• **Autres risques :**

Tout ce qui peut entrainer des pertes financières dans une société. Pertes plutôt associées à l'organisation, à la gestion des personnels (départ de personnels stratégiques, grèves, etc.).

4.1. La classification selon la technologie

2. Menace Informatique

Une menace informatique représente un danger lié aux ressources techniques. Ces types de menaces sont les plus courantes et représentent parfois les plus grands dangers pour la réalisation d'une attaque.

Exemples : virus, panne de serveurs, …

4.2. Classification selon l'intention

1. Menaces non intentionnelles

Les menaces non intentionnelles sont les menaces qui sont réalisées de façon accidentelle sans préméditation ou l'intention de nuire. Elles peuvent être :

- Des pannes ou dysfonctionnements matériels.
- Des pannes ou dysfonctionnements logiciels.
- Des erreurs : ces erreurs regroupent :
  - ✓Les erreurs d'exploitation : comme les oublis de sauvegarde.
  - ✓Les écrasements de fichiers.
  - ✓Les erreurs de manipulation des informations.
  - ✓Les erreurs de saisie.
  - ✓Les erreurs de transmission.
  - ✓Les erreurs de conception des applications.

4.2. Classification selon l'intention

2. Menaces Intentionnelles

Les menaces intentionnelles sont réalisées dans l'intention de nuire. Elle regroupe l'ensemble des actions malveillantes faites de façon délibérée (Malveillance Informatique).

Exemple :

Virus, Vers, Cheval de Troie, logiciel espion, spam, ...

4.3. Classification selon le comportement

1. Menaces Actives

Ce type de menaces implique la modification ou création des données ou des messages, afin d'introduire de fausses informations ou perturber le bon fonctionnement d'un système. Une menace active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ce type de menaces, bien qu'elles soient détectables (permettant ainsi une réponse adéquate).

Exemples :

- Virus qui détruit des données,
- Modification d'un e-mail par une tierce personne, . . .

4.3. Classification selon le comportement

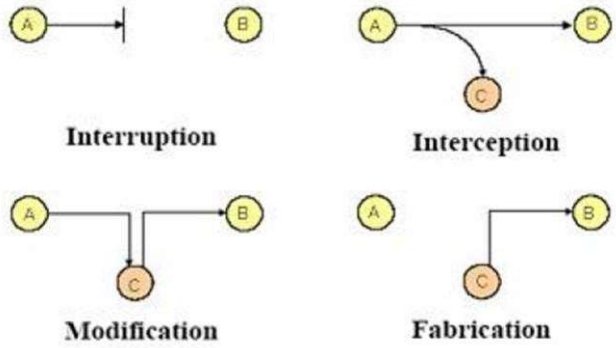
2. Menaces Passives

Une menace passive est une attaque qui ne modifie pas l'état des données ou du système. Elle consiste à écouter sans modifier les données ou le fonctionnement du système. Elles sont généralement indétectables mais une prévention est possible.

Une menace passive est souvent réalisée afin d'obtenir des données par écoute indiscrètes ou surveillance des transmissions.

4.3. Classification selon l'action

Cette classe de menaces regroupe les types répertoriés selon l'action effectuée lors de la réalisation de la menace. Il affecte le processus de communication et regroupe les menaces suivantes :



4.3. Classification selon l'action

1. Menace d'interruption

Un composant du système devient inutilisable ou inaccessible, empêchant le bon fonctionnement du service. Cela bloque la communication et entraîne une perte de ressources.

Exemple:

- Une attaque par déni de service (DDoS) qui surcharge un serveur jusqu'à ce qu'il devienne indisponible.
- Une coupure de courant qui rend un système informatique hors service pendant un certain temps.

2. Menace d'interception

Une personne ou un système non autorisé accède aux données pendant leur transmission. Cela compromet la confidentialité de l'information.

Exemples :

- Un pirate intercepte les données envoyées par Wi-Fi non sécurisé, comme des mots de passe.
- Une écoute clandestine sur un réseau (sniffing) qui capte les informations échangées entre deux ordinateurs.

Sécurité informatique : Introduction à la sécurité

4.3. Classification selon l'action

3. Menace de modification

Un attaquant accède à des données et les modifie sans être détecté. Le message reçu est altéré, ce qui affecte son intégrité.

Exemples :

- Un attaquant modifie les données d'une transaction bancaire en changeant le montant ou le destinataire.
- Une personne altère un fichier de configuration système pour en modifier le comportement à son avantage.

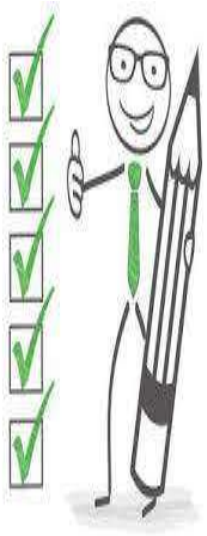
Menace de fabrication

Un intrus crée ou injecte de fausses données dans le système. Cela induit en erreur les destinataires en leur faisant croire qu'elles viennent d'une source légitime.

Exemples:

- Un pirate envoie de faux messages e-mail semblant provenir d'une source fiable (phishing).
- Un logiciel malveillant génère de fausses alertes système pour tromper l'utilisateur.

Exercice 1



1. Définir les notions suivantes : Vulnérabilité, menace, risque et contre mesure.
2. Ecrire et commenter la formule de risque.
3. Proposer un scénario englobant une vulnérabilité, une menace, un risque et une contre-mesure.
4. Comparer le système informatique et le système d'information.
5. Détailler les 03 objectifs de la SSI.
6. À quoi sert le cube de la sécurité informatique ?
7. Expliquer les trois dimensions de ce cube.

Sujet 1: Attaques informatiques et ses types (DoS, DDoS & MITM)

Sujet 2: Injection SQL, XSS

Sujet 3: Logiciel malveillant (Virus informatique, Virus vs ver, Virus infectant les fichiers & macro-virus, Virus pirate de navigateur & virus polymorphe, Copyright & BMDA, Rootkits)

Sujet 4: Terminologie (Cryptographie, cryptanalyse, cryptologie & cryptolecte Chiffrement, cryptage, cryptogramme & cryptosystème)

Sujet 5: Chiffrement symétrique, Chiffrement asymétrique & Fonctions de hachagen, Chiffrement de César , Chiffre de Vigénère

Sujet 6: Pare-feu et ses types, Principe de fonctionnement des firewallsn, Pare-feu applicatif, WAF,NGFW (Pare-feu de la nouvelle génération)

Attaque informatique

- une attaque informatique (ou cyberattaque) est une tentative sous de forme d'actions offensives afin d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé;
- Une intrusion est une attaque informatique réussie;
- Différents types de cyberattaques : DoS, DDoS, MITM, Hameçonnage, Injection SQL, XSS & Rootkits, etc.

Attaque informatique : DoS (1)

- DoS : Denial of Service (Déni de service);
- Dans cette attaque, l'attaquant effectue un nombre massif de requêtes dans le but de submerger les ressources d'un système ou une application pour le rendre indisponible;
- Le DoS est une attaque entre deux machines individuelles (l'attaquant utilise une seule machine pour mener l'attaque);
- Pour se protéger contre ce type d'attaque : Adoption de la redondance.

Attaque par Inondation (Flooding)

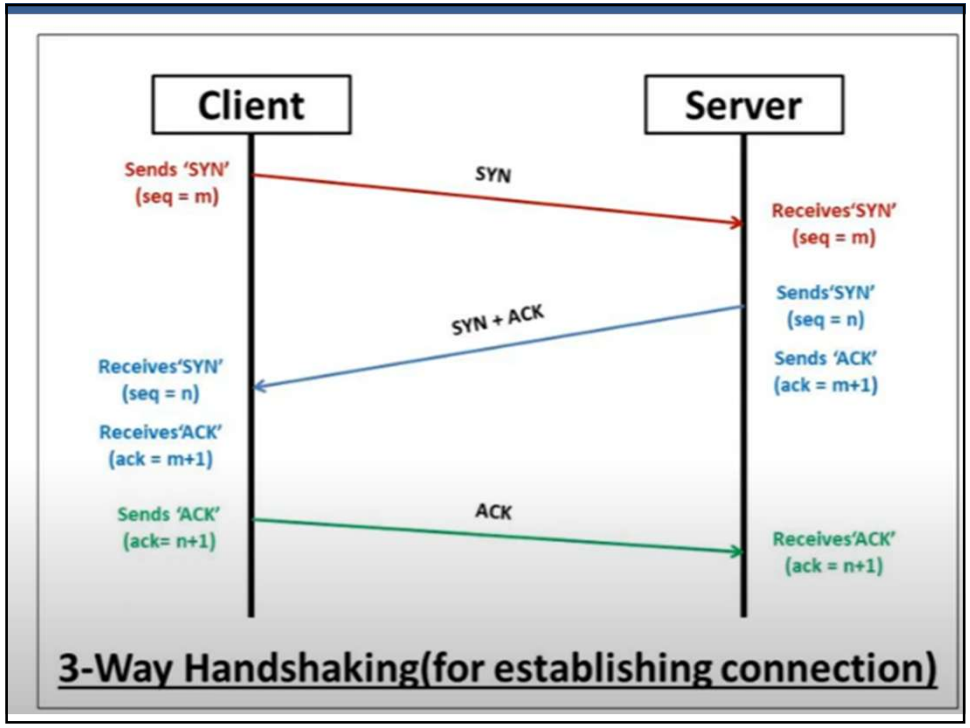
Submerger une cible avec un trafic massif pour saturer ses ressources (bande passante, CPU, mémoire).

Ex :

SYN Flood : Envoi de nombreuses requêtes TCP/SYN non terminées pour épuiser les connexions du serveur.

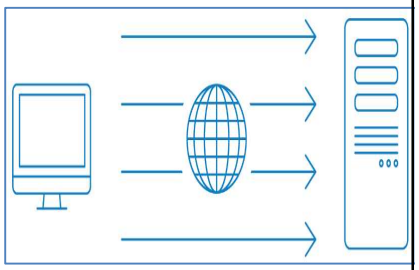
UDP Flood : Envoi de paquets UDP vers des ports aléatoires pour surcharger la cible.

HTTP Flood : Requêtes HTTP légitimes mais massives (via des bots) pour épuiser un serveur web.



Attaque informatique : DoS (1)

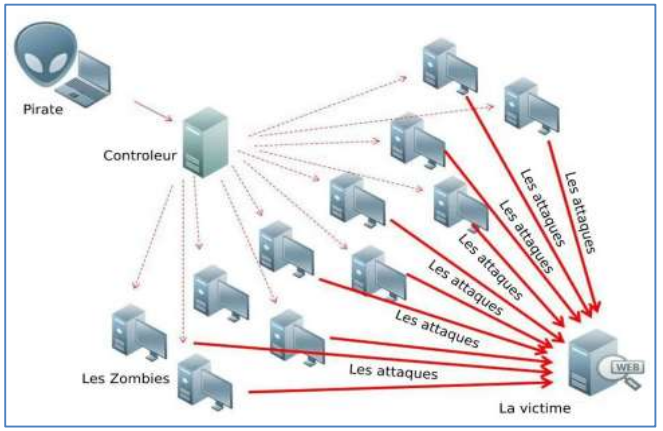
- **Une seule machine envoie un flot de trafic pour saturer une cible et la rendre indisponible.**
- **SYN Flood (Inondation de SYN) :**
- **Un pirate envoie des milliers de demandes de connexion (paquets SYN) à un serveur, mais ne complète jamais la connexion.**
- **Effet : Le serveur attend indéfiniment des réponses, épuisant ses ressources et bloquant les connexions légitimes.**



Attaque informatique : DDoS (1)

- DDoS : Distributed Denial of Service (Déni de service distribué);
- Une attaque DDoS (attaque de déni de service distribué) a aussi le même concept de submerger les ressources d'un système, mais elle est exécutée à partir d'autres machines hôtes infectées par un logiciel malveillant (Zombies) contrôlées par l'attaquant;
- Pour se protéger contre ce type d'attaque : Adoption de la redondance.

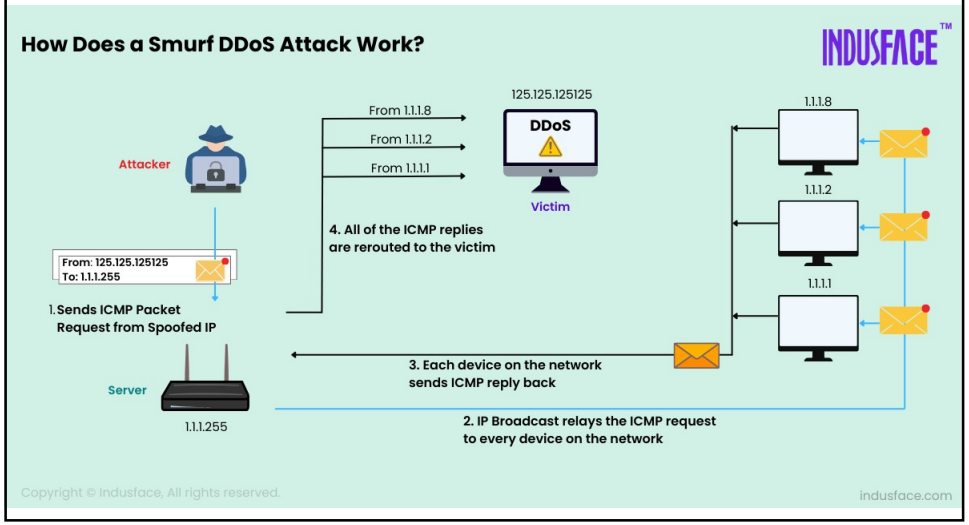
Attaque informatique : DDoS (1)



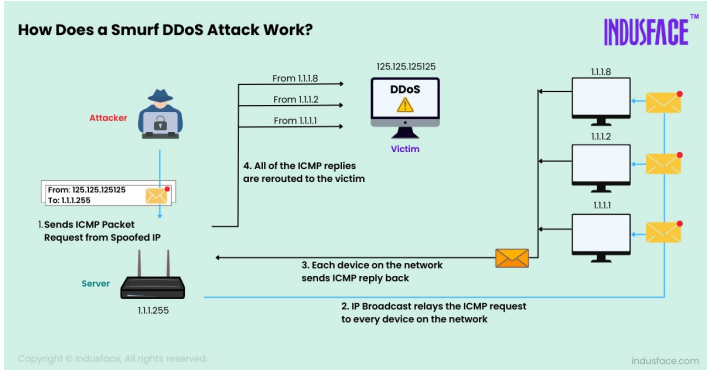
Attaques Protocolaires (Épuisent les ressources du serveur)

Smurf Attack : Le pirate envoie des paquets ICMP (ping) avec une IP usurpée à un réseau diffus.

Effet : Tous les appareils du réseau répondent à la victime, l'écrasant sous les réponses.



Attaques Protocolaires (Épuisent les ressources du serveur)

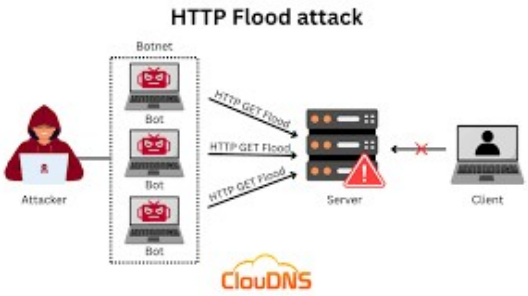


hping3 --icmp --spoof <IP_VICTIME> <ADRESSE_BROADCAST> --flood
--icmp : Utilise le protocole ICMP (ping).
--spoof : Usurpe l'IP source.
--flood : Envoi massif sans attendre de réponses.

Attaques de la Couche Applicative

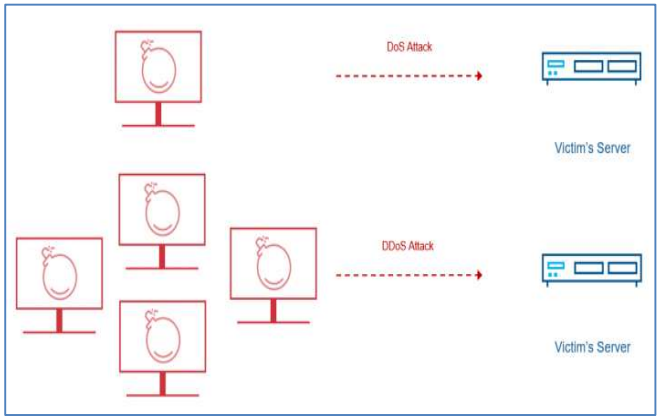
Des bots envoient des milliers de requêtes HTTP (comme des rafraîchissements de page) à un site web.

Effet : Le serveur web s'effondre sous la charge, comme lors du Black Friday sur un site mal préparé.

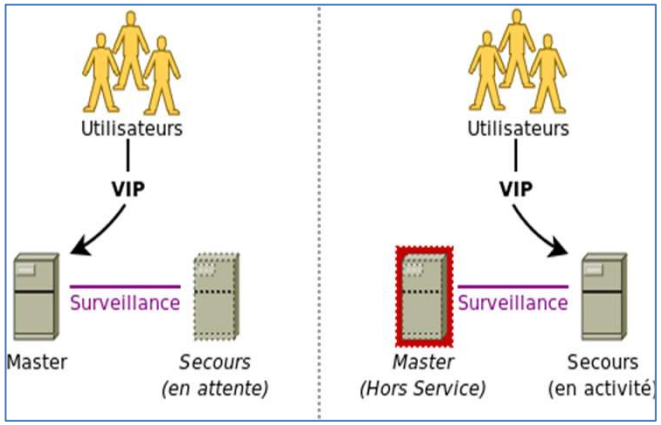


hping3 -S -p 80 --flood --rand-source <IP_CIBLE>
-S : Envoie des paquets SYN (simule des connexions HTTP).
-p 80 : Cible le port HTTP.
--rand-source : Génère des IP sources aléatoires (pour simuler un botnet).

Attaque informatique : Dos vs DDoS



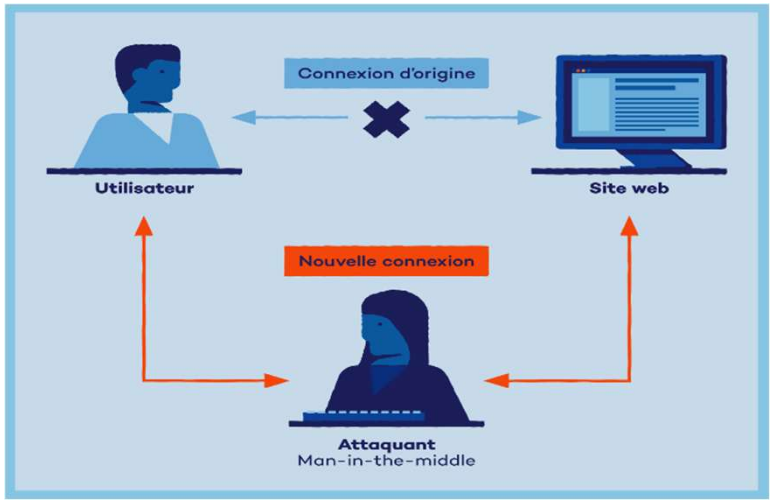
Attaques Dos & DDoS : Protection



Attaque informatique : MITM (1)

- MITM : Man In The Middle (L'homme du milieu);
- L'attaque MITM, parfois appelée attaque du monstre du milieu (monster in the middle attack) ou attaque de l'intercepteur;
- Elle est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été compromis;
- Ce type d'attaque viole la confidentialité des données;
- Pour se protéger contre une attaque MITM : Chiffrement.

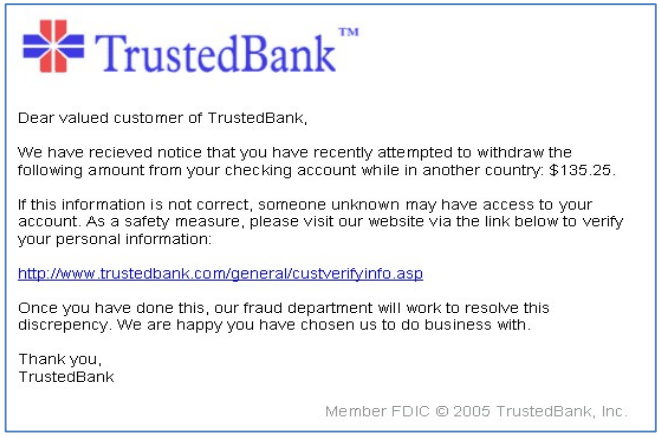
Attaque informatique : MITM (2)



Attaque informatique : Hameçonnage (1)

- L'hameçonnage (phishing ou fishing en anglais) est une technique frauduleuse destinée à leurrer les gens pour communiquer leurs données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance;
- Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc;
- L'hameçonnage est la forme de cyberattaque la plus simple et, en même temps, la plus dangereuse et la plus efficace.

Attaque informatique : Hameçonnage (2)



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Hameçonnage : Protection

- **Ne communiquez jamais d'informations sensibles par messagerie ou téléphone;**
- **Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien et vérifiez l'adresse du site qui s'affiche dans votre navigateur;**
- **En cas de doute, contactez si possible directement l'organisme concerné.**

Injections SQL

Les types de failles et attaques

les différents types de cyberattaques

Injections SQL :

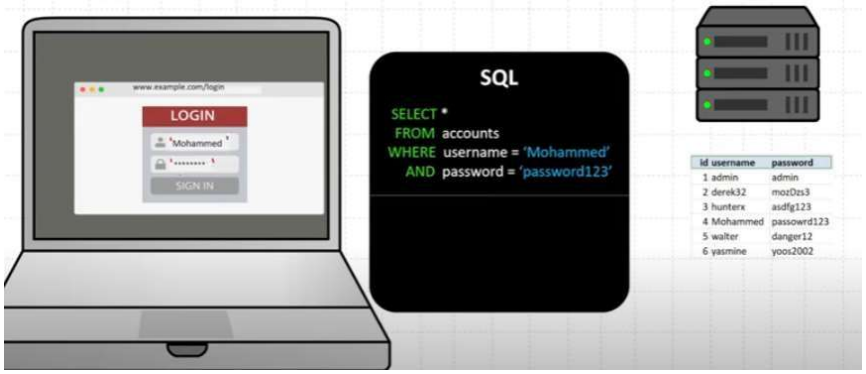
- L'injection SQL est une technique d'attaque courante utilisée pour compromettre la sécurité des bases de données. Cette attaque exploite les vulnérabilités des applications Web qui n'effectuent pas correctement la validation et la manipulation des entrées utilisateur. (exemple app web)

Les injections SQL sont généralement considérées comme critiques car elles permettent :

- **de récupérer (voire de modifier) le contenu de la base de données, notamment les identifiants, mots de passe, ou leurs hashs ;**
- **et pire encore, en fonction du moteur de base de données utilisé (MySQL, Oracle, MS SQL), de prendre le contrôle du serveur (via une Remote Code Execution, ou "RCE").**

Les types de failles et attaques

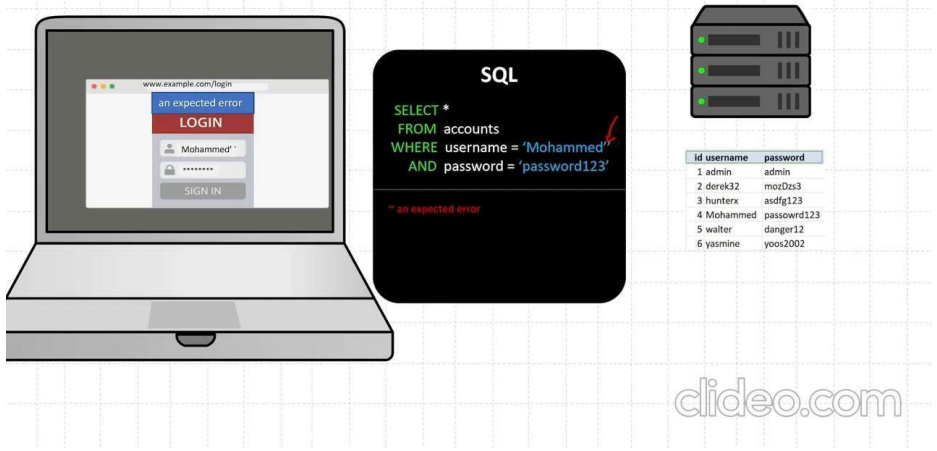
- Comment ça fonctionne une injection SQL ?



Les types de failles et attaques

- Le principe de l'injection SQL consiste à modifier la requête SQL qui va être envoyée.
- Comment on modifie une requête SQL ?
- En injectant des caractères spéciaux SQL dans le ou les champs qui seront pris en paramètre pour construire la requête SQL

ELHASSANI Mustapha



Méthode 1 : Contournement d'authentification

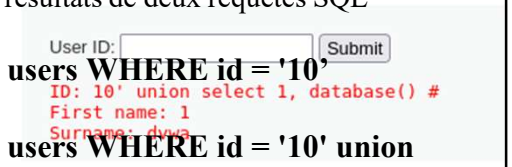
Dans le champ **username**, entrez : ' OR '1'='1' --
Laissez le mot de passe vide ou mettez n'importe quoi.
Cette injection transforme la requête SQL en :
SELECT * FROM utilisateurs WHERE username = '' OR '1'='1' -- ' AND password = '...'

- Le -- commente le reste de la requête, et '1'='1' est toujours vrai, ce qui permet de se connecter sans mot de passe.

Méthode 2 : Vol de données

10' union select 1, database()

union select : UNION combine les résultats de deux requêtes SQL
Requête originale
SELECT id, username FROM users WHERE id = '10'
Après injection
SELECT id, username FROM users WHERE id = '10' union select 1, database() #'



révéler la structure complète de la BDD

Cartographier la base de données :

06' union select 1, table_name from information_schema.tables # : Obtenir la liste complète des tables pour cibler celles contenant des données sensibles.

Identifier les colonnes sensibles

10' union select 1,column_name from information_schema.columns where table_name='users' # : Trouver des noms comme password

Blind SQL Injection

L'attaquant ne voit pas les données directement, mais déduit les informations en analysant le comportement de l'application (temps de réponse, erreurs conditionnelles, etc.).
Types :
Blind Booléenne : L'application répond différemment (vrai/faux).
' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='admin')='a' –
Si la page réagit différemment, le 1er caractère du mot de passe est 'a'.
Blind Temporelle (Time-Based) : L'attaquant utilise des délais (SLEEP(), WAITFOR DELAY).
'; IF (SELECT COUNT(*) FROM users) > 100 WAITFOR DELAY '0:0:5' –
Si la réponse met 5 secondes, il y a plus de 100 utilisateurs.

Les types de failles et attaques

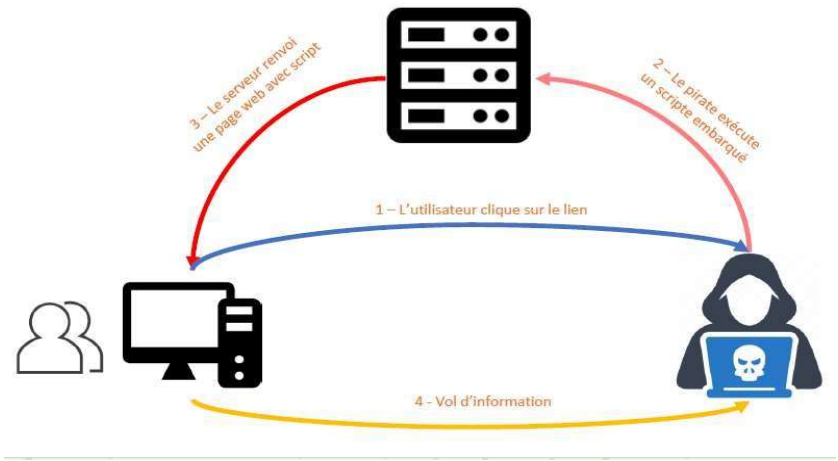
les différents types de cyberattaques

Cross-site Scripting (XSS) :Une vulnérabilité de sécurité dans les applications web. Elle permet à un attaquant d'injecter du code malveillant, généralement du code JavaScript, dans les pages web consultées par les utilisateurs. Ce code est ensuite exécuté côté client, c'est-à-dire sur le navigateur de la victime, ce qui peut entraîner diverses actions indésirables, telles que le vol de cookies de session, le vol d'informations confidentielles saisies par l'utilisateur……

Les attaques XSS peuvent être classées en trois catégories : **stockées**, **réfléchies** et **DOM-based**, en fonction de la façon dont le code malveillant est injecté et exécuté.

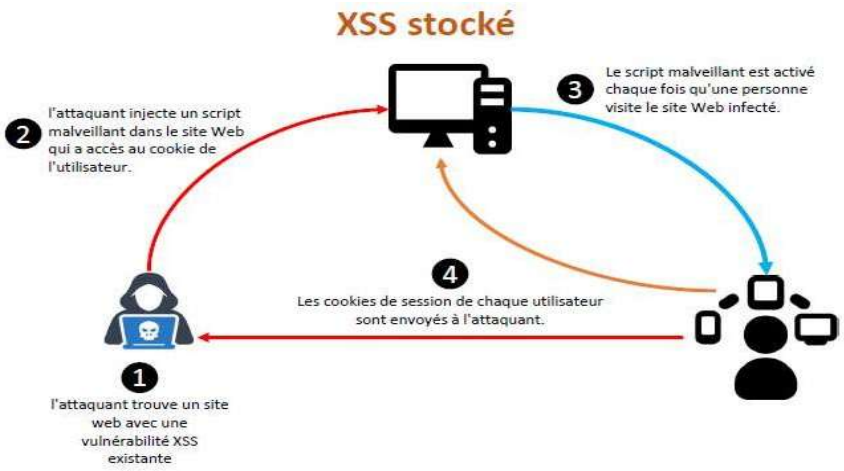
les différents types de cyberattaques

Cross-site Scripting (XSS) :



Types de script intersites (XSS)

- Le script est stocké de manière persistante dans l'application Web
- Les utilisateurs visitant l'application après l'infection récupèrent le script
- Un code malveillant exploite les failles de l'application Web
- Le script et l'attaque sont visibles côté serveur (pour le propriétaire de l'application)

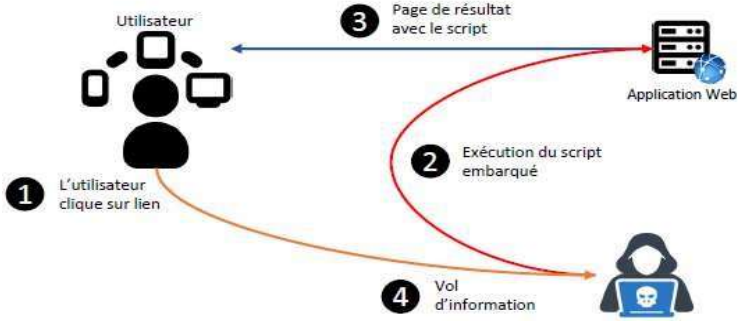


Types de script intersites (XSS)

Scripts intersites en miroir

- Ne stocke pas le contenu malicieux
- Le contenu est par exemple livré à la victime via une URL (exemple: envoyée par email <<< Phishing>>)
- Vise une seule victime

Scripts intersites en miroir



Types de script intersites (XSS)

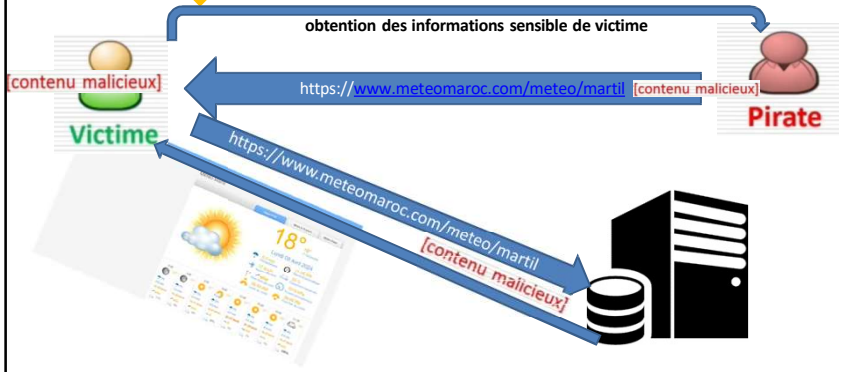
Scripts intersites en miroir

- Ne stocke pas le contenu malicieux
- Le contenu est par exemple livré à la victime via une URL (exemple: envoyée par email <<< Phishing>>)
- Vise une seule victime

Types de script intersites (XSS)

Scripts intersites en miroir

- Ne stocke pas le contenu malicieux
- Le contenu est par exemple livré à la victime via une URL (exemple: envoyée par email <<< Phishing>>)
- Vise une seule victime



Types de script intersites (XSS)

XSS basé sur Dom

- Attaques XSS basées sur le DOM (DOM based XSS).
- DOM est une structure utilisée pour représenter un document dans un navigateur
- Nécessite 'ou non' une interaction de la part de la victime
- Elle n'utilise pas le serveur web

Supposons que le code suivant soit utilisé pour créer un formulaire permettant à l'utilisateur de choisir sa langue préférée. Une langue par défaut est également fournie dans la chaîne d'interrogation, sous la forme du paramètre "default".

1
```
…
Choisissez votre langue:
<select><script>
document.write("<OPTION value=1>"+decodeURIComponent(document.location.href.substring(document.location.href.indexOf("default=")+8))+"</OPTION>");
document.write("<OPTION value=2>Français</OPTION>");
</script></select>
…
```

La page est invoquée avec une URL telle que :

2
```
http://www.some.site/page.html?default=French…
```

Une attaque DOM BasedXSS contre cette page peut être réalisée en envoyant l'URL suivante à une victime :

3
```
http://www.some.site/page.html?default=<script>alert(document.cookie)</script>
```

Lorsque la victime clique sur ce lien, le serveur répond avec la page contenant le code Javascript ci-dessus. Le navigateur crée un objet DOM pour la page, dans lequel l'objet document.location contient précédente. Le navigateur rend alors la page résultante et exécute le script de l'attaquant :

4
```
alert(document.cookie)
```