



République Algérienne Démocratique Et
Populaire

Ministère De L'enseignement Supérieur Et De
La Recherche Scientifique



Département Génie des systèmes
Filière IMSI : 4^{ème} année ingénieur

Sécurité des systèmes d'information

DR F.KABLI

kablifatima47@g
mail.com

L'analyse de risque

Concepts

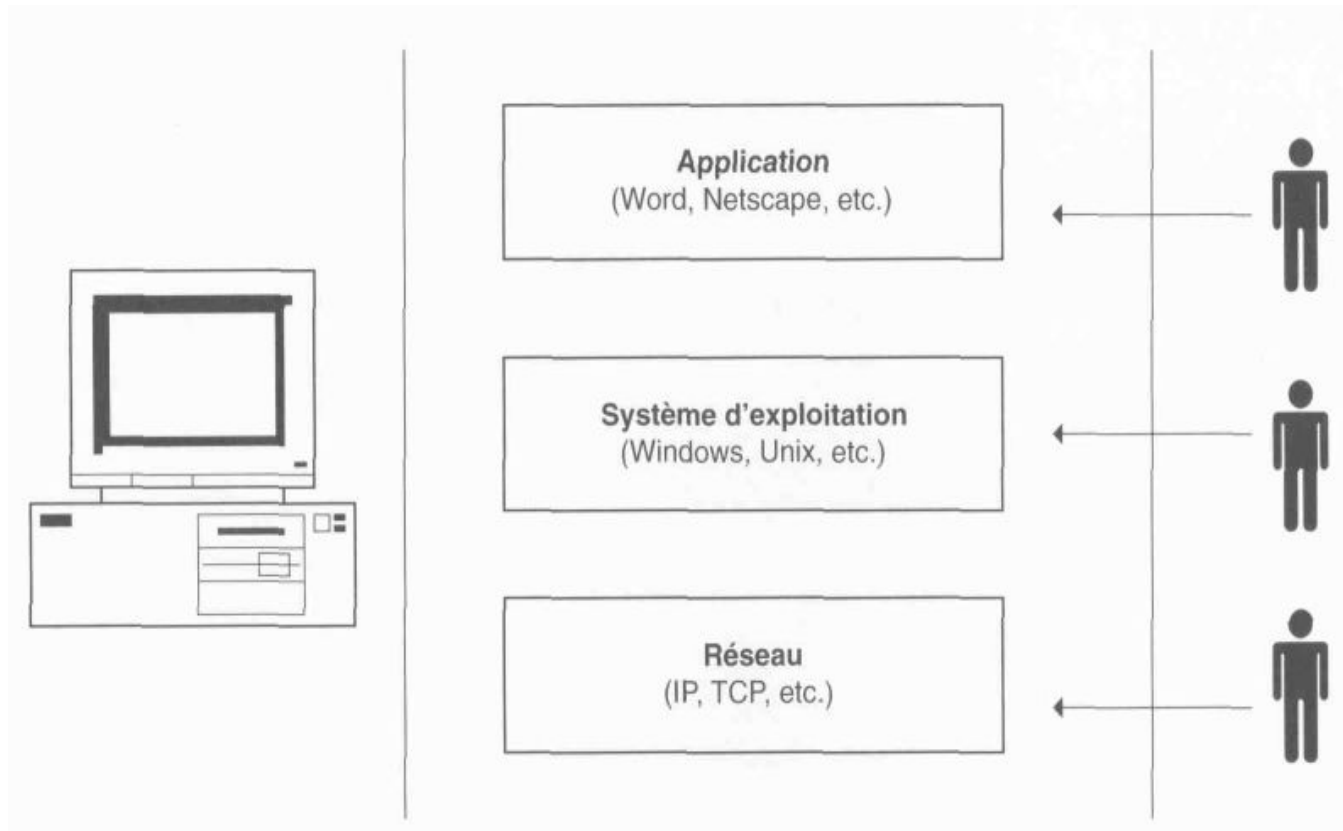
- Sécurité d'un réseau: implique la sécurité de chaque machine (client, serveur) du réseau.

'Hacker' : Programmeur qui utilise des attaques pour pénétrer au systèmes informatiques sans être détecté .

'Cracker' : Utilise des attaques pour réaliser des bénéfices économiques.

L'analyse de risque

Composantes d'un système susceptibles d'être attaquée



L'analyse de risque

Différents aspects de la sécurité

Aspect :

- Contrôle d'accès
- Authentification
- Confidentialité
- Intégrité
- disponibilité
- Antivirale

Exemple de mécanisme de protection :

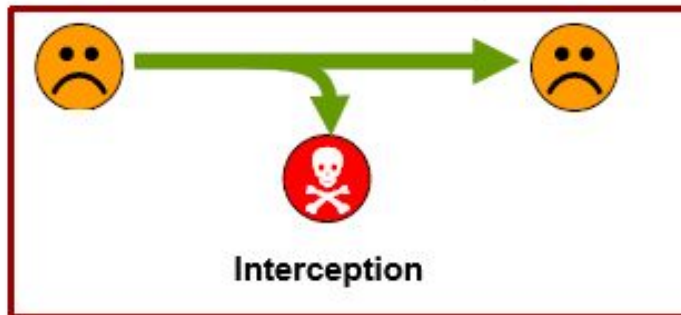
- Mot de passe
- Signature
- Cryptographie
- Anti-virus
- Firewall
- Sécurité de composants
- Surveillance de la disponibilité

L'analyse de risque

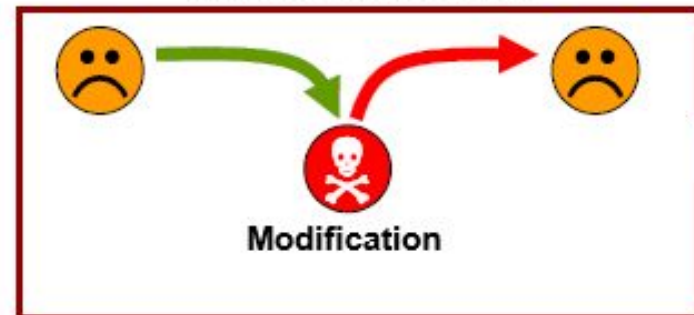
Classification des Attaques



violation de la vie privée



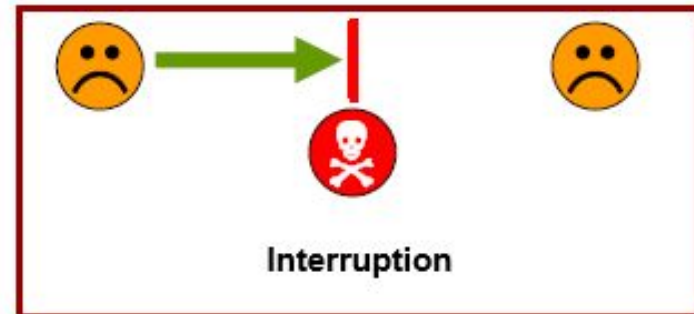
violation de l'intégrité



violation de l'authentification



violation de la disponibilité



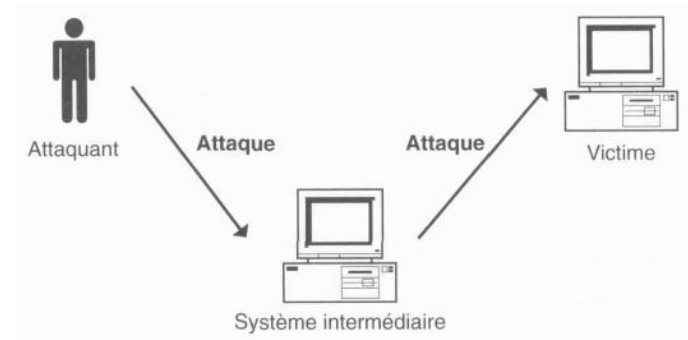
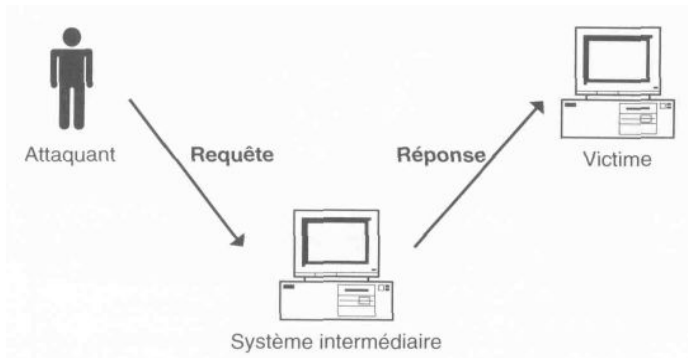
L'analyse de risque

Exemples d'attaques

Attaque directe



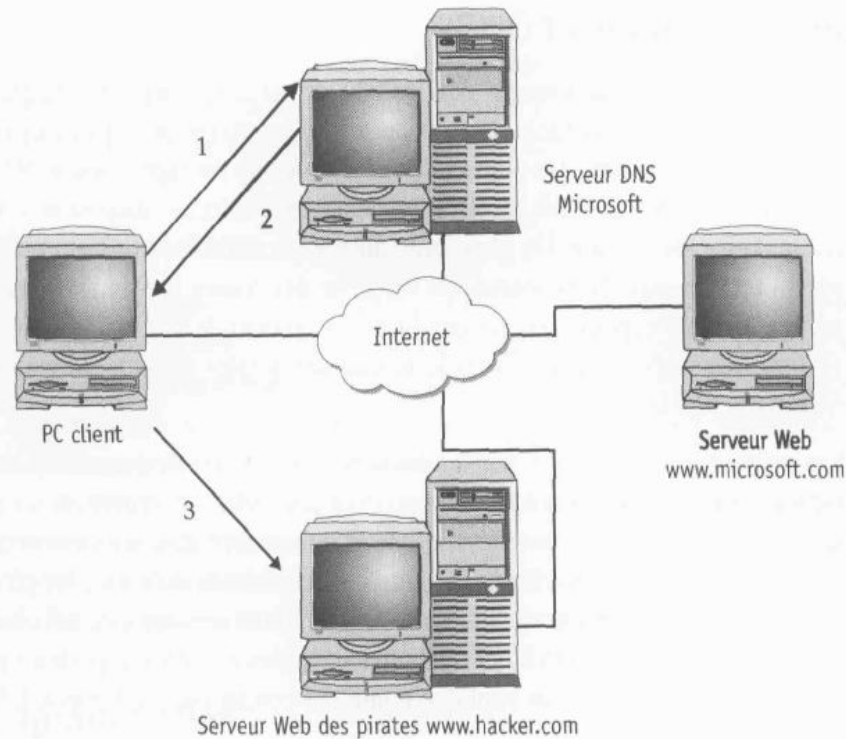
Attaque indirecte par réponse



L'analyse

de risque

Pollution du cache DNS



1) Le PC client demande à accéder au site Web de Microsoft. Le navigateur essaie de résoudre le nom *www.microsoft.com* en adresse IP.

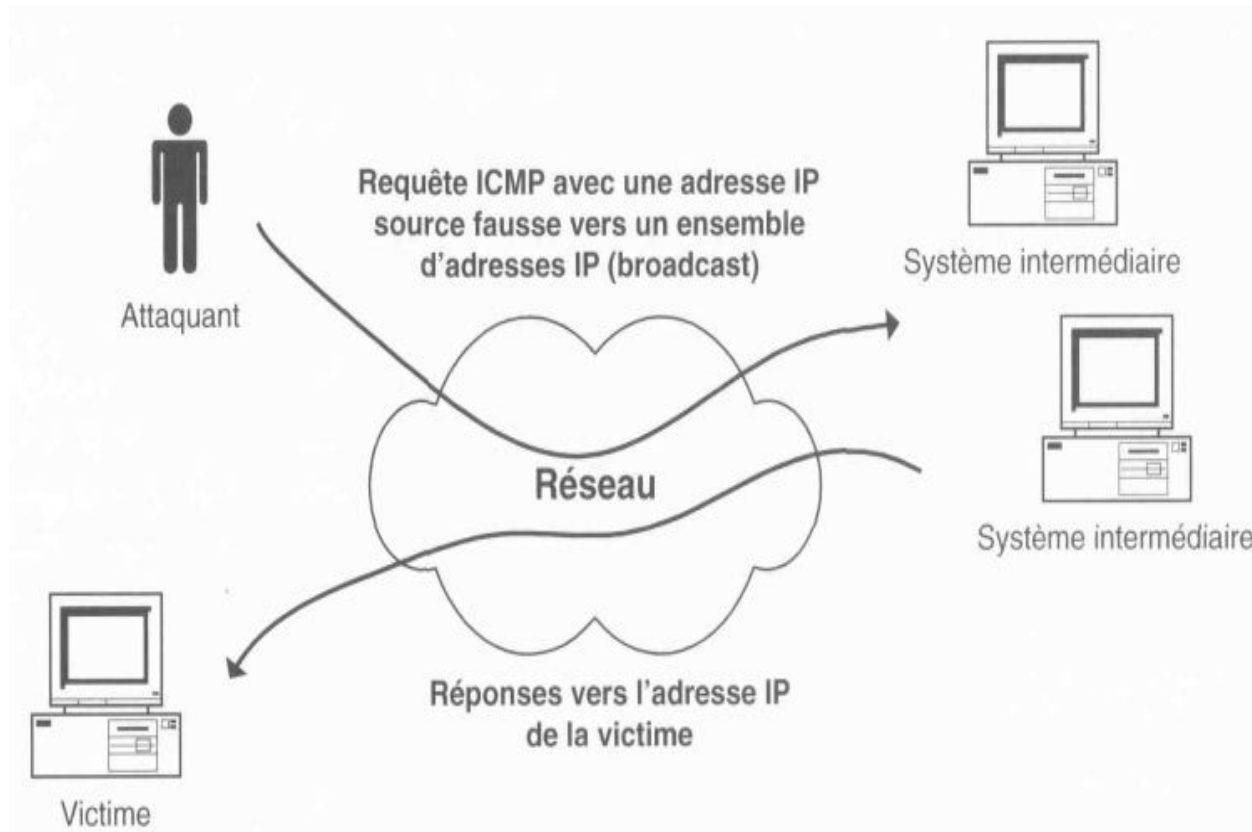
2) Le cache du serveur DNS a été contaminé par un pirate et renvoie l'adresse IP *www.hacker.com* au lieu de celle de Microsoft.

3) Le système des pirates se fait maintenant passer frauduleusement pour *www.microsoft.com*

L'analyse

de risque

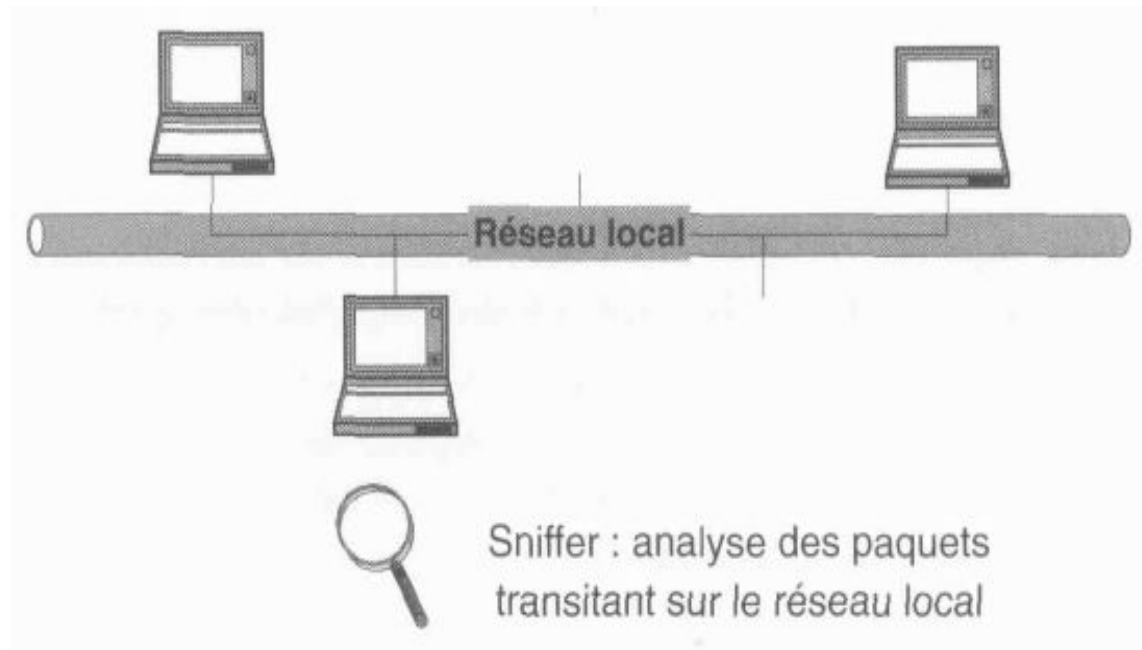
Inondation de Ping : ICMP



L'analyse

de risque

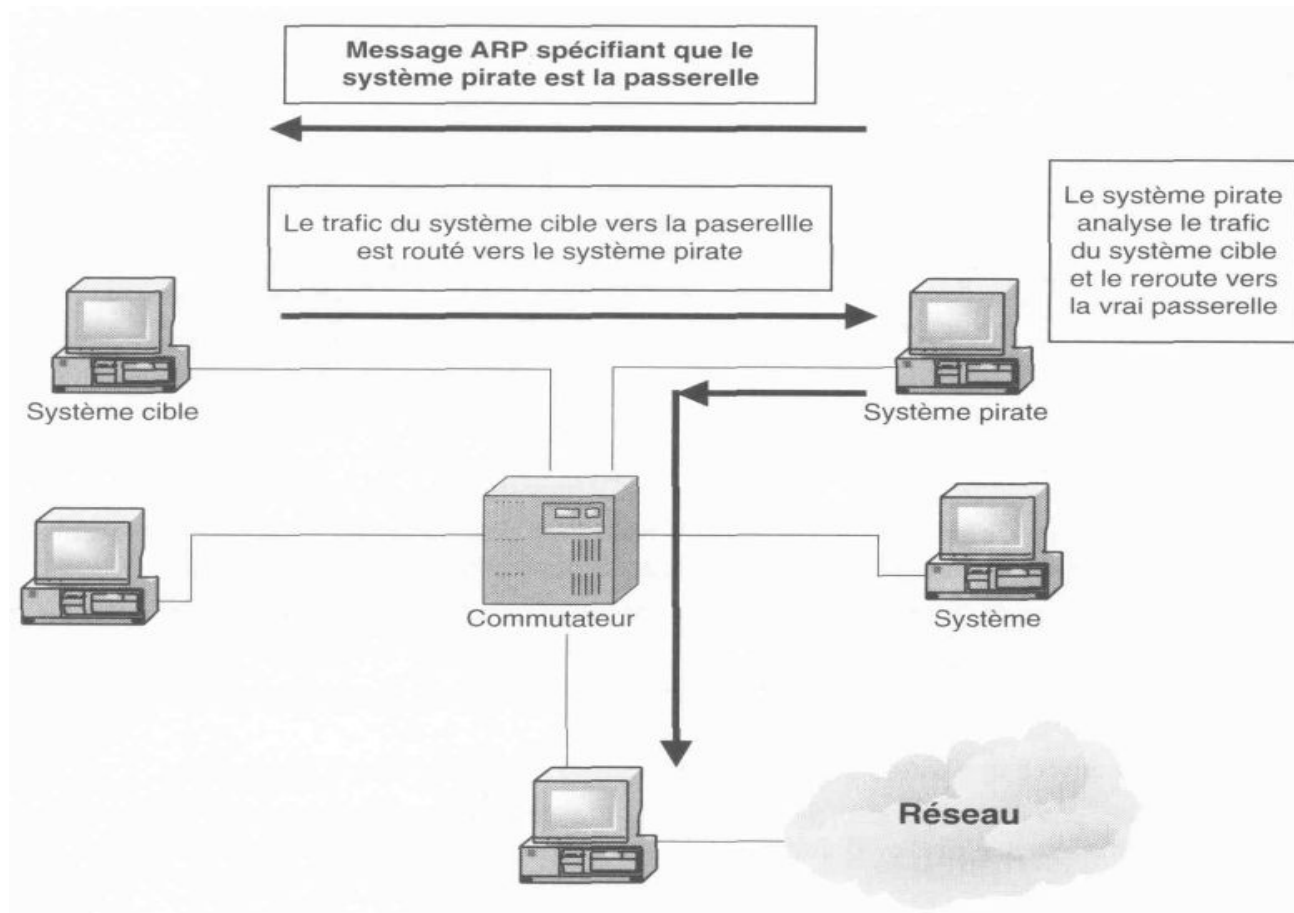
Écoute sur un réseau local



L'analyse

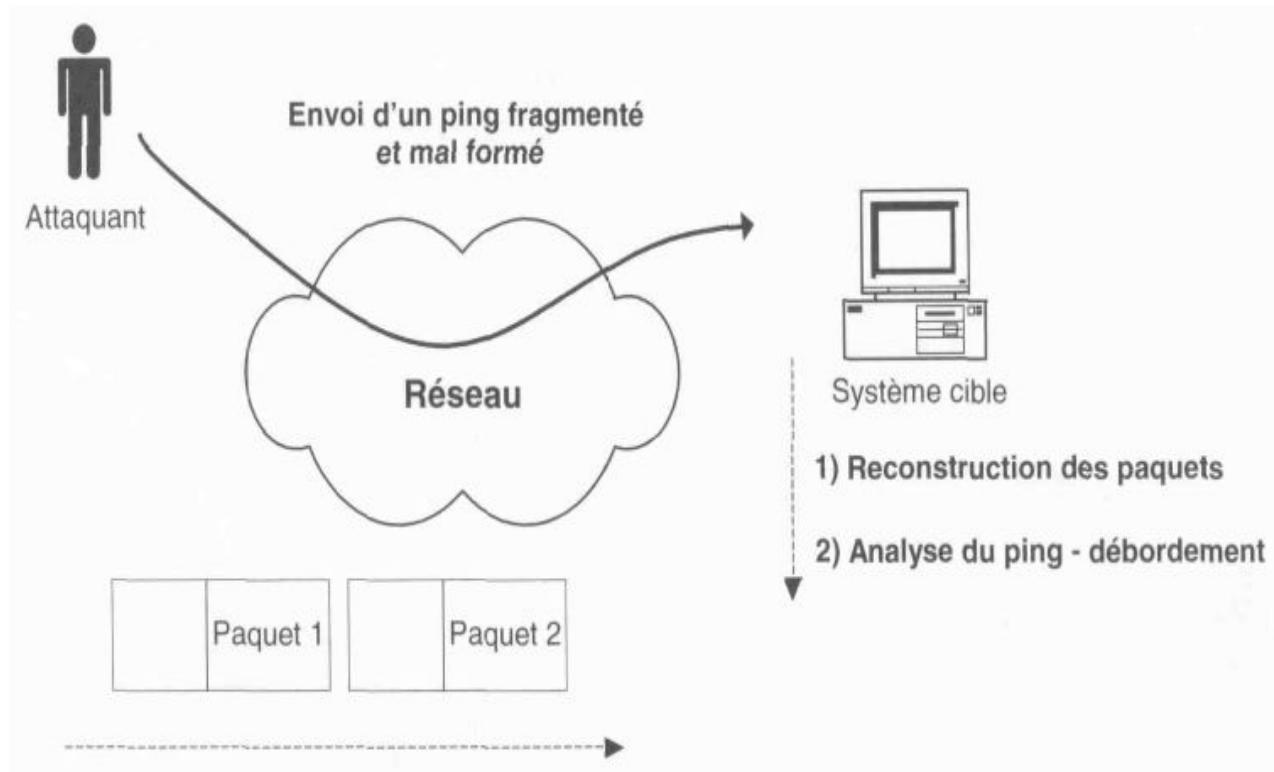
de risque

L'attaque ARP spoofing



L'analyse de risque

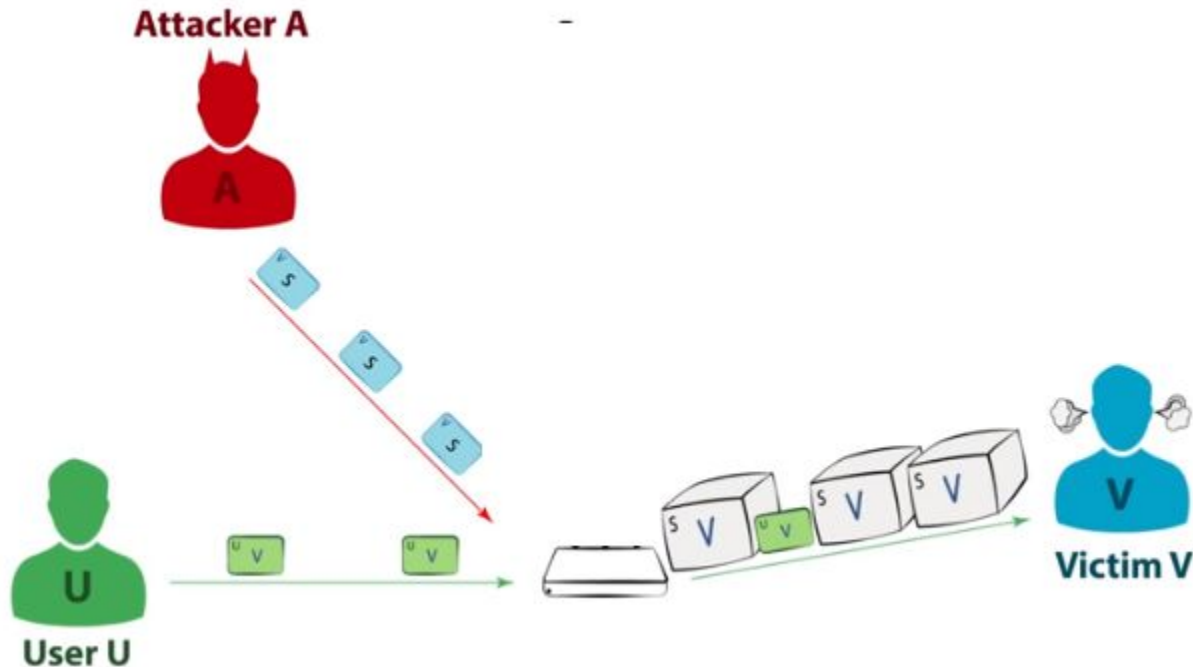
L'attaque ping de la mort



L'analyse

de risque

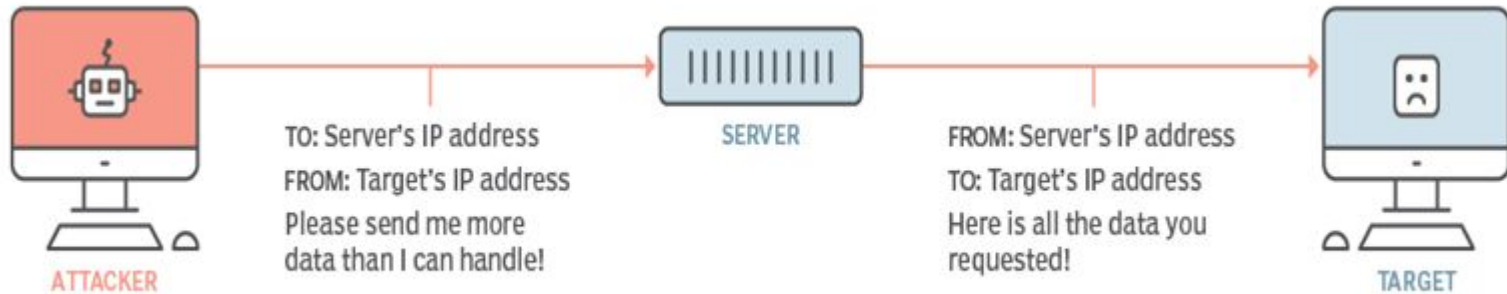
L'attaque IP spoofing(Machine)



L'analyse

de risque

L'attaque IP spoofing (serveur)



L'analyse

de risque

Dénie de Service (DOS)

Une attaque de déni de service (DoS - Denial of Service) est une tentative délibérée de rendre un système informatique, un service ou une ressource inaccessible, L'objectif principal d'une attaque DoS est de perturber ou d'interrompre les services normaux offerts par le système ciblé, entraînant ainsi une indisponibilité temporaire ou permanente.

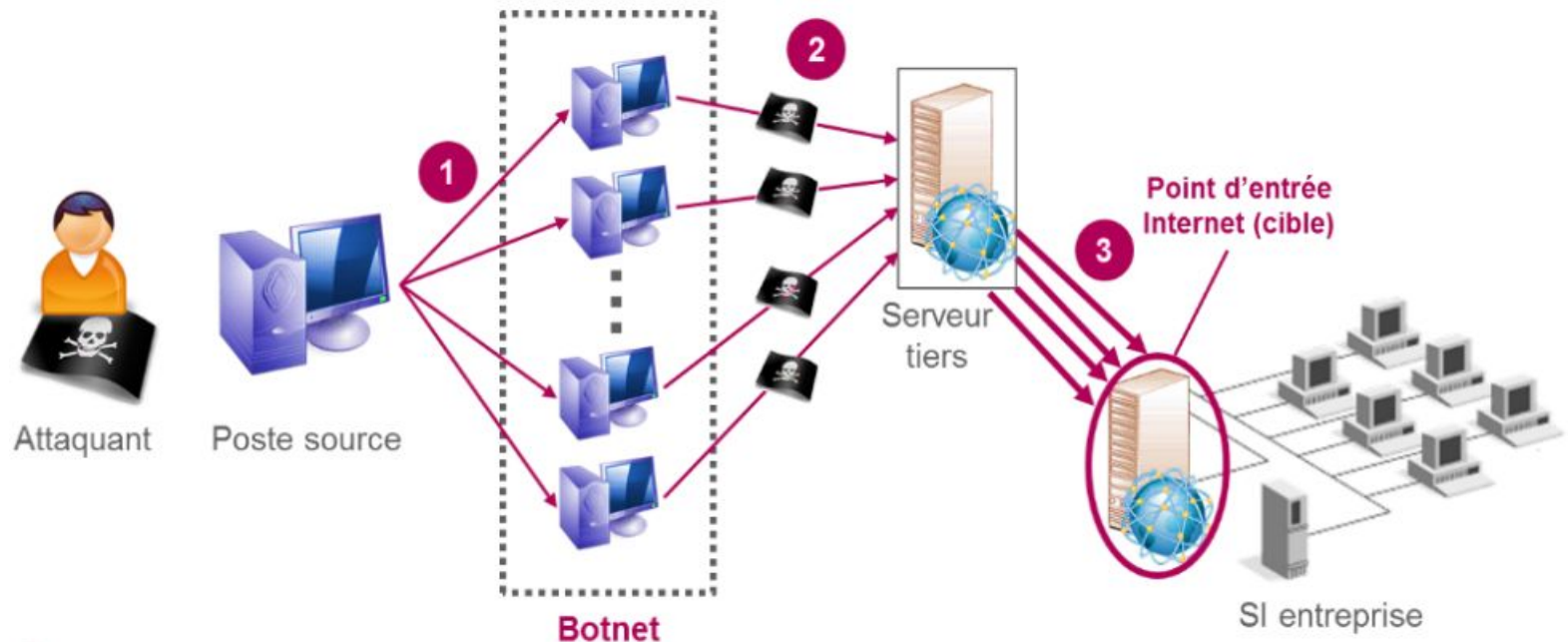
Déni de Service Distribué (DDoS)

Le déni de service distribué (DDoS) est une forme évoluée d'attaque DoS dans laquelle de multiples systèmes compromis, appelés zombies ou botnets, sont utilisés pour coordonner et amplifier l'attaque. Les attaques DDoS sont généralement plus difficiles à détecter et à contrer en raison de leur nature distribuée.

L'analyse

de risque

Exemple de DDOS



L'analyse

de risque

Les Modes DDOS

- Surcharge de bande passante
- Surcharge des ressources (Serveur WEB, DNS ,)
- Les informations sur la configuration sont détruites ou modifiées
 - Destruction et modification des composants physiques du réseau
- Attaques de couche d'application(Exemple: HTTP Get-Post)

L'analyse

de risque

Exemples : Attaques DDOS

L'attaque DDoS de GitHub : 2018

L'attaque de Google : 2022

L'attaque DDoS d'AWS : 2020

L'attaque contre DynDNS en 2016

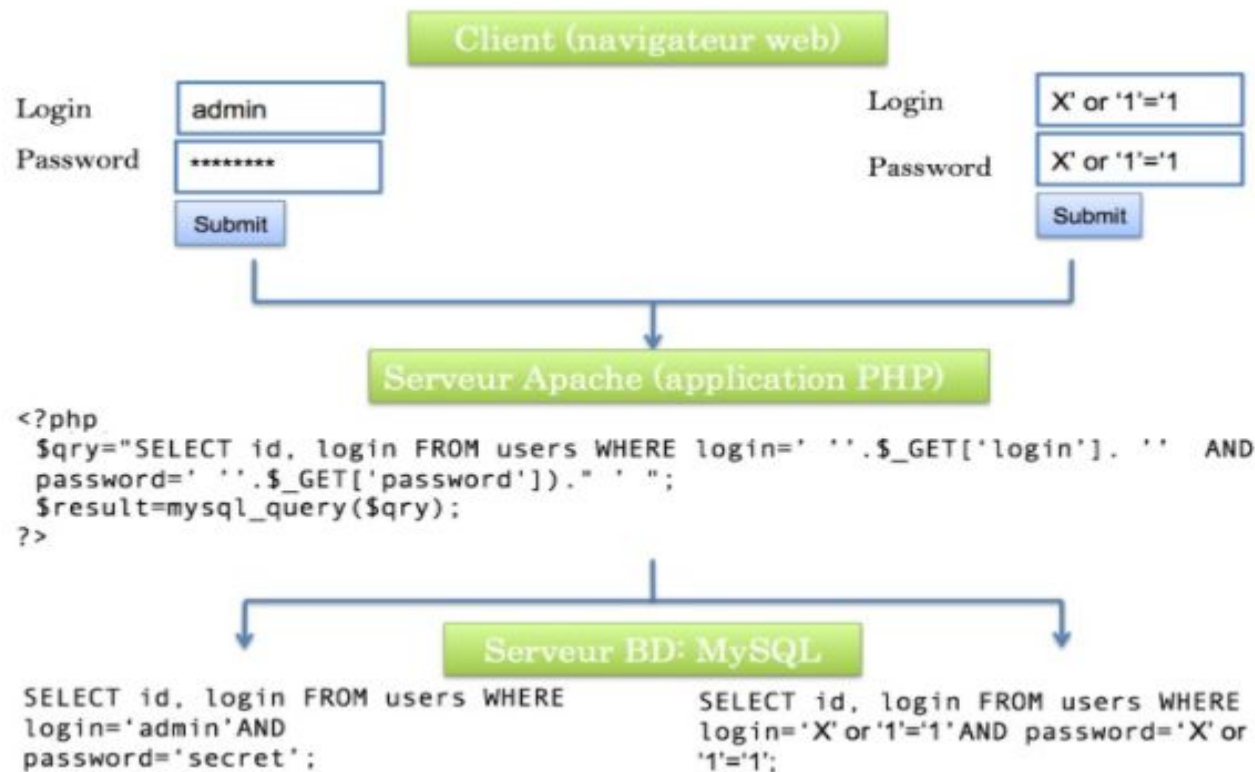
L'analyse

de risque **Injection SQL**

L'injection SQL est un type d'attaque discrète dans laquelle le pirate insère son propre code dans un site web afin de contourner ses mesures de sécurité et d'accéder à des données protégées. Une fois dans le site, il peut prendre le contrôle de sa base de données et pirater les informations concernant les utilisateurs

L'analyse de risque

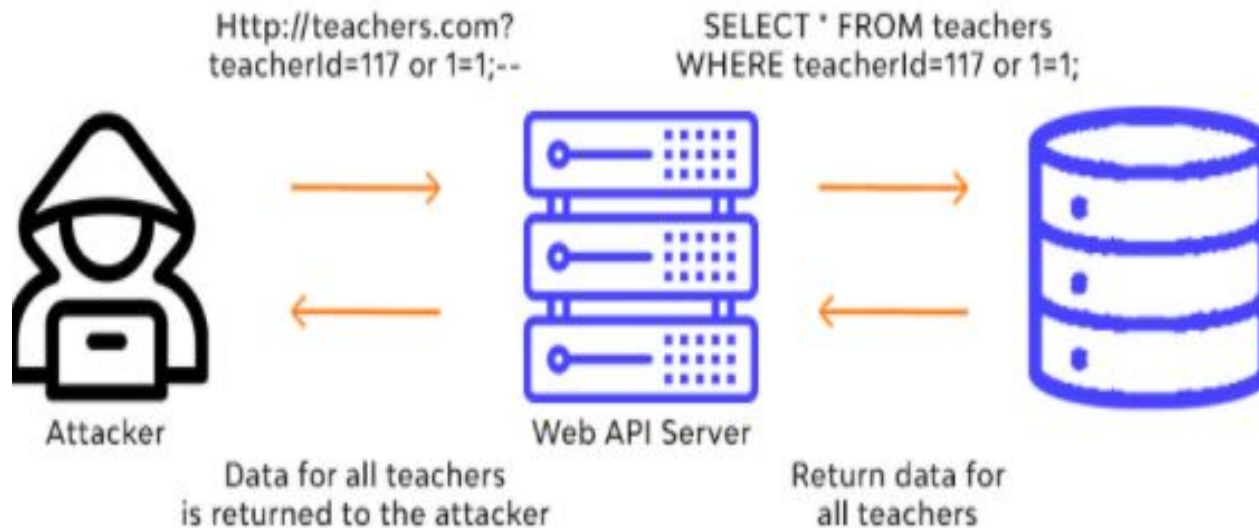
Attaque Injection SQL



L'analyse

de risque

Attaque Injection SQL



La cryptographie et ses applications

- ❑ Les algorithmes cryptographiques se basent sur des fonctions mathématiques qui dépendent d'une clé secrète.
- ❑ La sécurité est au niveau clés, pas au niveau algorithmes cryptographiques.
- ❑ Les algorithmes cryptographiques sont publiés et connus par tout le monde.

Définition : Un message en clair est **transformé** en une forme ambiguë, **incompréhensible** par le public.

- ❑ Lors de sa réception, seul le destinataire **légitime** peut renverser le processus et obtenir le message **original** en clair.
- ❑ La **cryptologie** peut être définie littéralement comme la *science du secret*. Elle se compose de deux grandes branches distinctes :

« La Cryptographie , La Cryptanalyse »

La cryptographie et ses applications

- ❑ Le verbe **crypter** est parfois utilisé le verbe **chiffrer**.
- ❑ **Modifier les messages** de telle façon à les rendre **incompréhensibles**, (le résultat de cette modification [le message chiffré] est appelé **cryptogramme** [en anglais **ciphertext**] par opposition au message initial, appelé message en **clair** [en anglais **plaintext**]).
- ❑ Les termes **chiffrement/ déchiffrement** sont généralement confondus avec les termes **cryptage /décryptage**.
- ❑ **Chiffrement** : processus de transformation du message M de telle manière à le rendre incompréhensible :
 - ✓ On se base sur une **fonction** de **chiffrement** « E »
 - ✓ On génère ainsi un message chiffré **$C = E(M)$**
- ❑ **Déchiffrement** : processus de reconstruction du message clair à partir du message chiffré
 - ✓ On se base sur une fonction de **déchiffrement** « D » .
 - ✓ On a donc **$D(C) = D(E(M)) = M$** .

La cryptographie et ses applications

Opérations de base

❑ Substitution :

Remplacement de chaque élément (bit, lettre, groupe de bits ou de lettres) dans le texte clair par un autre élément.

❑ Transposition :

réarrangement des éléments du texte clair.

❑ Opérations algébriques simples :

La plupart des systèmes utilisent plusieurs étapes de transposition et de substitution.

La cryptographie et ses applications

Opérations de base


Substituer un caractère ou un groupe de caractères par un autre dans le texte à chiffrer.

Exemple :

- Mono alphabétique
- Homophonique
- Poly-Alphabétique
- Autres

La cryptographie et ses applications

Exemple1 :

plaintext:	abcdefghijklmnopqrstuvwxyz
	
ciphertext:	mnbvcxzasdfghjklpoiuytrewq

Plaintext:	bob. how are you. alice
ciphertext:	nkn. akr moc wky. mgsbc

La cryptographie et ses applications

Exemple 2 :

Table des fréquences d'apparition des lettres pour un texte français :

Lettre	Fréquence %	Lettre	Fréquence %
A	9.42	N	7.15
B	1.02	O	5.14
C	2.64	P	2.86
D	3.39	Q	1.06
E	15.87	R	6.46
F	0.95	S	7.90
G	1.04	T	7.26
H	0.77	U	6.24
I	8.41	V	2.15
J	0.89	W	0.00
K	0.00	X	0.30
L	5.34	Y	0.24
M	3.24	Z	0.32

La cryptographie et

Lettre	Fréquence	Symboles
A	8,01	09, 12, 33, 47, 53, 67, 78, 92
B	0,88	48
C	3,23	13, 41, 62
D	3,91	01, 03, 45, 79
E	15,52	14, 16, 24, 25, 31, 39, 44, 46, 55, 57, 64, 74, 81, 82, 87, 98
F	1,06	10
G	1,06	6
H	0,88	23
I	7,35	32, 50, 70, 73, 83, 88, 93
J	0,44	15
K	0,05	4
L	5,77	26, 37, 51, 84, 88
M	2,9	22, 27, 56
N	7,22	18, 39, 58, 59, 66, 71, 91
O	5,43	00, 05, 54, 72, 90
P	2,94	07, 38, 95
Q	1,14	94
R	6,69	29, 35, 40, 42, 77, 80
S	8,17	11, 19, 36, 43, 65, 76, 86, 96
T	7,07	17, 20, 30, 49, 69, 75, 97
U	6	08, 52, 60, 61, 63, 99
V	1,41	34
W	0,02	89
X	0,47	28
Y	0,3	2
Z	0,12	21

La cryptographie et ses applications

- ❑ Avec le tableau de substitution précédent, le mot **EVENEMENT** pourra être codé **253455588756149117**
- ❑ Si ce tableau tombait dans des mains ennemies, tous les messages chiffrés devenaient lisibles!