République Algérienne Démocratique Et Populaire
Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
ECOLE NATIONALE POLYTECHNIQUE D'ORAN MAURICE AUDIN

Département Génie des systèmes
Filière IMSI : 4ème année ingénieur

Sécurité des systèmes d'information

DR F.KABLI

kablifatima47@gmail.com

L'analyse de risque

Différents aspects de la sécurité

Aspect :	**Exemple de mécanisme de protection :**
• Contrôle d'accès	
• Authentification	• Mot de passe, Firewall
• Confidentialité	• Signature
• Intégrité	• Cryptographie
• disponibilité	• Anti-virus
• Virus	

L'analyse de risque

Concepts

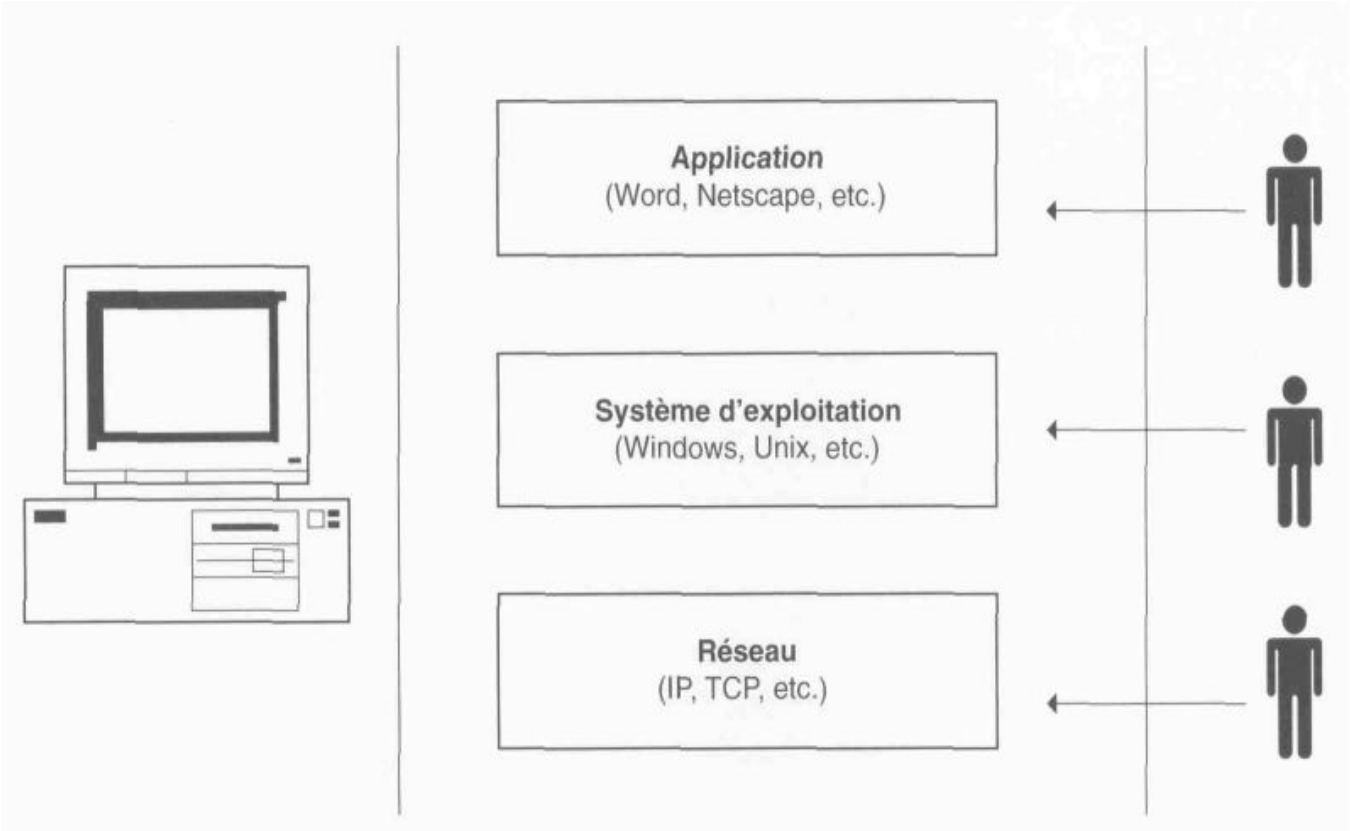
- Sécurité d'un réseau: implique la sécurité de chaque machine (client, serveur) du réseau.

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

- 'Cracker': utilise des attaques pour réaliser des bénéfices économiques.

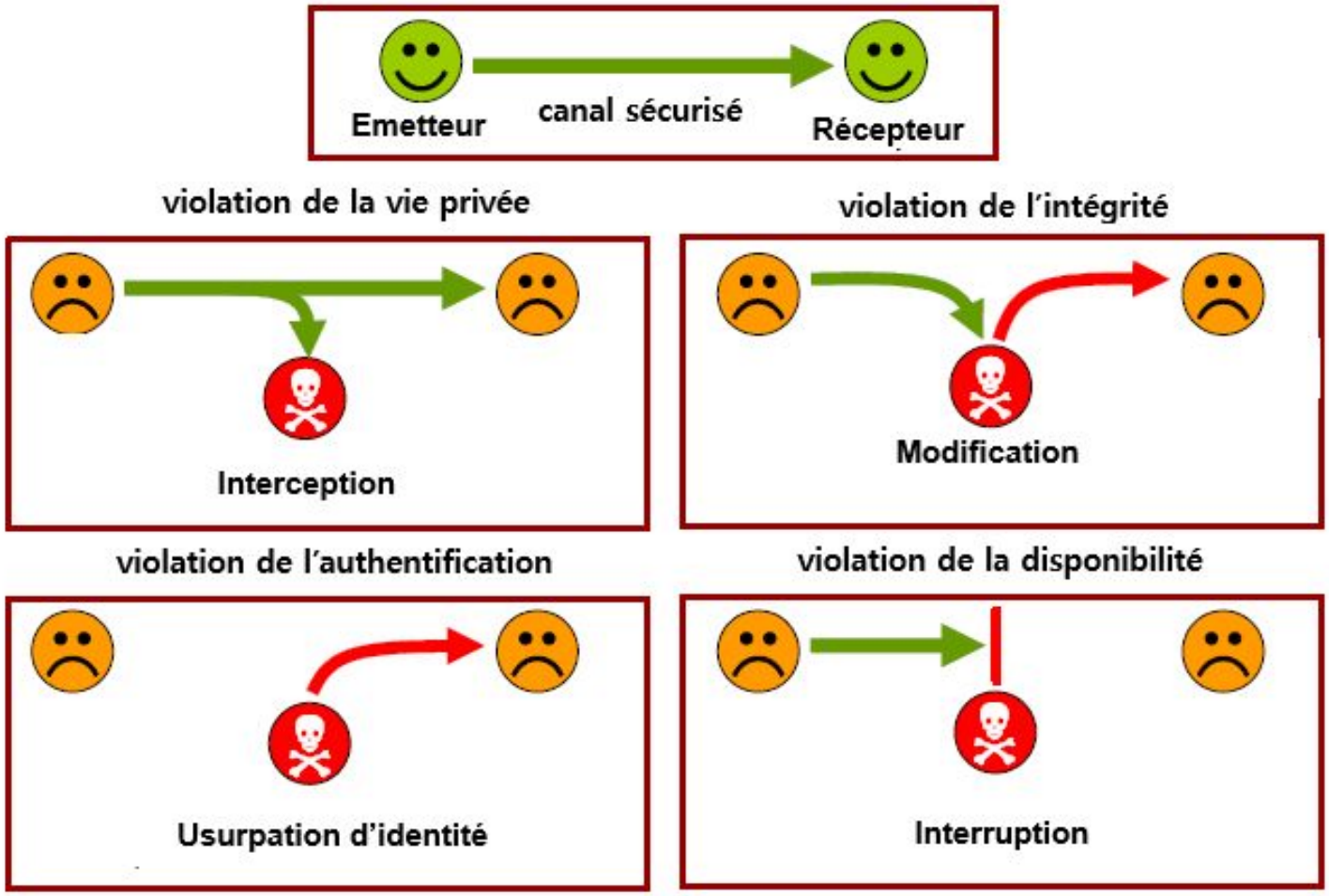
L'analyse de risque

Composantes d'un système susceptibles d'être attaquée



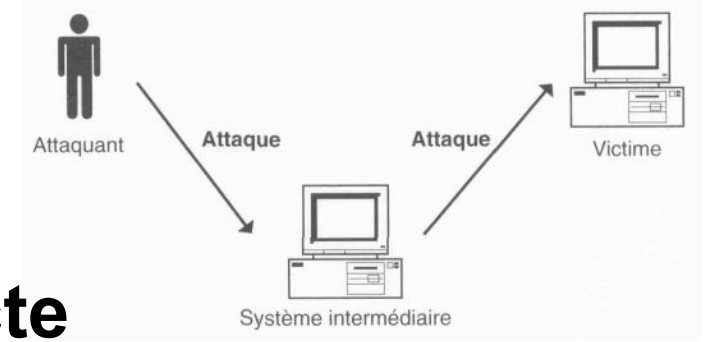
L'analyse de risque

Classification des Attaques

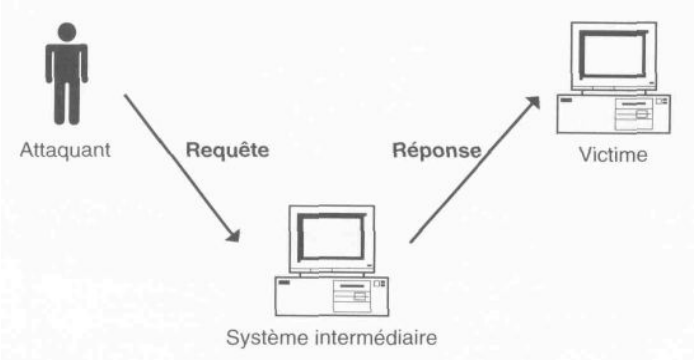


L'analyse de risque

Exemples d'attaques



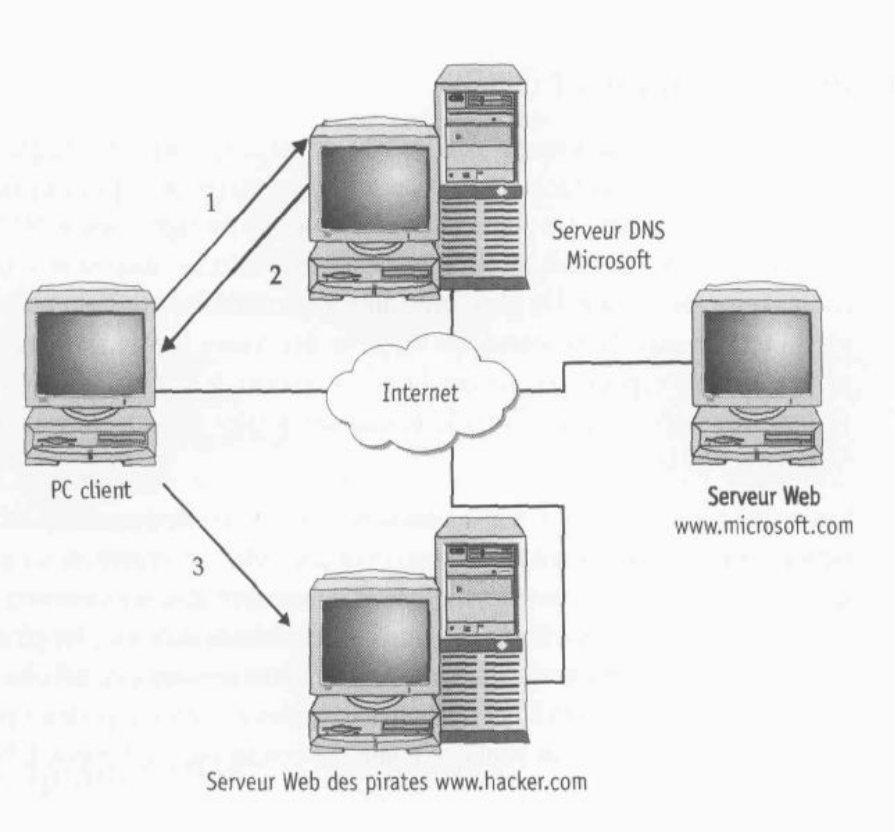
Attaque directe



Attaque indirecte par réponse

L'analyse de risque

Pollution du cache DNS



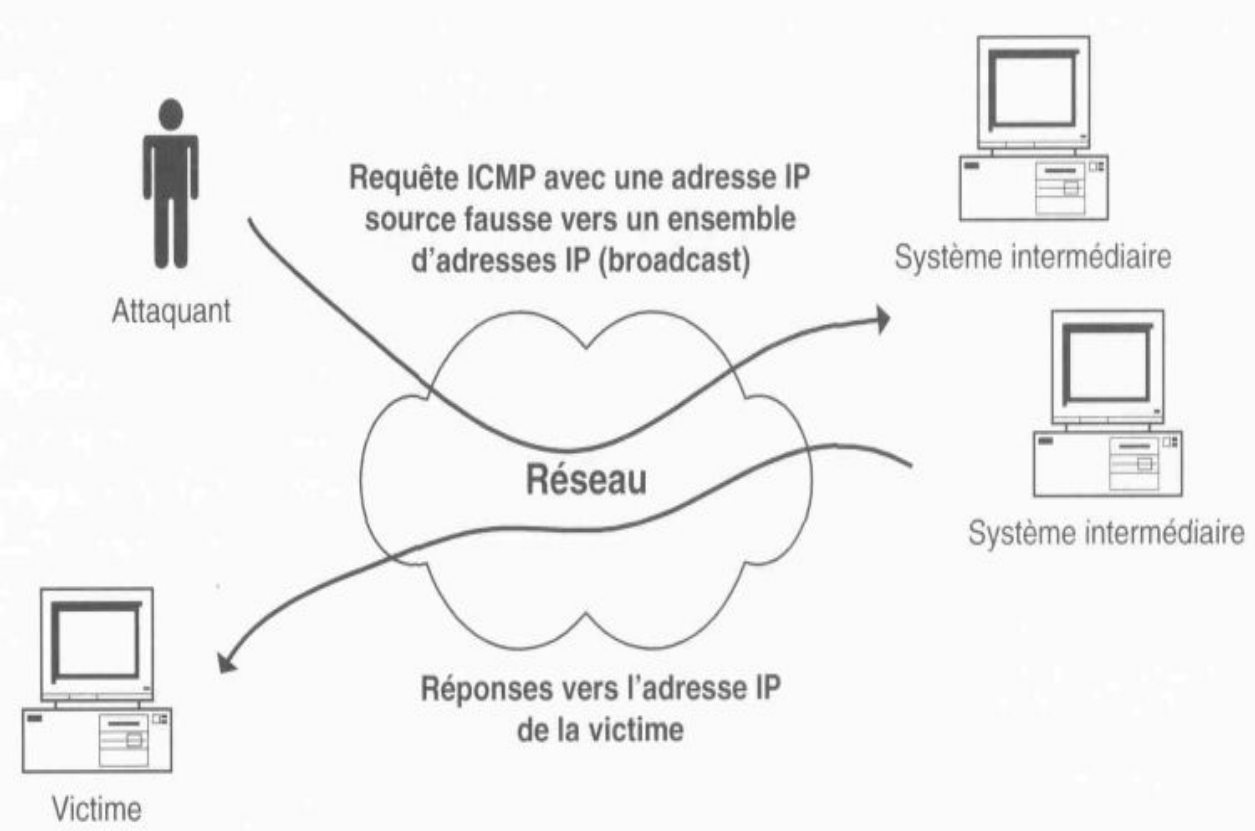
1) Le PC client demande à accéder au site Web de Microsoft. Le navigateur essaie de résoudre le nom *www.microsoft.com* en adresse IP.

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*

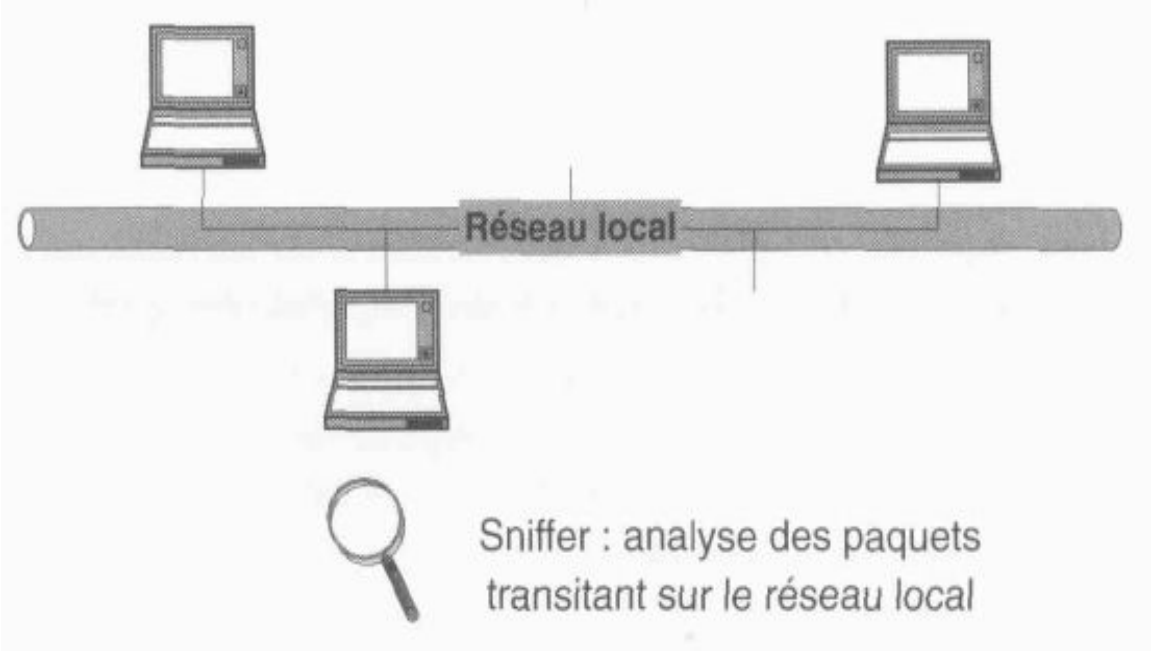
L'analyse de risque

Inondation de Ping : ICMP



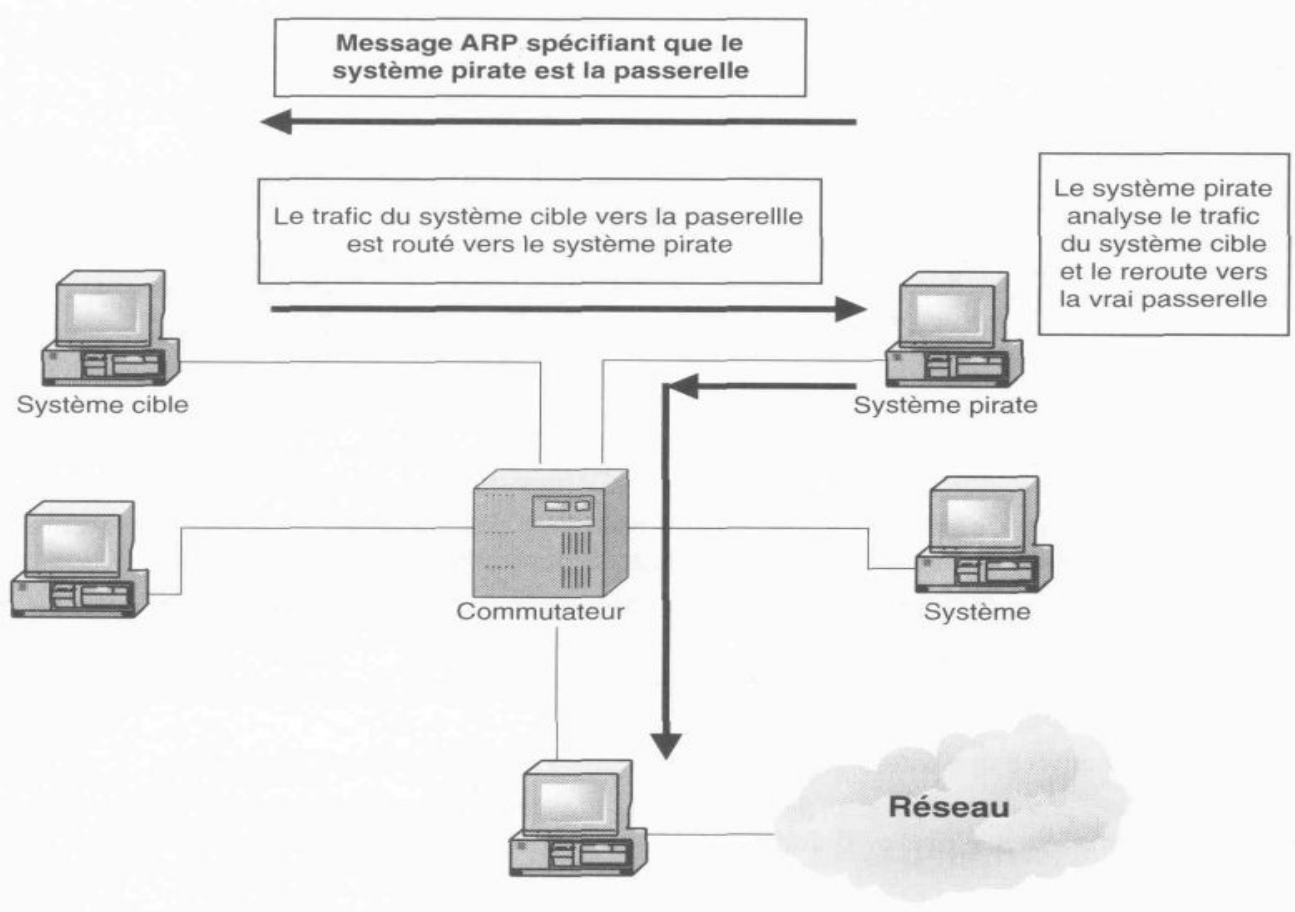
L'analyse de risque

Écoute sur un réseau local



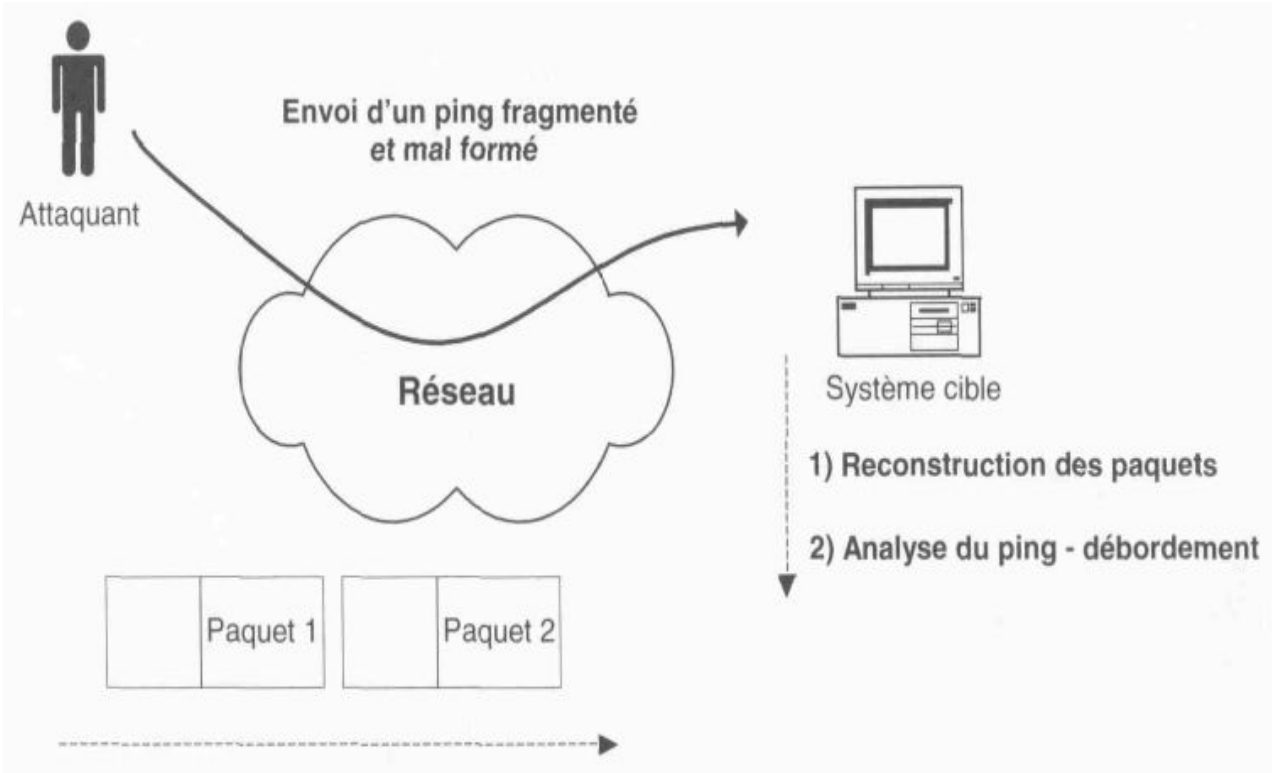
L'analyse de risque

L'attaque ARP spoofing



L'analyse de risque

L'attaque ping de la mort



L'analyse de risque

Analyse de réseau

Balayage d'hôtes (découverte d'hôtes)

Détection des @ IP des hôtes actifs Outils :

Ping sweeps,

Nmap, Nessus

Principe :

Exploiter ICMP et sa fonction echo-request

Méthode:

- Diffuser un paquet icmp : Echo-request
- Si Echo-reply reçu alors hôte accessible.

L'analyse de risque

Analyse de réseau

Balayage de ports

Détection des services en écoute (ports ouverts)

Services : http, ftp, ssh, etc.

Outils : Nmap, Nessus,

Principe : Exploiter le mode de connexion TCP (3 way handshake)

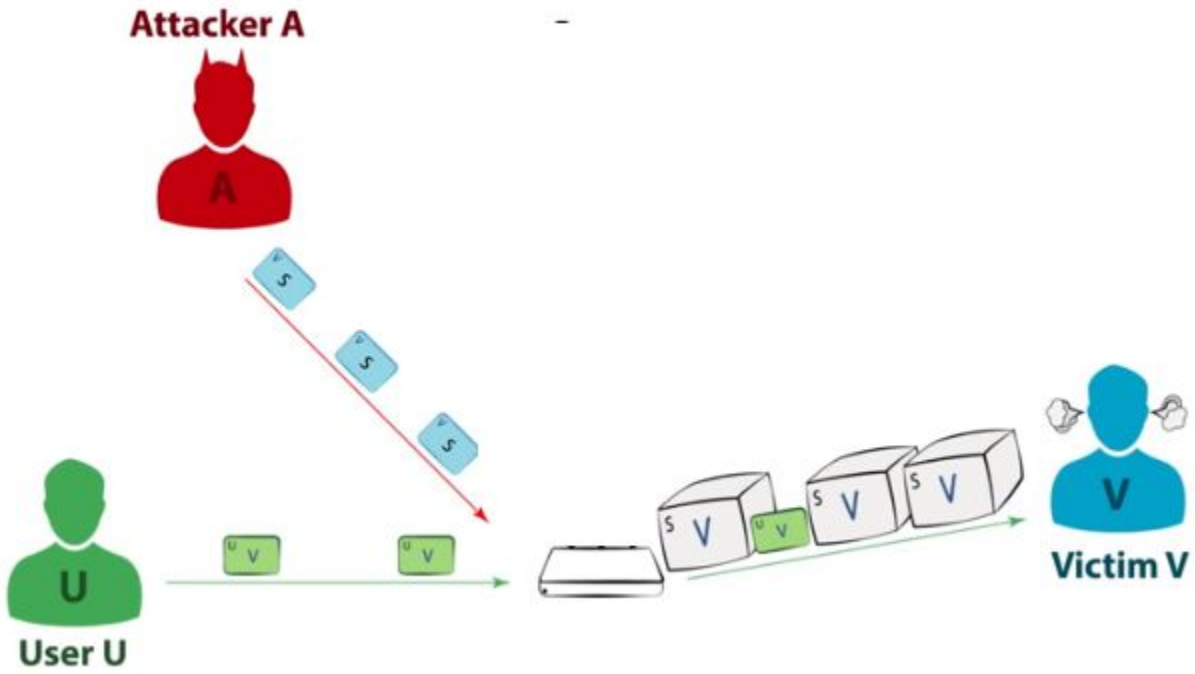
Méthode : Envoyer un paquet de test : SYN

Si SYN/ACK reçu alors port ouvert

Si RST reçu, alors port fermé

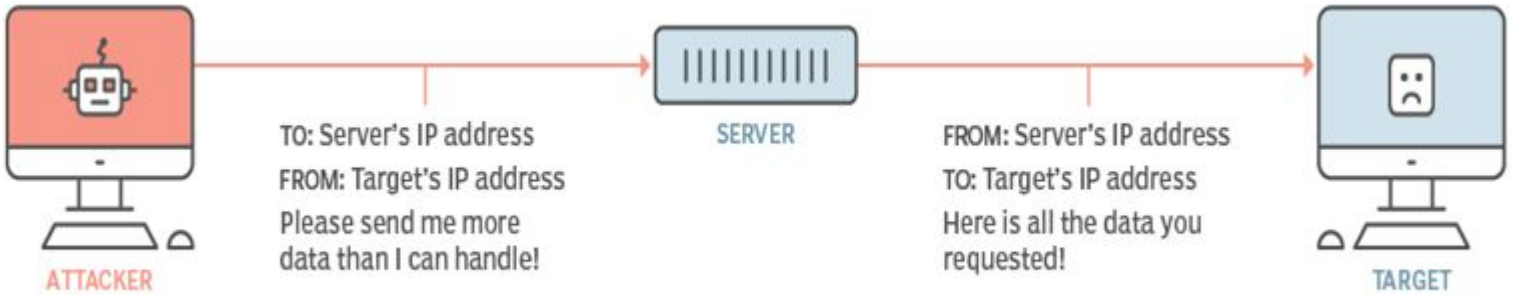
L'analyse de risque

L'attaque IP spoofing



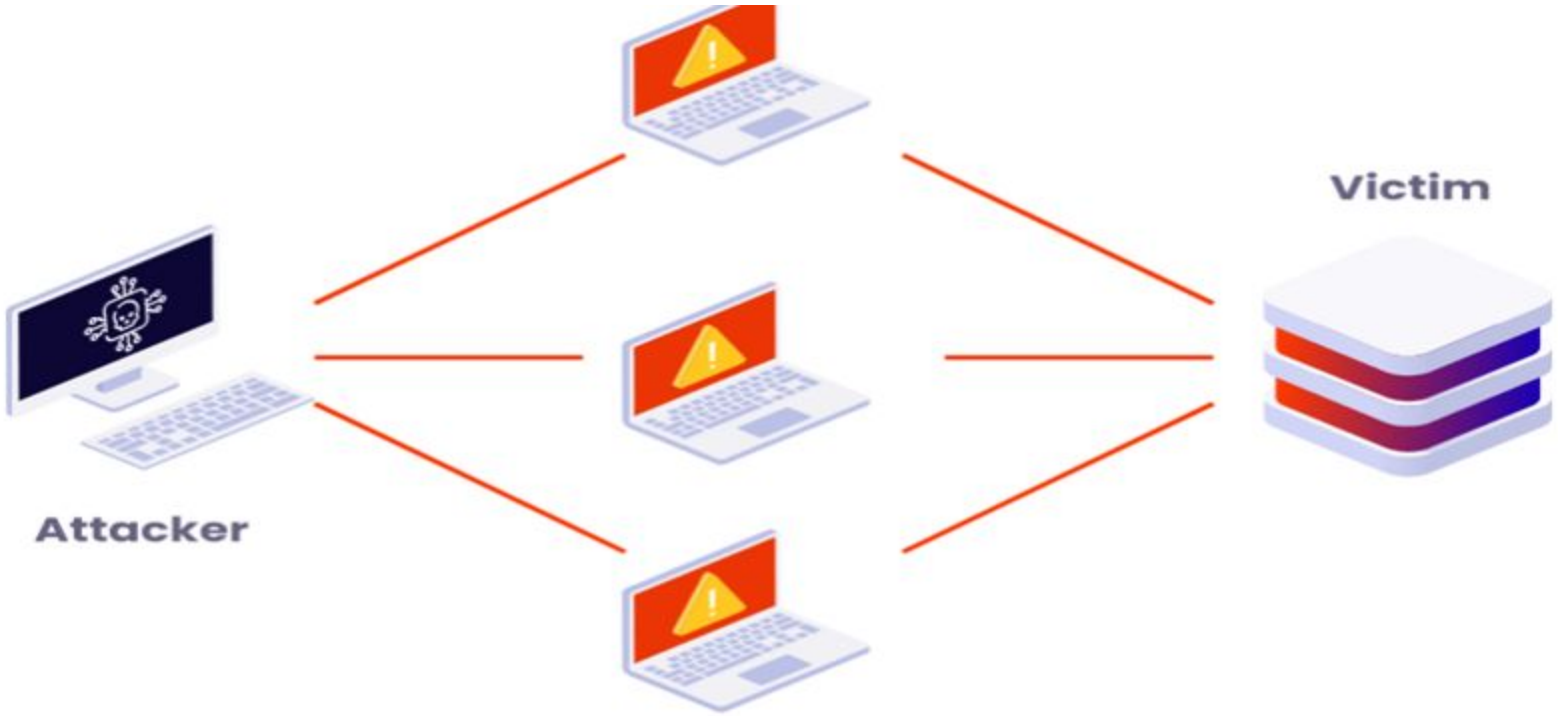
L'analyse de risque

L'attaque IP spoofing (serveur)



L'analyse de risque

L'attaque IP spoofing (DDOS)



L'analyse de risque

L'attaque IP spoofing (Protection)

- Configurez des systèmes pour examiner les en-têtes source des paquets IP entrants
- Ne laissez pas les connexions rester ouvertes sans un certain type de vérification ou de contrôle de la qualité
- Utilisez le cryptage de niveau IP.

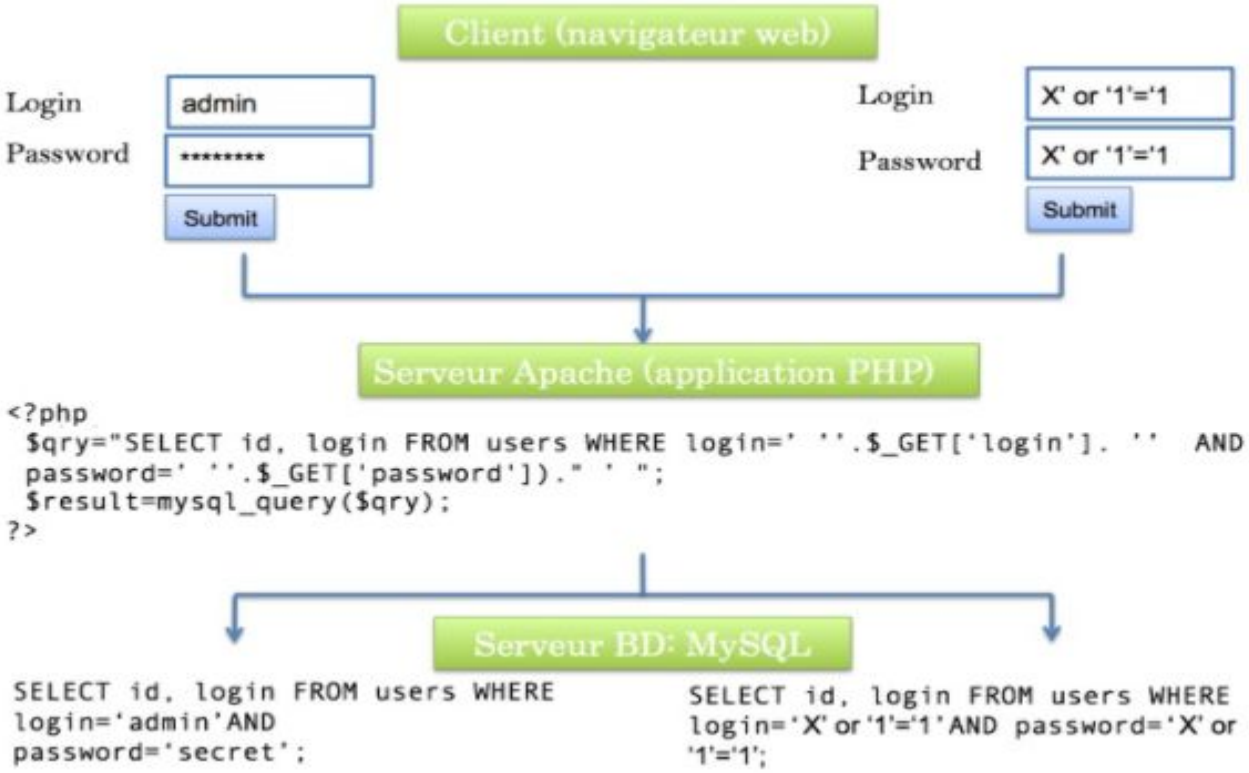
L'analyse de risque

Analyse de réseau

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 ses utilisateurs

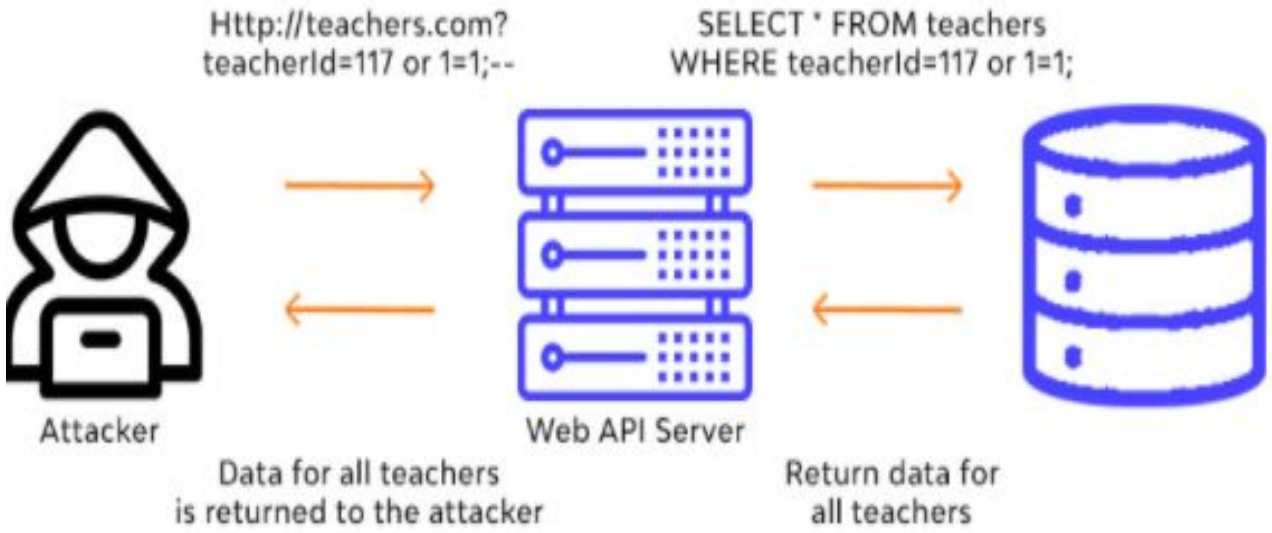
L'analyse de risque

Attaque Injection SQL



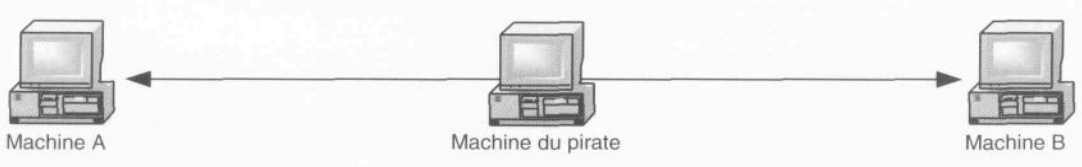
L'analyse de risque

Attaque Injection SQL

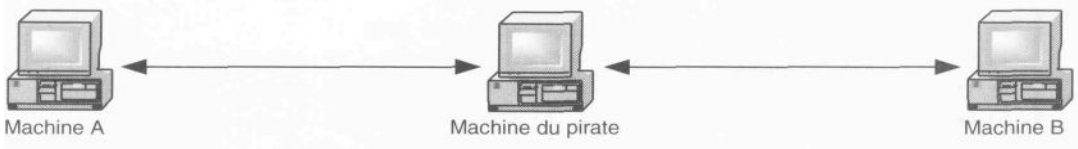


L'analyse de risque

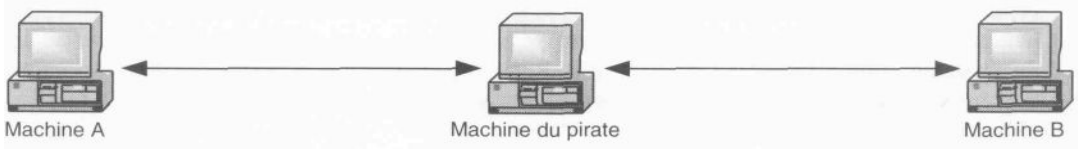
Machine du pirate (Man-in-the-middle)



en tant que relais transparent



en tant que relais applicatif



en tant que hijacker

L'analyse de risque

Les Attaques :

- **Attaques réseaux**

✔ Connexion réseaux
✔ Service
✔ ……

- **Attaques systèmes**

✔ Fichier mot de passe
✔ Page web

La cryptographie et ses applications

- Les algorithmes cryptographiques se basent sur des fonctions mathématiques qui dépendent d'une clés secrète.

- La sécurité est au niveau clés, pas au niveau algorithmes cryptographiques.

- Les algorithmes cryptographiques sont publiées est connu par tout le monde.

Définition : Un message en clair est **transformé** en une forme ambigüe, **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

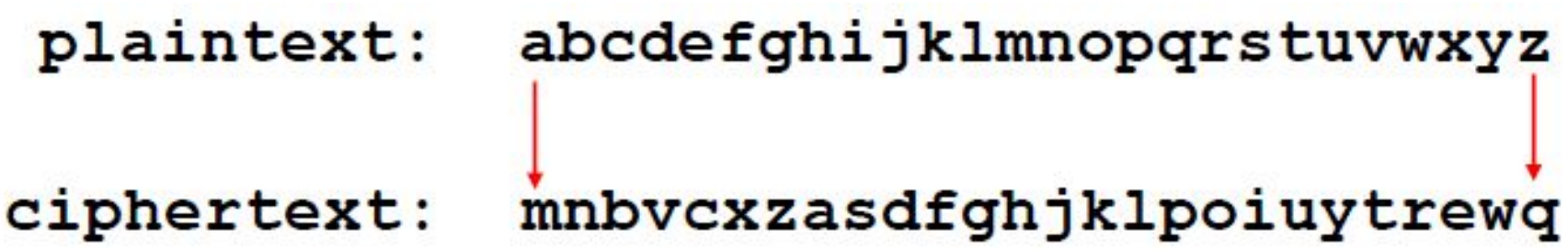
Substituer un caractère ou un groupe de caractères par un autre dans le texte à chiffrer.

Exemple :

- Mono alphabétique
- Homophonique
- ……..

La cryptographie et ses applications

Exemple1：



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 %
A	9.42
B	1.02
C	2.64
D	3.39
E	15.87
F	0.95
G	1.04
H	0.77
I	8.41
J	0.89
K	0.00
L	5.34
M	3.24

Lettre	Fréquence %
N	7.15
O	5.14
P	2.86
Q	1.06
R	6.46
S	7.90
T	7.26
U	6.24
V	2.15
W	0.00
X	0.30
Y	0.24
Z	0.32

La cryptographie et ses applications

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 **25345558875614 9117**

- Si ce tableau tombait dans des mains ennemies, tous les messages chiffrés devenaient lisibles!