



-Cours-

Ingénierie et **M**anagement de la **S**écurité des **S**ystèmes d'**I**nformation

Dr. KHALDI Miloud

m.khaldi@esi-sba.dz

- Chapitre II-

Panorama des vulnérabilités, des menaces et des risques

Notions liées aux vulnérabilités, menaces et risques

Notion de risque

Exemple d'un risque: cambrioleur



Vulnérabilité:
Clés sous le tapis.



Menace:
Cambrioleur essaie d'entrer.

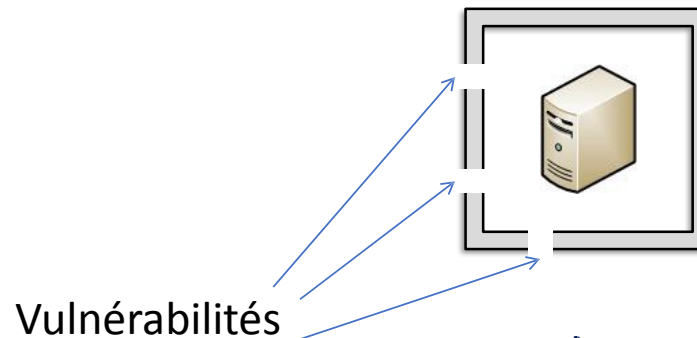


Impact: Cambrioleur casse l'armoire, vole de l'argent, crée des ennuis.

Notions liées aux vulnérabilités, menaces et risques

Vulnérabilité (vulnerability)

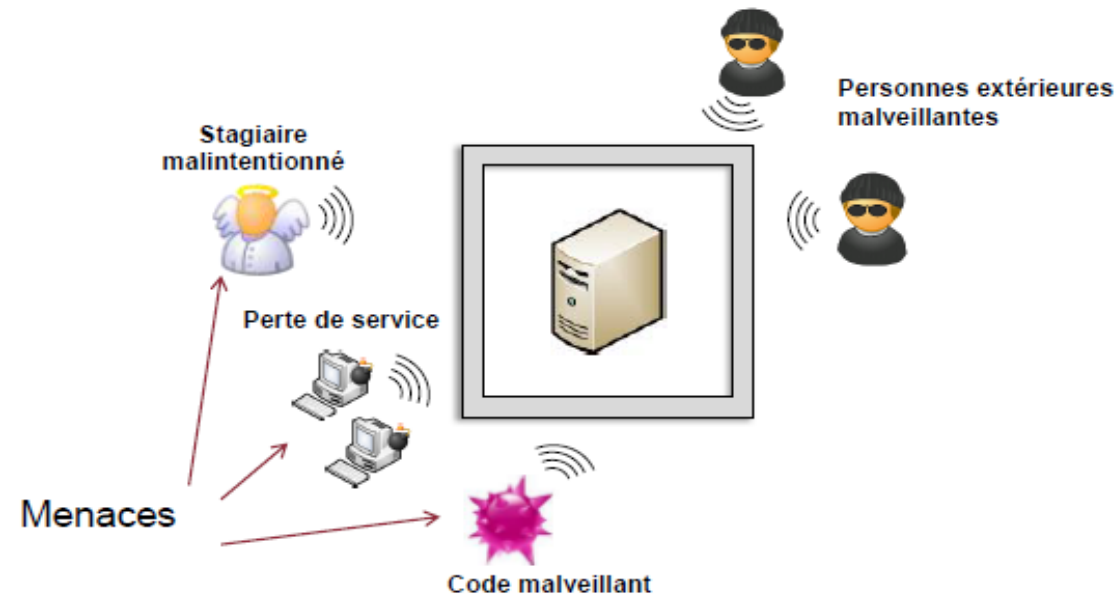
- **Faiblesse/faille**: faute **accidentelle** ou **intentionnelle** introduite dans la **spécification, conception, réalisation, installation, configuration** ou **utilisation** du système.
- **Caractéristique** du système qui peut être **exploitée** par une **menace**.
- La vulnérabilité = la surface d'**attaque**.



Notions liées aux vulnérabilités, menaces et risques

Menace (threat)

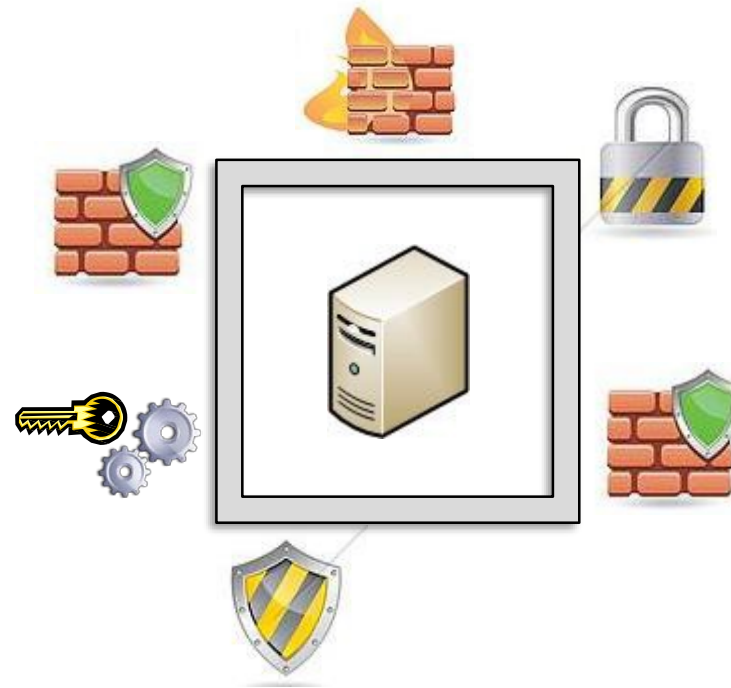
- Type d'action susceptible de **nuire** (la source du **risque**)
- Violation potentielle d'une **propriété** de sécurité



Notions liées aux vulnérabilités, menaces et risques

Contre-mesure

- L'ensemble des **actions** mises en œuvre afin d'empêcher la **menace**.



Notions liées aux vulnérabilités, menaces et risques

Impact

- **Conséquence** du risque sur l'organisme et ses objectifs,
 - L'impact peut, quant à lui, être qualifié en termes de niveau de **sévérité**.

$$\text{Risque} = \text{Menace} \times \text{Vulnérabilité} \times \text{Impact}$$

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

Types de vulnérabilité d'un SI

a. Vulnérabilités humaines

Provient des faiblesses/points faibles du caractère humain par rapport à la fonction requise par le SI:

- Surexploitation (faire travailler un employé au-delà de la limite de ses capacités normales);
- Manque de compétences;
- Négligence;
- Laxisme.

⇒ Bonnes pratiques...

- Sensibilisation des utilisateurs aux problèmes liés à la SSI ;
- Formation (de base/ approfondie) à la SSI pour les utilisateurs / les équipes opérationnelles de sécurité;

Types de vulnérabilité d'un SI

b. Vulnérabilités matérielles/physiques

Vulnérabilités liées aux événements imprévisibles (pannes et accidents des matériels):

- Non-redondance (serveurs, câblage...);
- Manque de contrôle d'accès aux éléments physiques (salles informatiques, serveurs, etc.);
- Mauvaise conservation de supports de sauvegarde (température, humidité...).

⇒ **Bonnes pratiques...**

- Contrôle d'accès au matériel ;
- Analyser les caractéristiques physiques (emplacement, température, humidité, etc.) des salles et équipements informatiques;

Types de vulnérabilité d'un SI

c. Vulnérabilités logicielles/techniques

Ces vulnérabilités sont à la base dues à une négligence/erreur humaine lors de la conception, la réalisation et la configuration des logiciels:

- Existence des bogues dans un dispositif logiciel;
- Complexité des règles sur les pare-feu et routeurs;
- Failles liées aux problèmes d'interopérabilités et de migration;
- Non-fiabilité des mises à niveau et correctifs (patches).

⇒ Bonnes pratiques...

- Utilisation de logiciels de sécurité (antivirus, IDS, pare-feu...);
- Installation des mises à niveau et correctifs régulièrement.

Types de vulnérabilité d'un SI

d. Vulnérabilités organisationnelles / gestion/ management

Absence des documents formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de SSI :

- Manque de maîtrise de la SSI ;
- Manque de définition des responsabilités;

⇒ **Bonnes pratiques...**

- Mettre en place une charte déontologique/éthique comprenant notamment des clauses relatives :
 - ✓ à la définition des responsabilités au sein du SI ;
 - ✓ aux procédures de sécurité ;
 - ✓ au respect de la législation et aux principales lois au sein du SI, etc.
- Examiner les plans organisationnels d'urgence et de sécurité régulièrement
- Procédures d'audit du SI.

Types de vulnérabilité d'un SI

e. Vulnérabilités mise en œuvre

Les vulnérabilités mise en œuvre peuvent être dues à la non prise en compte de certains aspects lors de la réalisation d'un projet.

- La non prise en compte des procédures de maintenance dans un projet d'acquisition et de mise en production d'un serveur de données.

⇒ **Bonnes pratiques...**

- Contrat de maintenance,
- Contrat de garantie.

Exemples de vulnérabilités d'un SI

- Mots de passe inexistant/faible/par défaut utilisé pour une longue durée,
- Mises à jours non effectuées,
- Transmission du trafic en clair sans procédé de chiffrement ;
- Protection insuffisante des clés cryptographiques,
- Traces inexploitées (pas d'audit - log)
- Disqualification des employés
- Manque de copies de sauvegarde,
- Manque de systèmes d'identification et d'authentification
- Téléchargement non contrôlé depuis internet

Types des menaces d'un SI

Menaces informatiques et non-informatiques

Menaces du SI	Menaces non-informatiques	Menaces informatiques
Menaces accidentelles	<ul style="list-style-type: none">- Sinistre (incendie, inondation, etc.);- Maladie d'un actif humain ;- etc.	<ul style="list-style-type: none">- Erreurs d'exploitation :<ul style="list-style-type: none">. Oubli de sauvegarde;. Ecrasement de fichiers;- Erreurs de manipulation des informations :<ul style="list-style-type: none">. Erreurs de saisie,. De transmission ou d'utilisation;
Menaces intentionnelles	<ul style="list-style-type: none">- Vol, sabotage et destruction du matériel;- Départ de personnels;- Grèves; stratégiques- etc.	<ul style="list-style-type: none">- Actions malveillantes visant à compromettre le triade DIC du SI:<ul style="list-style-type: none">- Déni de service,- Ecoute passive,- Virus;- etc. <div data-bbox="2076 1035 2356 1135">Attaques Informatiques</div>

Types des menaces d'un SI

Éléments de la politique de sécurité

- Défaillance matérielle : une bonne garantie avec support technique
- Défaillance logicielle (bugs) : MAJ + Correctifs (patches),
- Un sinistre (incendie, inondation, ...) : sauvegarde de données + sites de secours,
- Vol, sabotage et destruction du matériel, support de stockage : contrôle d'accès, mettre en place des dispositifs de surveillances (badge, surveillance vidéo, etc),
- Erreurs de manipulation des informations (erreurs de saisie, de transmission ou d'utilisation) : formation du personnel,

Classification des menaces d'un SI

- **Le furetage** est l'interception non autorisée de l'information
- **La modification** est la mise-à-jour non autorisée de l'information
- **L'écoute passive** est l'interception, généralement indétectable, de messages
- **L'écoute active** est la modification délibérée du flot de messages
- **La mascarade** est l'usurpation de l'identité d'une entité par une autre
- **Le refus d'approuver** l'origine est le refus de reconnaître avoir envoyé quelque chose
- **Le déni de réception** est le refus de reconnaître avoir reçu quelque chose
- **Le retard** est l'inhibition temporaire d'un service

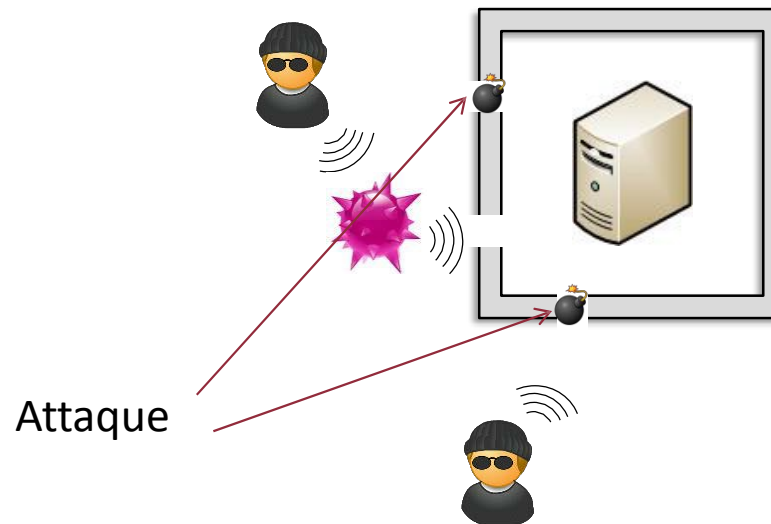
Classification des menaces d'un SI

- **Le dénie de service** est l'inhibition durable d'un service
- **Le feuilletage** est la recherche d'information dans la mémoire d'un ordinateur
- **La fuite** est la transmission d'informations à des utilisateurs non autorisés
- **L'inférence** est la déduction d'informations confidentielles sur un individu particulier par la mise en corrélation de statistiques
- **La falsification** est la modification délibérée d'informations dans la mémoire d'un ordinateur
- **La destruction** accidentelle est l'écrasement involontaire ou l'effacement d'informations

Attaques contre les SI

Attaque

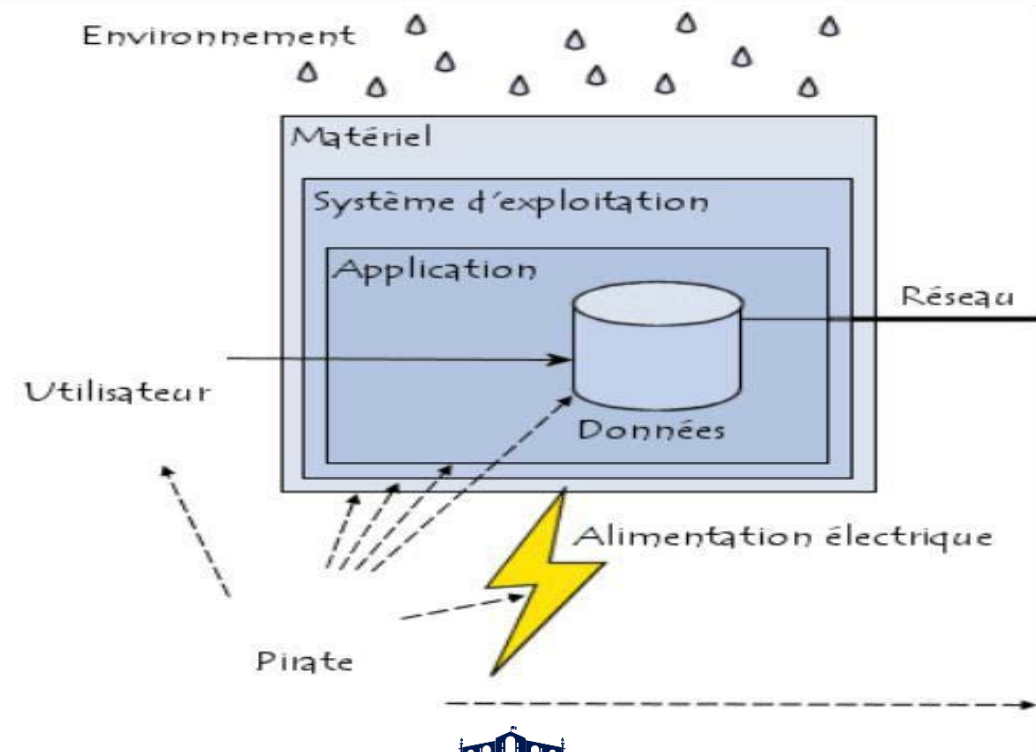
- ❑ C'est l'**exploitation** d'une **vulnérabilité** d'un SI:
 - Système d'exploitation,
 - Logiciel,
 - Utilisateur.
- ⇒ La **concrétisation** d'une **menace** ;



Attaques contre les SI

Les SI utilisent différentes composantes, allant de **l'électricité** pour alimenter les machines au **logiciel** exécuté via **le système d'exploitation** et utilisant le **réseau**.

⇒ **Les attaques** peuvent intervenir à chaque maillon de cette chaîne.



Attaques contre les SI

Accès physique

Il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :

- Coupure de l'électricité,
- Extinction manuelle des machines,
- Ouverture du boîtier de l'ordinateur et vol de disque dur.

Hacker

Hacker (to hack = découper quelque chose)

- Le terme « **hacker** » est souvent utilisé pour désigner un pirate informatique.
- Aujourd'hui ce mot est souvent utilisé pour désigner les personnes s'introduisant dans les **SI**.

⇒ Personne apte à modifier astucieusement un objet pour le destiner à un autre usage que celui prévu initialement

Hacker

Types de pirates

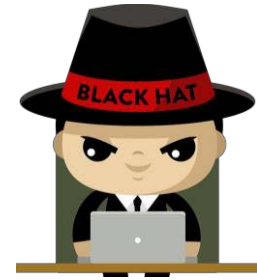
White hat - chapeau blanc (hacker éthique)

- Réalise des tests d'intrusion et d'autres méthodes de test afin d'assurer la sécurité des SI,
- Informer les propriétaires du SI des vulnérabilités existantes.



Black hat - chapeau noir (hacker mal intentionné)

- Réalise des actions malveillantes (modifier, voler, détruire, etc.):
 - **Phreakers**: s'intéressent au réseau téléphonique;
 - **Crackers**: casser la protection des logiciels payants, etc.



Grey hat - chapeau gris (hybride entre white et black)

- Son intention n'est pas forcément mauvaise,
- Il commet occasionnellement un délit pour des raisons qu'ils jugent éthiques



Hacker

Motivations des pirates

❑ Motivations des black hats:

- L'attrance de l'interdit ;
- L'intérêt/gain financier:
 - ✓ N° carte bancaire usurpé et réutilisé pour des achats en ligne,
 - ✓ Chantage,
 - ✓ Malware récents (ransomware - rançongiciel).
- Le désir de la renommée ;
- L'envie de nuire (détruire des données, empêcher un système de fonctionner).

❑ Motivations des white hats:

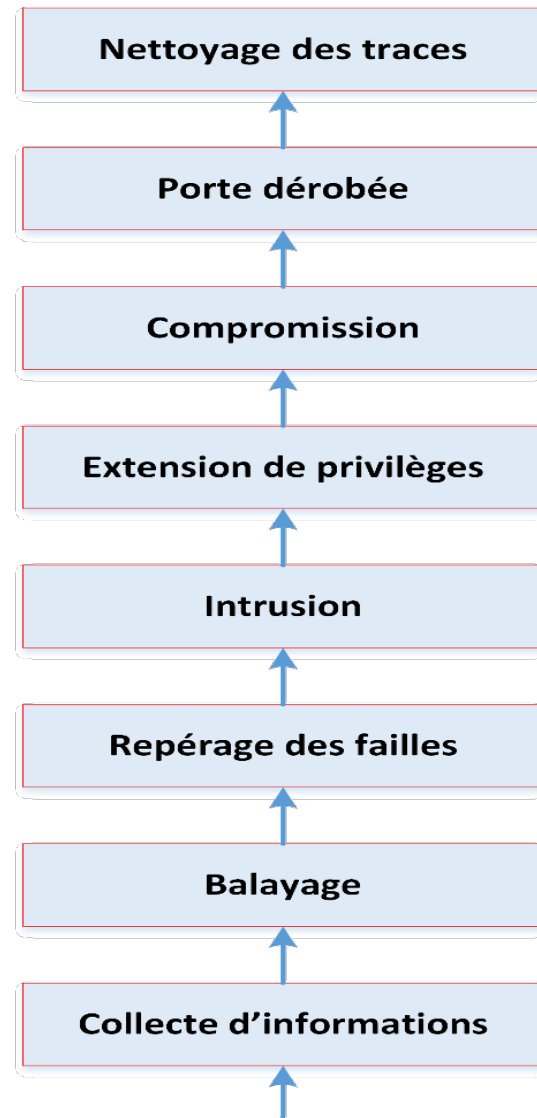
- L'apprentissage ;
- L'optimisation des SI ;
- Rendre la vulnérabilité immédiatement publique.

Hacker

Man-in-the-Middle (MITM) - l'homme du milieu

- Le but de l'attaquant est de surveiller tout le trafic réseau entre le client et le serveur, et de le modifier à sa guise pour l'obtention d'informations (mots de passe, clés de chiffrement, etc.).
- La plupart du temps, l'attaquant utilise les techniques de détournement de flux (par exemple DNS Spoofing) pour rediriger les flux du client et du serveur vers lui.

Méthodologie d'une attaque dans un SI



Méthodologie d'une attaque dans un SI

1. Collecte d'informations

(Prise d'empreinte - finger printing)

Récupérer le maximum d'informations sur le système cible:

- Systèmes d'exploitations, applications,
- Architecture/Topologie du réseau,
- Adressage IP,
- Noms de domaine,
- Protocoles de réseau,
- Services activés, etc.

Exemple: Les bases publiques d'attribution des adresses IP et des noms de domaine:

- <http://www.iana.net>
- <http://www.ripe.net> pour l'Europe
- <http://www.arin.net> pour les Etats-Unis

Méthodologie d'une attaque dans un SI

1. Collecte d'informations

Techniques utilisées:

➤ **Ecoute passive du réseau (Sniffing):**

- Ecouter le trafic pour capturer les informations qui y circulent;
- Utilisant un dispositifs **renifleur (sniffer)**;

Outils utilisés :

- Renifleur (Sniffer) : Wireshark (anciennement Ethereal), Dsniff, tcpdump, windump, etc.
- Website: <https://www.netcraft.com>

Méthodologie d'une attaque dans un SI

1. Collecte d'informations

Outils utilisés :


Website: <https://www.netcraft.com>



Background

Site title	ESI SBA	Date first seen	March 2020
Site rank	1113690	Netcraft Risk Rating ?	1/10 <div></div>
Description	Not Present	Primary language	English

Network

Site	https://www.esi-sba.dz ↗	Domain	esi-sba.dz
Netblock Owner	Chlef University	Nameserver	ns.esi-sba.dz
Hosting company	Network Internet Center.dz	Domain registrar	unknown
Hosting country	 DZ ↗	Nameserver organisation	unknown
IPv4 address	193.194.79.197 (VirusTotal ↗)	Organisation	unknown
IPv4 autonomous systems	AS3208 ↗	DNS admin	root@esi-sba.dz
IPv6 address	Not Present	Top Level Domain	Algeria (.dz)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown

SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	www.esi-sba.dz	Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC7301 application-layer protocol negotiation
Subject Alternative Name	www.esi-sba.dz	Issuer unit	Not Present
Validity period	From Feb 21 2022 to May 22 2022 (3 months)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	Apache	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	Not Present
Protocol version	TLSv1.3	Certificate Hash	IAq86O6+W5+ViT7Aiqq126PMMoU
Public key length	2048	Public Key Hash	a07f1a238fbc3437795fc72cb630eae8fad8c9812c07c2bbcae631a02d10007b
Certificate check	ok	OCSP servers	http://r3.o.lencr.org - 100% uptime in the past 24 hours Performance Graph
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	No response received

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Chlef University Chlef	193.194.79.197	Linux		30-Nov-2020

Méthodologie d'une attaque dans un SI

1. Collecte d'informations

Commandes utilisés :

host (linux) ou **nslookup** (windows)

⇒ Connaitre l'@ip d'un nom de domaine et l'inverse

```
(khaldi@kali)-[~]  
$ host dns.google  
dns.google has address 8.8.4.4  
dns.google has address 8.8.8.8  
dns.google has IPv6 address 2001:4860:4860::8844  
dns.google has IPv6 address 2001:4860:4860::8888
```

```
C:\>nslookup 8.8.8.8  
Serveur : UnKnown  
Address: 192.168.1.1  
  
Nom : dns.google  
Address: 8.8.8.8
```

Méthodologie d'une attaque dans un SI

1. Collecte d'informations

Commandes utilisés :

ping

⇒ Déterminer si les adresses publiquement accessibles sont actives ou non,

whois (linux)

(ou le site <https://www.whois.com/whois/>)

⇒ Recherche dans une BBD mondiale des noms de domaines, @ip, les informations publiques liées au nom de domaine demandé :

- Propriétaire du nom de domaine,
- Son adresse postale,
- Email, Numéro de téléphone,
- etc.

Méthodologie d'une attaque dans un SI

1. Collecte d'informations

Commandes utilisés :

tracert (linux), **tracert** (windows)

⇒ Lister les nœuds intermédiaires entre un point de départ et un point d'arrivée (Informe sur le routage des paquets).

```
C:\>tracert www.esi-sba.dz

Détermination de l'itinéraire vers www.esi-sba.dz [193.194.79.197]
avec un maximum de 30 sauts :

 1    <1 ms    <1 ms    <1 ms    192.168.1.1
 2    22 ms    22 ms    24 ms    41.96.0.1
 3    21 ms    21 ms    21 ms    10.103.31.37
 4    *        *        *        Délai d_attente de la demande dépassé.
 5    *        *        *        Délai d_attente de la demande dépassé.
 6    29 ms    28 ms    29 ms    172.28.16.61
 7    30 ms    30 ms    33 ms    172.28.16.62
 8    35 ms    31 ms    30 ms    172.17.116.2
 9    32 ms    31 ms    32 ms    172.17.116.85
10    33 ms    31 ms    31 ms    10.16.250.110
11    44 ms    43 ms    45 ms    172.16.100.50
12    42 ms    40 ms    41 ms    10.31.1.50
13    41 ms    41 ms    41 ms    193.194.79.197

Itinéraire déterminé.
```


Méthodologie d'une attaque dans un SI

2. Balayage du réseau

Déterminer à l'aide d'un outil logiciel quelles sont:

- Les adresses IP actives sur le réseau,
- Les ports ouverts correspondant à des services accessibles,
- Le système d'exploitation utilisé par les serveurs.

Techniques utilisées :

Interroger les services susceptibles :

- Serveurs Web (Hypertext Transfer Protocol – port 80)
- Serveurs FTP (File Transfer Protocol – port 21)
- Serveurs DNS (Domain Name Service – port 53),
- Serveurs NFS (Network File System – port 2049),
- Etc.

Méthodologie d'une attaque dans un SI

2. Balayage du réseau

Outils utilisés :

Siphon :

- Scanneur de ports (mappeur passif),
- Indétectables car il n'envoie pas de paquets.

Nmap :

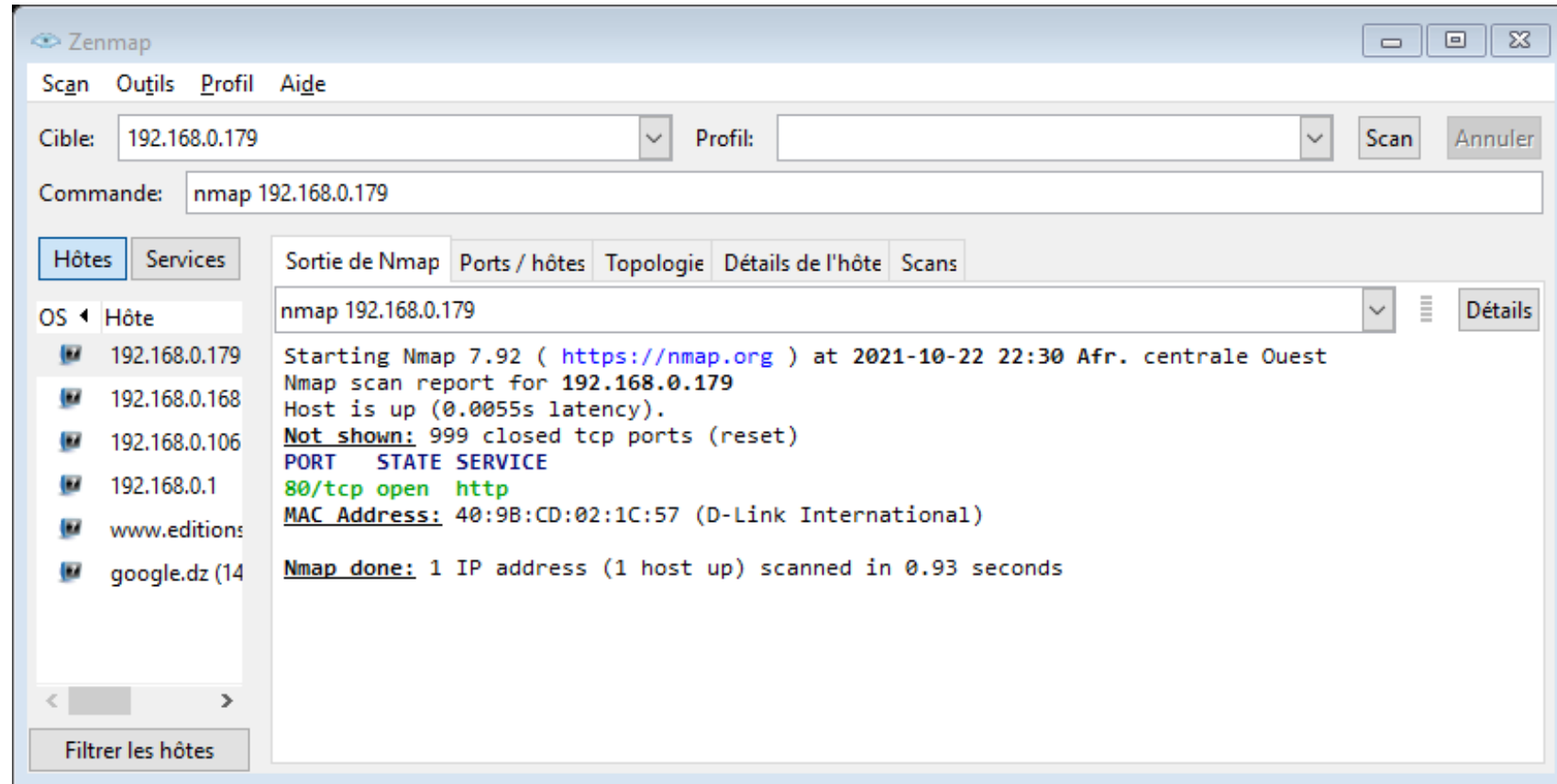
- Envoie des paquets TCP/ UDP sur un réseau;
- Analyse les réponses (pour chaque machine scannée) pour déterminer :
 - Les ports ouverts,
 - Le type de service ouvert.

Méthodologie d'une attaque dans un SI

2. Balayage du réseau

Outils utilisés :

Nmap (Logiciel)



Méthodologie d'une attaque dans un SI

2. Balayage du réseau

Outils utilisés :

Nmap

(Commande linux)

```
(khaldi@kali)-[~]  
$ nmap 192.168.1.*  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-11 13:51 EST  
Nmap scan report for 192.168.1.1  
Host is up (0.0056s latency).  
Not shown: 995 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
23/tcp    open  telnet  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap scan report for 192.168.1.3  
Host is up (0.012s latency).  
Not shown: 988 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsure  
912/tcp   open  apex-mesh  
3306/tcp  open  mysql  
49152/tcp open  unknown  
49153/tcp open  unknown
```

Méthodologie d'une attaque dans un SI



3. Repérage des failles

a. Consulter les failles recensées :

- Etablir des tests d'intrusion pour découvrir les failles de sécurité des applications.

Exemple d'outil de test d'intrusion: **Metasploit** (*Pen Testing Tool*)

- Utiliser des scanners de vulnérabilité: **Nessus**, **SAINT** (problème de discrétion)

SecurityFocus (BDD en ligne)

(<https://bugtraq.securityfocus.com/archive>)

- Exemples de vulnérabilités: services jugés faibles :

- ✓ La commande Telnet ,

- ✓ Les commandes **R** de **Berkeley** : rsh (Remote Shell), rlogin (Remote Login), rcp (remote copy)

- ⇒ Peu sécurisées (connexion en claire entre les deux hôtes)

- ⇒ On suggère par exemple de remplacer par SSH,

Méthodologie d'une attaque dans un SI

3. Repérage des failles

b. Éliminer les failles non fondées :

- Les **failles non fondées** : les failles concernant des services qui ne sont pas utilisés sur la machine cible,
- but :
 - Ne pas avoir une longue liste d'**exploits** à tester, afin de rester le plus discret possible;
 - Seuls les **exploits** touchant des failles exploitables doivent être testés.

Méthodologie d'une attaque dans un SI



4. Intrusion

(Création de l'attaque)

Plusieurs méthodes sont utilisées par les pirates

- L'exploitation des vulnérabilités (Ex: **Metasploit**),
- Installation des Malwares (**virus, vers, chevaux de Troie, ...**),
- Modification / destruction/ vol des données,
- Cassage de mots de passe :
 - Attaque par **force brute** (*brute force*): faire des essais dans l'ordre jusqu'à trouver le bon mot de passe,
 - Attaque par **dictionnaire** (à partir d'une liste prédéfinie qui contient les mots de passe les plus courants),
- Etc.

Méthodologie d'une attaque dans un SI

5. Extension des privilèges :

- Augmenter ses privilèges en obtenant l'accès root/super utilisateur afin de contrôler une plus grande partie du SI.
- Pour avoir cet accès le pirate utilise différents techniques :
 - Ecouter le trafic par un sniffer et intercepter le compte superuser,
 - Consulter les annuaires du SI, la messagerie ou les partages de fichiers, etc.
 - Appuyer sur les vulnérabilités des commandes **R** de **Berkeley** : rsh, rlogin, rcp, ...

6. Compromission :

- Lorsqu'un accès administrateur est obtenu, on parle alors de compromission de la machine

Méthodologie d'une attaque dans un SI

7. Backdoor (Porte dérobée - Trappe):

(Assurer son accès/Faciliter son retour)

Le pirate installe une porte dérobée afin de créer artificiellement une faille de sécurité (accès secret) qui va lui permettre de revenir à la machine compromise.

Portes dérobées – backdoors : outils logiciels (s'exécutent dans les systèmes sans être détectés) permettant d'entrer dans la machine même si tous les mots de passe ont été changés;



Méthodologie d'une attaque dans un SI

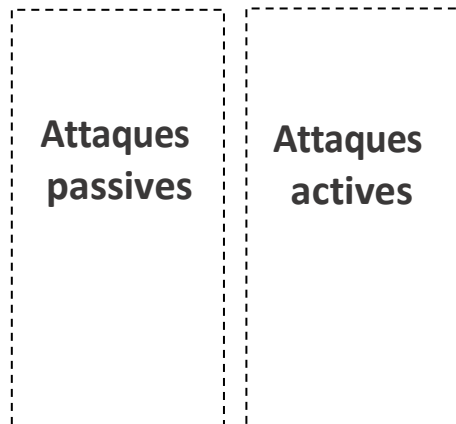
8. Nettoyage des traces :

Afin de ne pas laisser des soupçons à l'administrateur de la machine/du réseau compromis, le pirate doit nettoyer les traces de l'attaque :

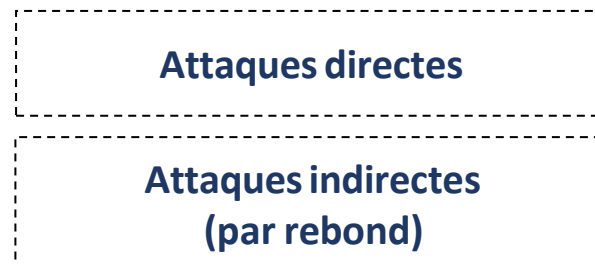
- Supprimer les fichiers créés,
- Remettre en propre tous les fichiers modifiés,
- Nettoyer les fichiers de logs (historique) des machines dans lesquelles il s'est introduit (Ne pas effacer les fichiers journaux mais les modifier pour enlever les traces) :
 - Linux : dossier /var/log;
 - Windows : Observateur d'événement : C:\Windows\System32\winevt\Logs
- Masquer les actions, services lancés, l'historique de ses commandes, etc. en utilisant des outils (**rootkits**).

Classification des attaques informatiques

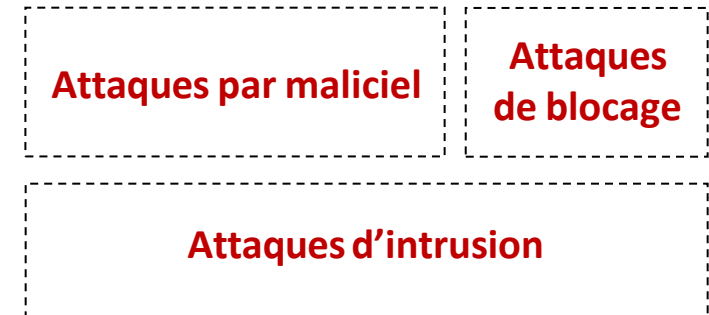
(1)



(2)



(3)

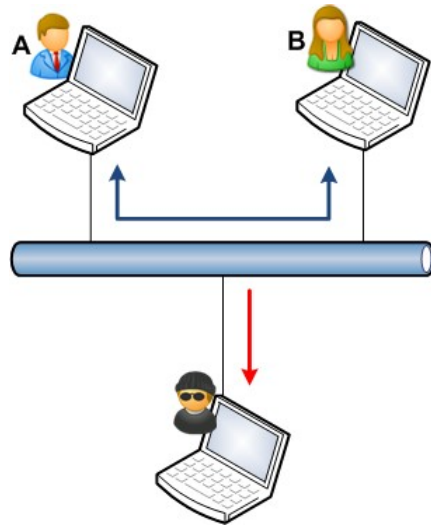


Classification des attaques informatiques

(1)

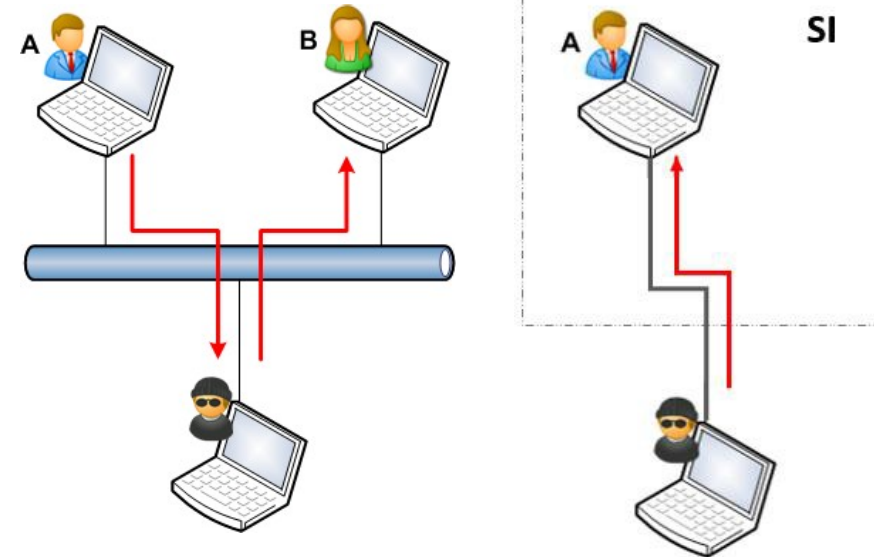
Attaques passives	Attaques actives

Attaques passives



Ecoute / Interception du trafic entre A et B,
(atteinte à la **confidentialité** du SI).

Attaques actives



Modification/ Interruption/ Fabrication / Dénî de service
pour un SI,
(atteinte à la **disponibilité**, **intégrité**, **authenticité** du SI).

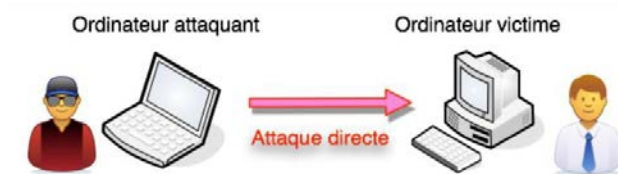
Classification des attaques informatiques

(2)

Attaques directes

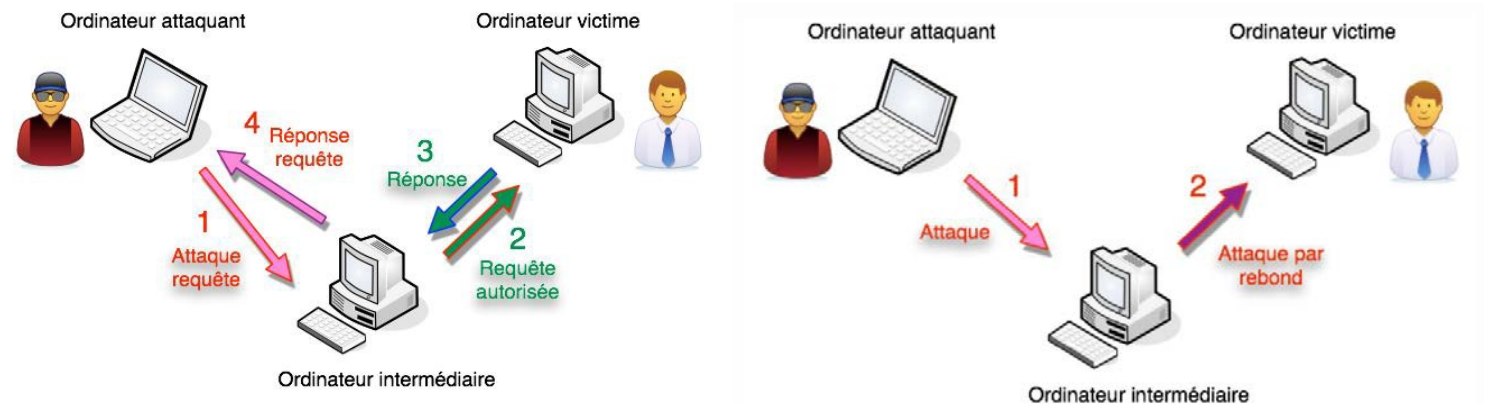
Attaques indirectes
(par rebond)

Attaques directes



- Possible de remonter à l'origine de l'attaque.

Attaques indirectes (par rebond)



- + Masquer l'identité (l'adresse IP) du hacker,
- + Peut utiliser les ressources du rebond (CPU, bande passante,...) pour attaquer.

Classification des attaques informatiques

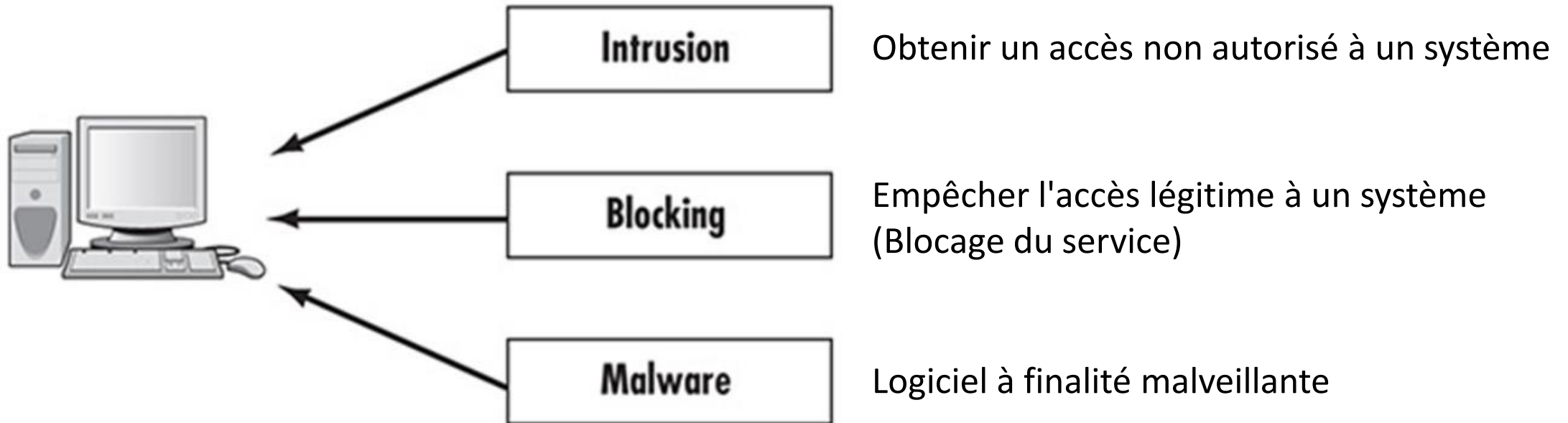
(3)

Attaques par logiciel

Attaques de blocage

Attaques d'intrusion

(3)



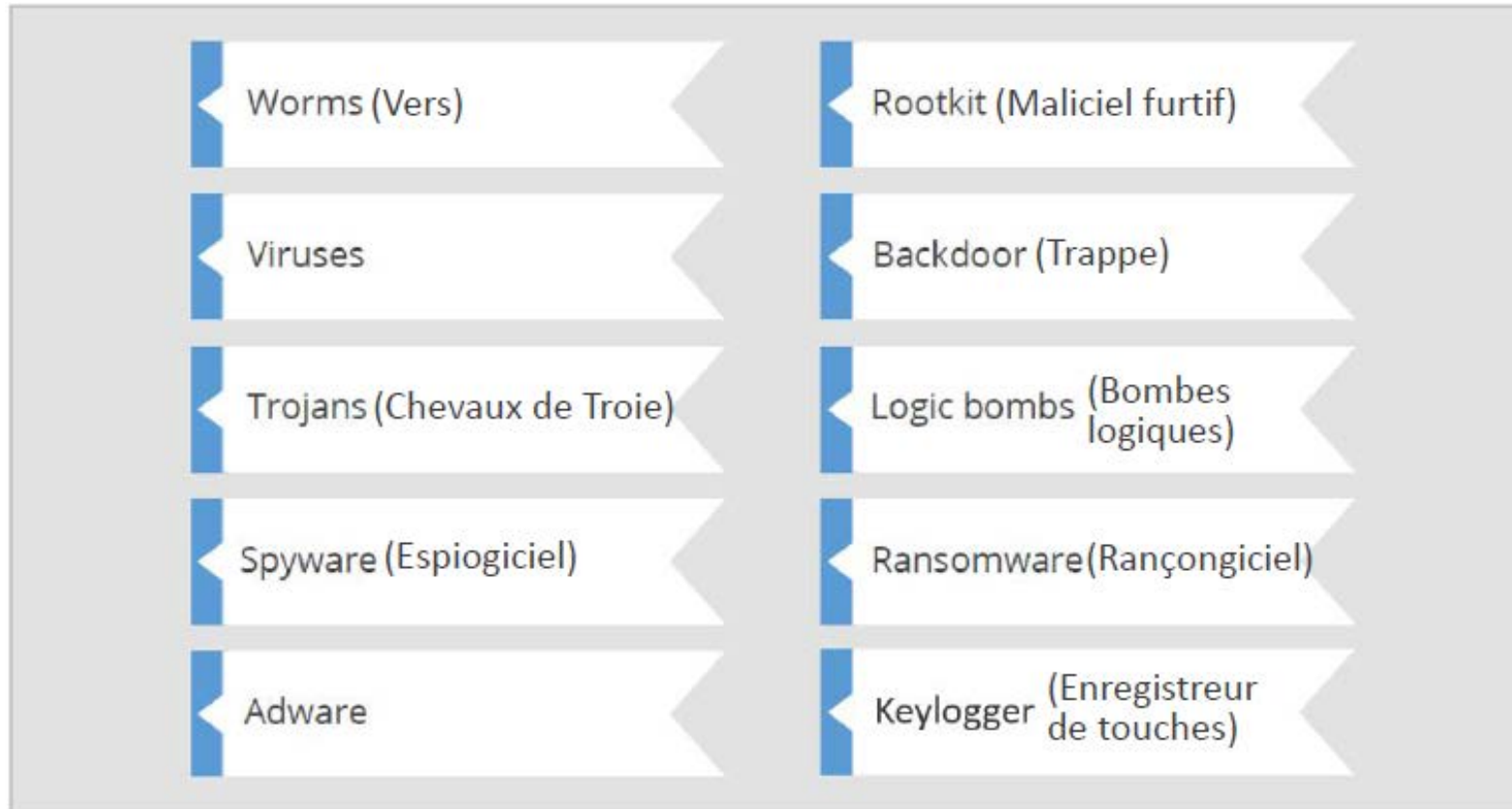
Attaques par Maliciel (Malware)

(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion



Attaques par Maliciel (Malware)

Virus

Code malveillant qui :

- S'**implante** dans le corps d'un autre,
- Se **réplique** (se multiplie) **localement**,
- Se **reproduit** (propage) par les réseaux et les supports amovibles,
- Nécessite une **intervention** pour infecter une machine (télécharger un fichier, ouvrir une pièce jointe, etc.),
- Peut supprimer des fichiers, endommager le système ou modifier ses paramètres, etc.

Types de virus:

- **Résident en mémoire** : s'installe puis reste dans la RAM,
- **Virus mutant** : virus clone, réécrit par d'autres utilisateurs,
- **Virus macro** : infecte les fichiers bureautiques : word, excel, etc.,
- **Virus polymorphe** : modifie automatiquement leur signature,
- **Virus de secteur d'amorçage** : infecte le secteur de démarrage d'un disque dur.

(3)



Shamoon (2012)

- ✓ Virus pour Microsoft windows,
- ✓ Voler des données des systèmes des entreprises énergétiques.

Attaques par Maliciel (Malware)

Virus

(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion

Un exemple de virus qui ouvre le lecteur CD infiniment.

```
Set oWMP = CreateObject("WMPlayer.OCX.7")
Set colCDROMs = oWMP.cdromCollection
do
if colCDROMs.Count >= 1 then
For i = 0 to colCDROMs.Count - 1
colCDROMs.Item(i).Eject
Next
For i = 0 to colCDROMs.Count - 1
colCDROMs.Item(i).Eject
Next
End If
wscript.sleep 5000
loop
```

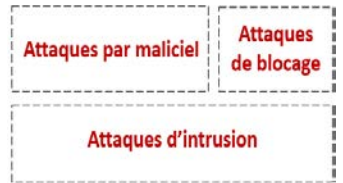
File.bat



Attaques par Maliciel (Malware)

Worm (Ver)

(3)



Code malveillant **indépendant** :

- Ne s'implante pas sein d'un autre programme,
- Se reproduit (propage) sur plusieurs machines par l'Internet ou tout autre réseau (virus réseau),
- Auto-répliquant : **ne requiert aucune intervention** de l'utilisateur pour se déclencher,
- Se propagent principalement grâce à la messagerie et grâce à des fichiers attachés.



WannaCry (Ver et Ransomware)

- ✓ Utilise l'exploit EternalBlue (NSA 2017),
- ✓ Chiffre les fichiers de l'utilisateur et lui demandait une rançon,
- ✓ Détecter les appareils vulnérables dans le réseau, s'y installer et répéter l'opération,
- ✓ Environ 4 milliards de dollars de dommages.

Attaques par Maliciel (Malware)

Trojan (Cheval de Troie)

(3)



Un programme effectuant une **fonction illicite** tout en donnant l'apparence d'effectuer une **fonction légitime**:

- Divulguer des informations,
- Ouvrir une porte dérobée,
- Etc.



WinZip

- ✓ Outil de compression/décompression des fichiers,
- ✓ Fut, durant de nombreuses années, un cheval de Troie.

KeyGen

- ✓ Pirater des logiciels et obtenir des clés de licence,
- ✓ Un trojan piégé d'un backdoor.

Attaques par Maliciel (Malware)

Rootkit (maliciel furtif)

(Outil de dissimulation d'activité)

Un ensemble de programmes (outils) permettant au pirate d'accéder à distance à un SI :

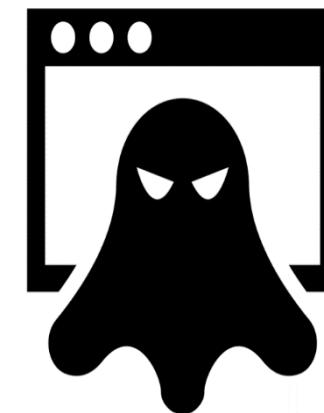
- S'utilise après une intrusion et l'installation d'une **porte dérobée**,
- Permet de camoufler la mise en place d'une porte dérobée,
- Opère des modifications sur les commandes systèmes.

👉 L'installation d'un rootkit nécessite des droits d'administrateur.

Peut intervenir à **plusieurs niveaux** :

- Matériel/micrologiciel : s'implanté dans les firmwares (bios),
- Hyperviseur : il devient l'hyperviseur => OS devient invité chez le rootkit,
- Noyau : s'intègre au niveau de noyau du système d'exploitation,
- Bibliothèque : Remplace des appels système par du code malveillant,
- Applicatif : intégrer du code malveillant aux applications.

(3)



Necurs

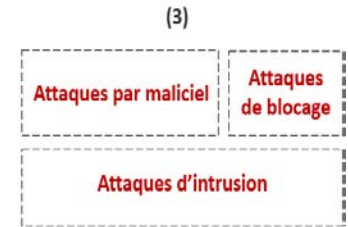
- ✓ Prendre le contrôle du système d'exploitation, sans alerter les mécanismes de sécurité du système)..

TDSS

- ✓ S'implanter dans l'ordinateur avec des privilèges plus élevées.

Attaques par Maliciel (Malware)

Spyware (Espionnage)



Programme espion avec des objectifs de commerce et de renseignement :

- Transmettre les habitudes d'un internaute (traçabilité des URL des sites visités),
- Affecte la **confidentialité** des données:
 - Mots de passe saisis,
 - Informations de paiement (numéro de carte, code secret, ...),
 - etc.

Types de spyware :

- Externe : programme autonome,
- Interne : spyware intégré (code parasite - routine) dans le code d'un programme.



CoolWebSearch

- ✓ Exploite des vulnérabilités d'Internet Explorer pour :
 - Modifier les paramètres
 - Envoyer des données à son auteur.

Gator

- ✓ Surveiller les habitudes de navigation des victimes sur le Web.

Attaques par Maliciel (Malware)

Keylogger (enregistreur de touches)

(3)



Dispositif d'espionnage chargé d'enregistrer les **frappes** de touches du **clavier** et les **envoyer** au pirate.

Certains keylogger peuvent :

- Enregistrer les URL visitées, les emails consultés/envoyés, etc.
- Créer une vidéo retraçant toute activité de l'ordinateur;
- Si pas d'internet, un fichier caché (crypté) est créé puis envoyé lors d'internet.

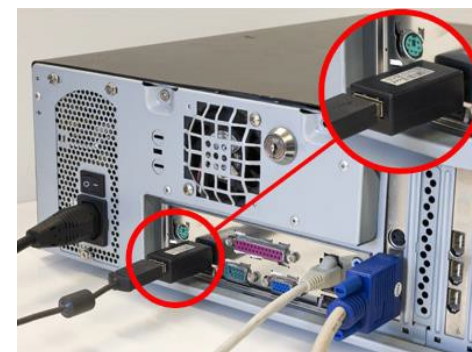
Types de keyloggers :

- Logiciel : Se lance au démarrage de la machine,
- Matériel : branché entre l'ordinateur et le clavier.



Phoenix (windows)

- ✓ Captures d'écran,
- ✓ Télécharger et installer d'autres malwares.



Attaques par Maliciel (Malware)

Adware

(3)



Logiciel malveillant qui :

- Affiche des publicités sans fin et des fenêtres contextuelles (pop-up),
- Ne peut pas être arrêté par les bloqueurs de pop-up traditionnels.



Fireball

- ✓ Change la page d'accueil et le moteur de recherche en 'Trotux',
- ✓ Insère des publicités intrusives,
- ✓ Empêche la modification des paramètres du navigateur.

Appearance

- ✓ Grand nombre de publicités dans le navigateur, ce qui rend la navigation presque impossible.

Attaques par Maliciel (Malware)

Logic bombe (Bombe logique)

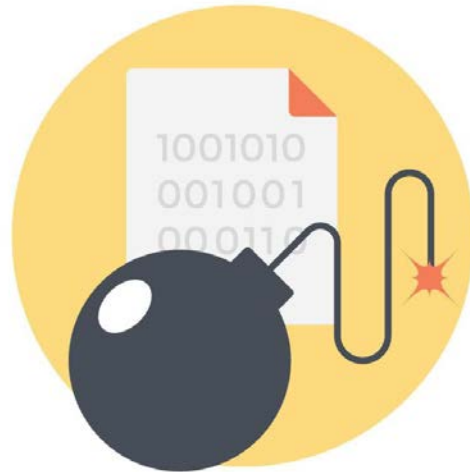
(3)



Programme malveillant qui infecte un système et restent en sommeil jusqu'à ce qu'elles soient déclenchées par une condition spécifique.

Types de bombes logiques:

- Bombe logique : qui se déclenche par une action (lancement d'une commande, appel système, etc.),
- Bombe à retardement : qui se déclenche avec une date.



CIH (Tchernobyl) 26/04

- ✓ a vidé les disques durs de toutes leurs informations et
- ✓ a endommagé le BIOS de certaines cartes mères.

Attaques par Maliciel (Malware)

Ransomware (Rançongiciel)

(3)



Logiciel malveillant qui prend **en otage** des données personnelles / **contrôle** de la machine :

- En **chiffrant** les données et les fichiers,
- Puis **demander** au propriétaire de **payer la rançon** en échange de la clé qui permettra de les **déchiffrer**.



CryptoLocker

- ✓ Chiffre les fichiers (chiffrement asymétrique),
- ✓ Puis affiche un message de devoir payer une rançon.

Attaques de déni de service (Denial of Service – DoS)

(3)

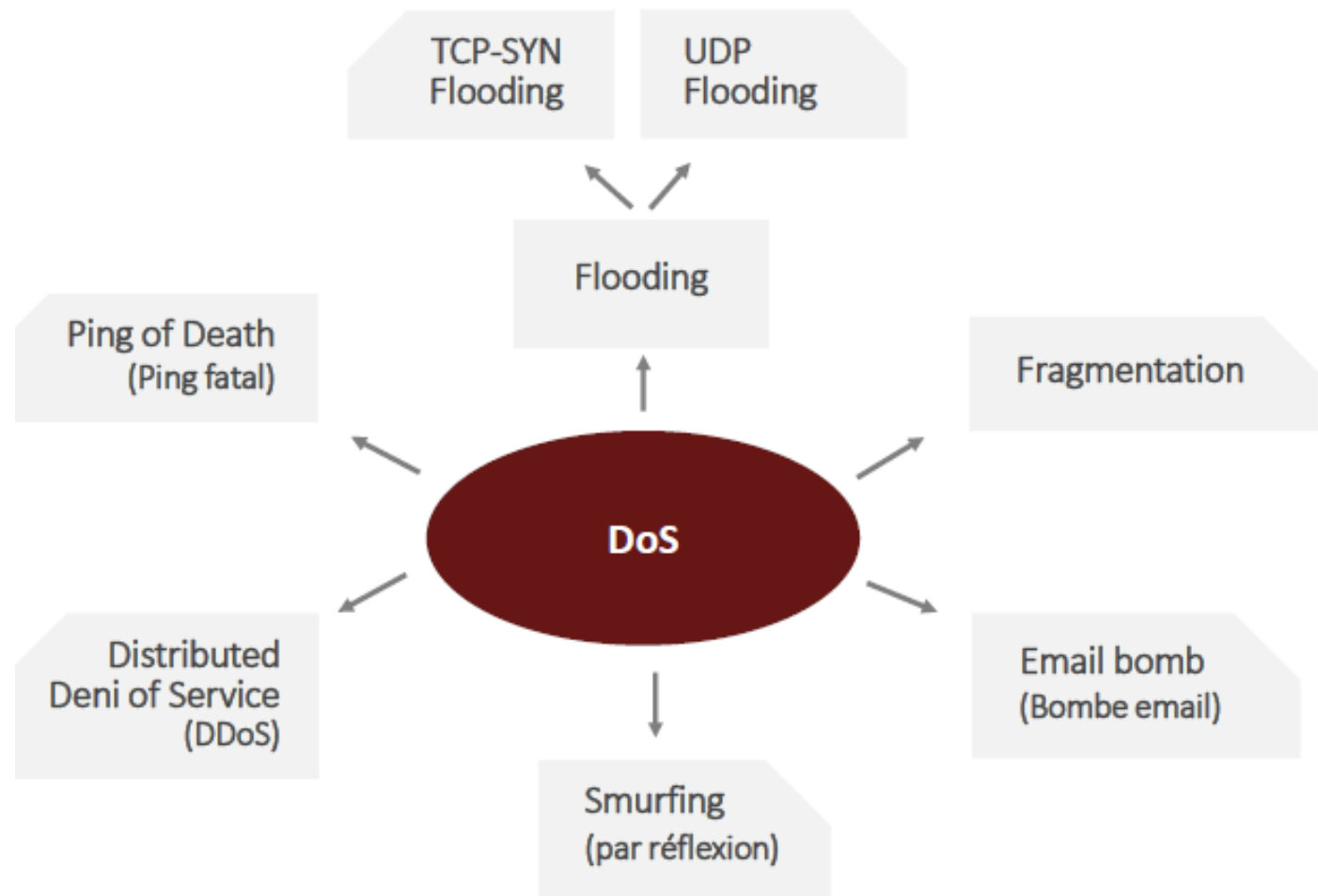
Attaques par maliciel

Attaques de blocage

Attaques d'intrusion

Empêcher l'accès légitime à un système / l'utilisation d'un service en provoquant la saturation d'une des ressources du SI: bande passante, mémoire, puissance de calcul, capacité de stockage, etc.

Mettre le système hors-service (Blocage du service)



Attaques de déni de service (Denial of Service – DoS)

Ping fatal (Ping of Death – PoD)

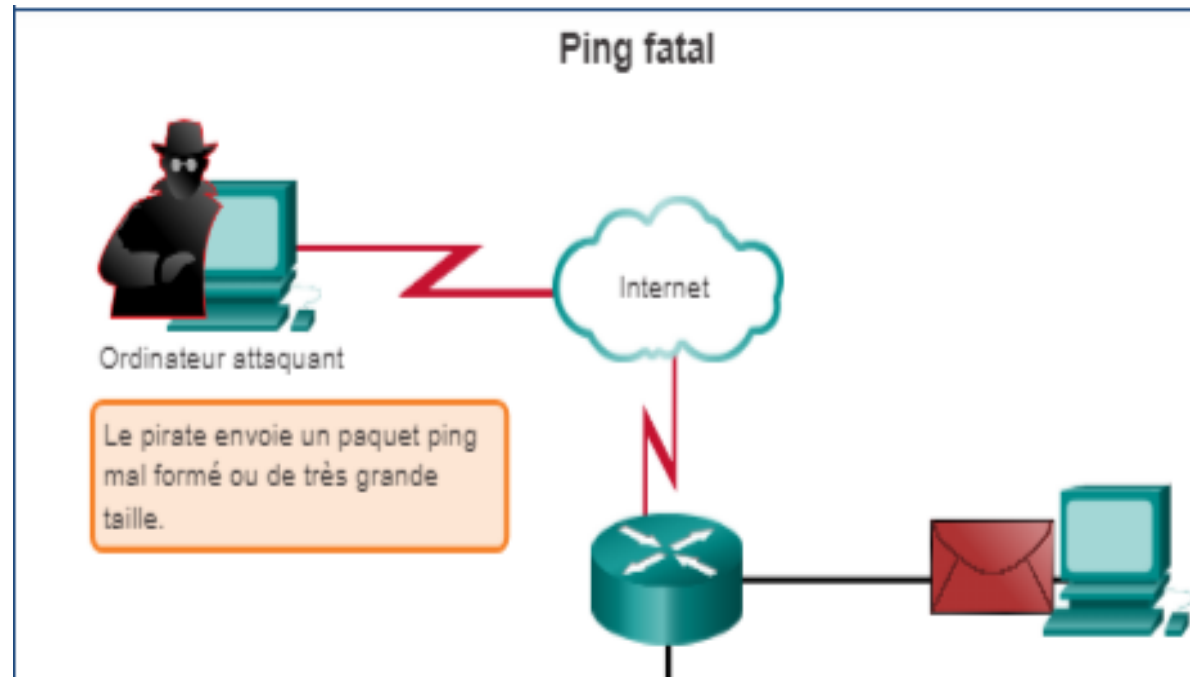
(3)



Envoi de paquet **ping** (echo-request) mal formé à la machine cible et attend une réponse (Reply).

⇒ Bloquer, arrêter ou redémarrer la cible.

N.B: PoD devient moins courante avec les nouvelles versions des SE (qui suppriment les paquets surdimensionnés).



Exemple:

Le pirate envoie un paquet **ping** mal formé de très grand taille (que celle autorisée)

(Commande)

```
ping 192.168.0.179 -l 65510 -w 1 -n 1
```

(Fichier bat)

```
:loop  
ping <192.168.0.179> -l 65510 -w 1 -n 1  
goto :loop
```

Attaques de déni de service (Denial of Service – DoS)

Email bomb (email bombe)

(3)

Attaques par maliciel

Attaques de blocage

Attaques d'intrusion

Envoyer de gros ou de nombreux fichiers à un/plusieurs utilisateur(s):

- Saturer l'espace de sa boîte mail (serveur de mails),
- Le rend inaccessible (en panne),
- Saturer la bande passante du serveur de mails.

Exemples :

- Envoyer des fichiers compressés qui se décompressent en très gros fichiers,
- Réseaux botnets (milliers voire millions d'ordinateurs envoient des emails),
- S'inscrire l'adresses email du victime à plusieurs listes de diffusions (forums de discussion).



Attaques de déni de service (Denial of Service – DoS)

SYN Flood (Inondation SYN)

S'applique dans le cadre du protocole **TCP**:

Une connexion **TCP** normale se déroule en trois étapes (**Three-way handshake**):

- Le client demande une connexion en envoyant un message **SYN** (**synchronize**) au serveur,
- Le serveur accepte en envoyant un message **SYN-ACK** (**synchronize-acknowledgment**) vers le client,
- Le client répond à son tour avec un message **ACK** (**acknowledgment**) pour établir la connexion.

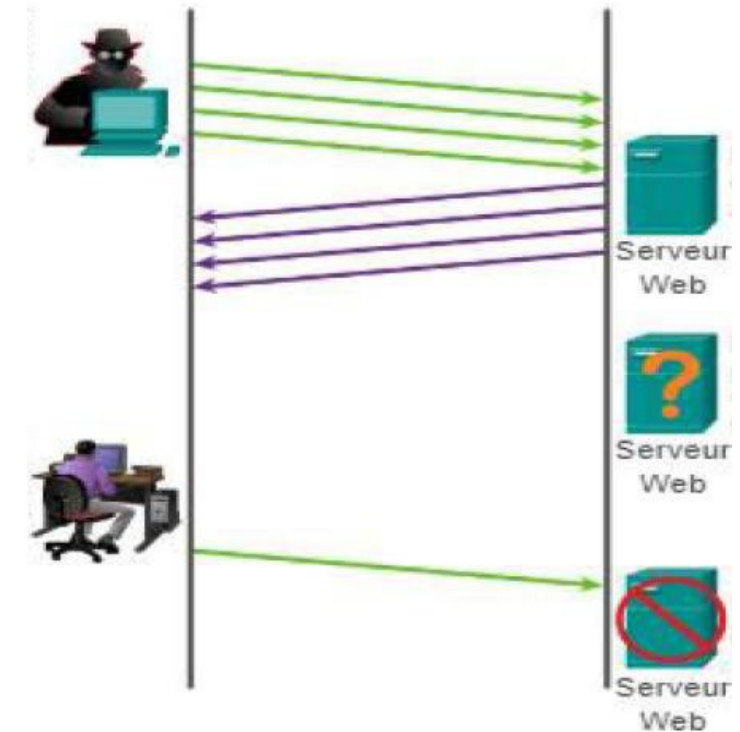
Un pirate envoie à la cible (serveur) une succession de requêtes **SYN** (demandes de connexion) avec @sources différentes (spoofed IP) vers la cible sans les jamais terminer (sans envoyer un **ACK** pour établir la connexion).

⇒ Connexion **semi-ouverte**:

- Réserve alors de plus en plus de ressources (ports, mémoire, bande passante,...) du côté serveur.

⇒ La cible (serveur) devient inaccessible/indisponible (surcharge des ressources).

(3)



Attaques de déni de service (Denial of Service – DoS)

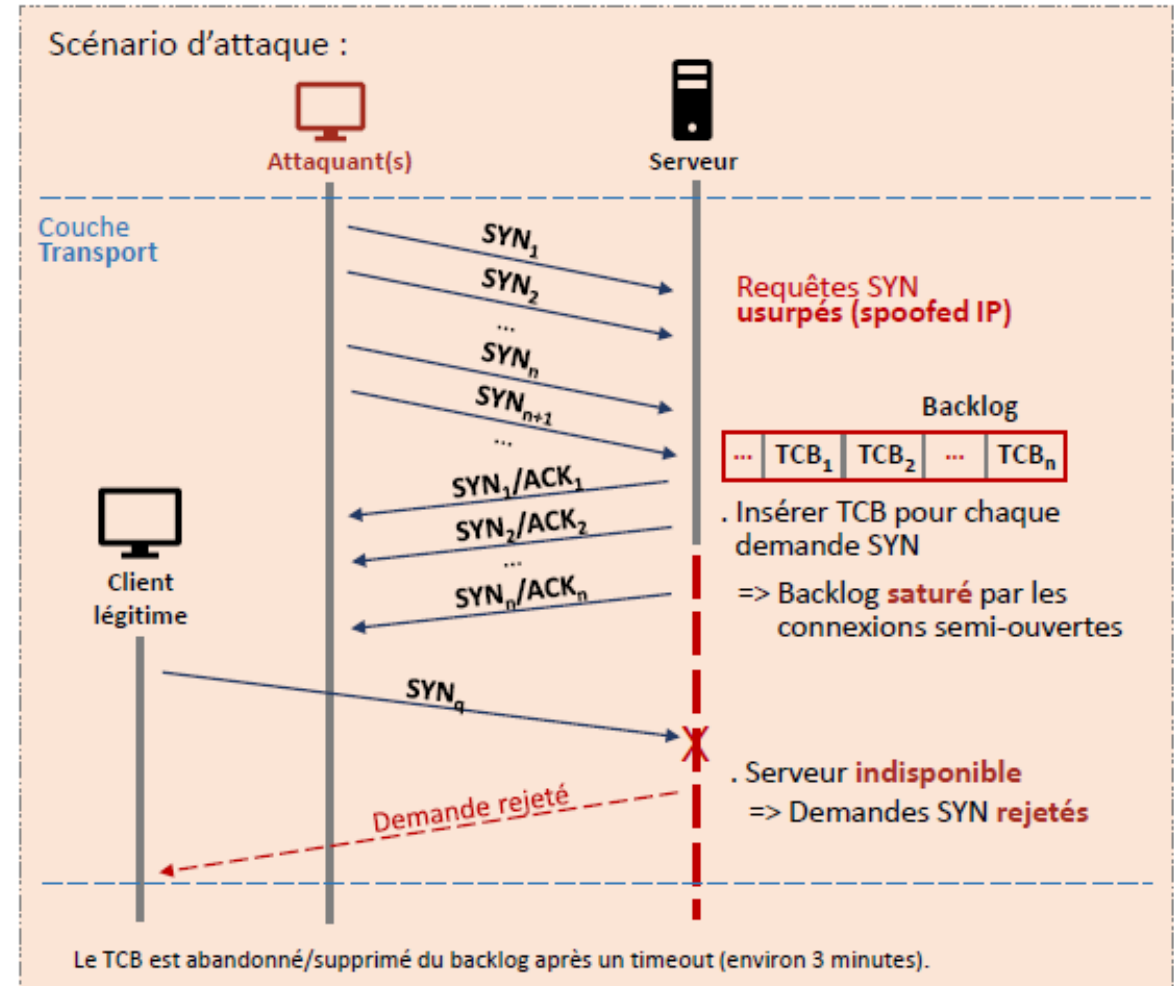
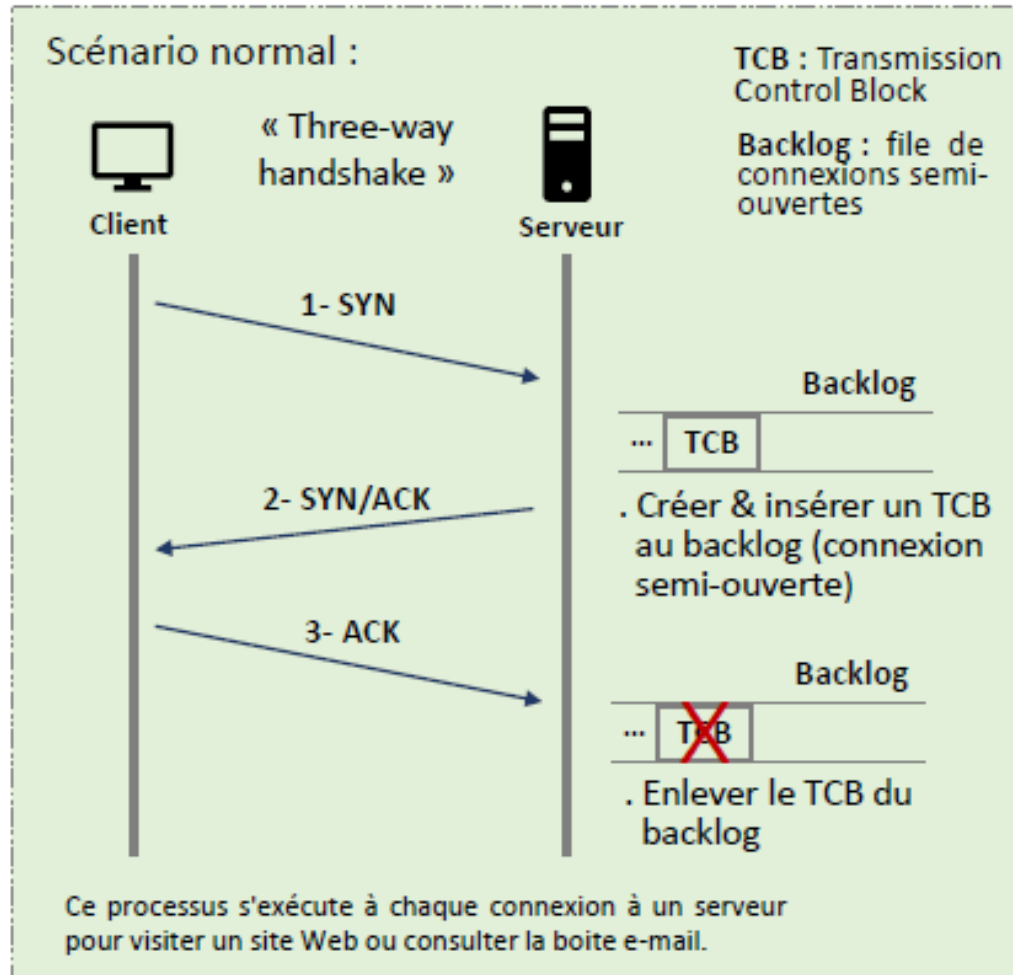
SYN Flood (Inondation SYN)

(3)

Attaques par maliciel

Attaques de blocage

Attaques d'intrusion



Attaques de déni de service (Denial of Service – DoS)

SYN Flood (Inondation SYN)

(3)



Exemple d'attaque :

```
#hping3 -S -p <port> <@IP> -c <nombre_paquets>
```

s: SYN p: numéro de port c: nombre de requêtes SYN

```
(root@kali)-[~]
# hping3 -S -p 80 192.168.44.1 -c 1000
HPING 192.168.44.1 (eth0 192.168.44.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.44.1 ttl=128 DF id=1732 sport=80 flags=RA seq=0 win=0 rtt=4.9 ms
len=46 ip=192.168.44.1 ttl=128 DF id=1733 sport=80 flags=RA seq=1 win=0 rtt=5.1 ms
len=46 ip=192.168.44.1 ttl=128 DF id=1734 sport=80 flags=RA seq=2 win=0 rtt=7.6 ms
len=46 ip=192.168.44.1 ttl=128 DF id=1735 sport=80 flags=RA seq=3 win=0 rtt=7.6 ms
```

hping3 : outil réseau capable d'envoyer des paquets TCP/IP sur commande,
hping3 traite la fragmentation, les contenus de paquets et les tailles arbitraires.

Attaques de déni de service (Denial of Service – DoS)

UDP Flood

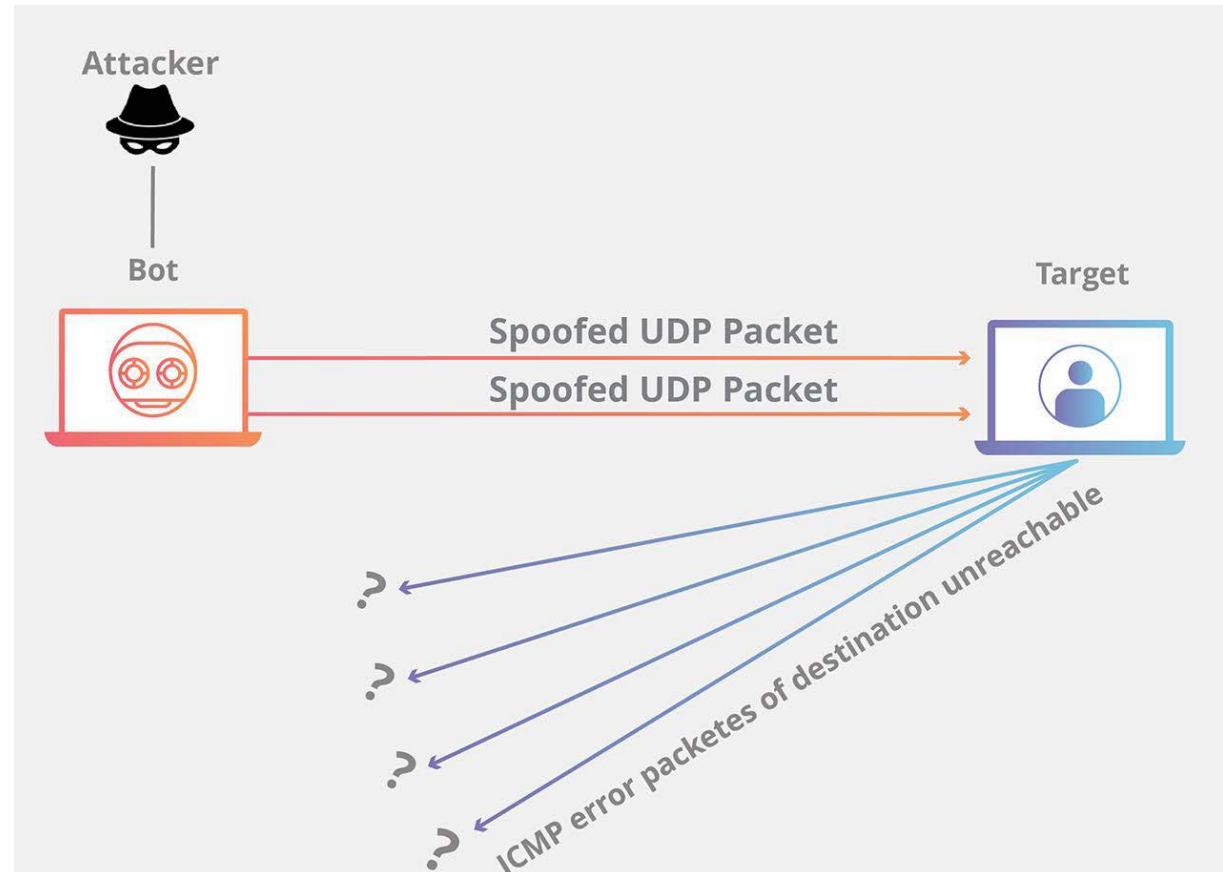
S'applique dans le cadre du protocole **UDP** (de même manière que SYN flooding) ;

Envoyer à la cible (serveur) un grand nombre de requêtes UDP avec **@source(s) différente(s) (spoofed IP)** et numéros de **ports aléatoires**:

- ⇒ Troubler/submerger le serveur (réception des requêtes UDP et renvoi des paquets ICMP),
- ⇒ Saturer le trafic.

UDP : User Datagramme Protocole
Le trafic **UDP** est prioritaire que le trafic **TCP**

(3)



Attaques de déni de service (Denial of Service – DoS)

UDP Flood

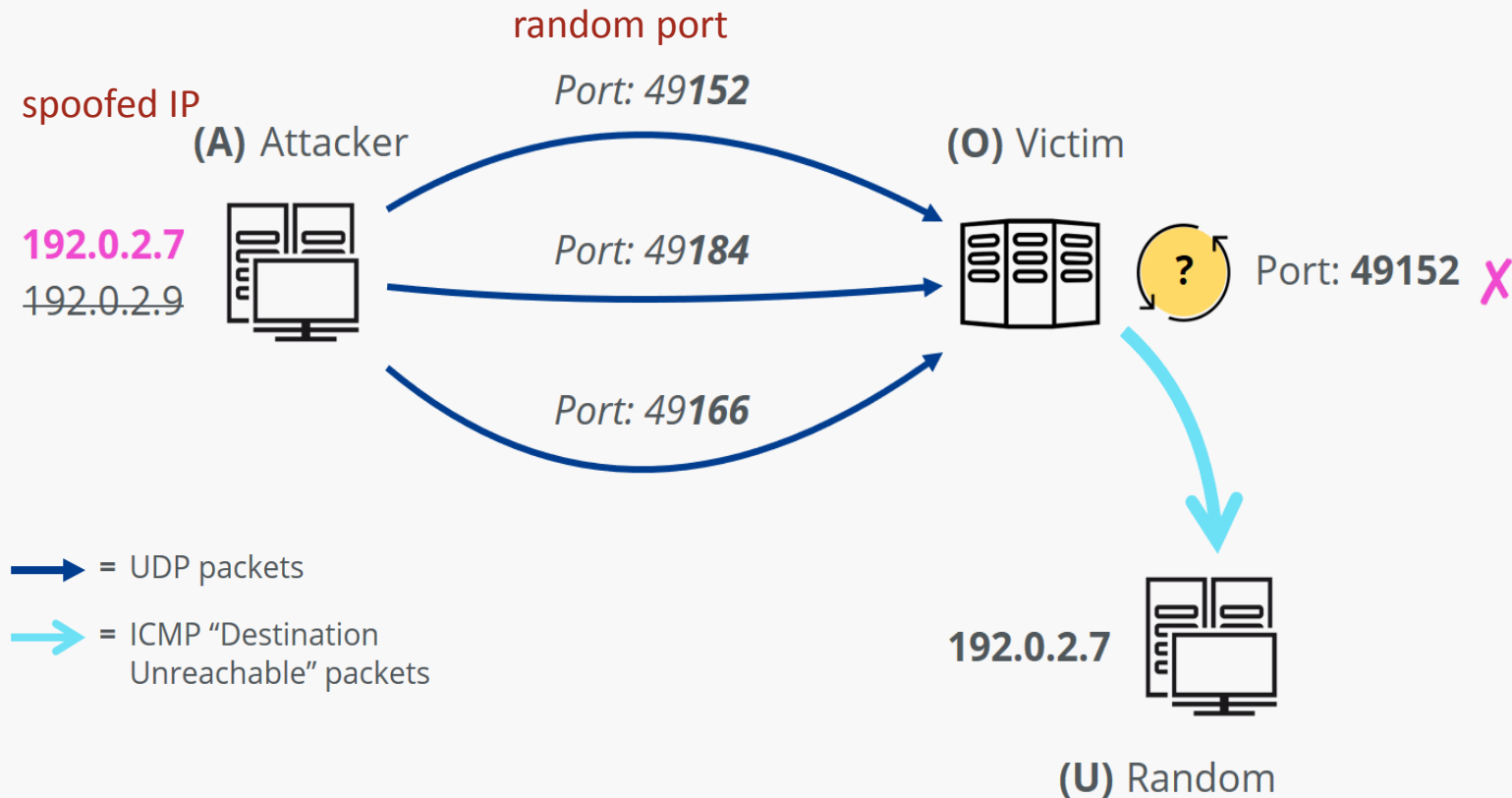
(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion

Scénario d'attaque :



Attaques de déni de service (Denial of Service – DoS)

Déni de service distribué (Distributed Denial of Service – DDoS)

(3)

Attaques par maliciel

Attaques
de blocage

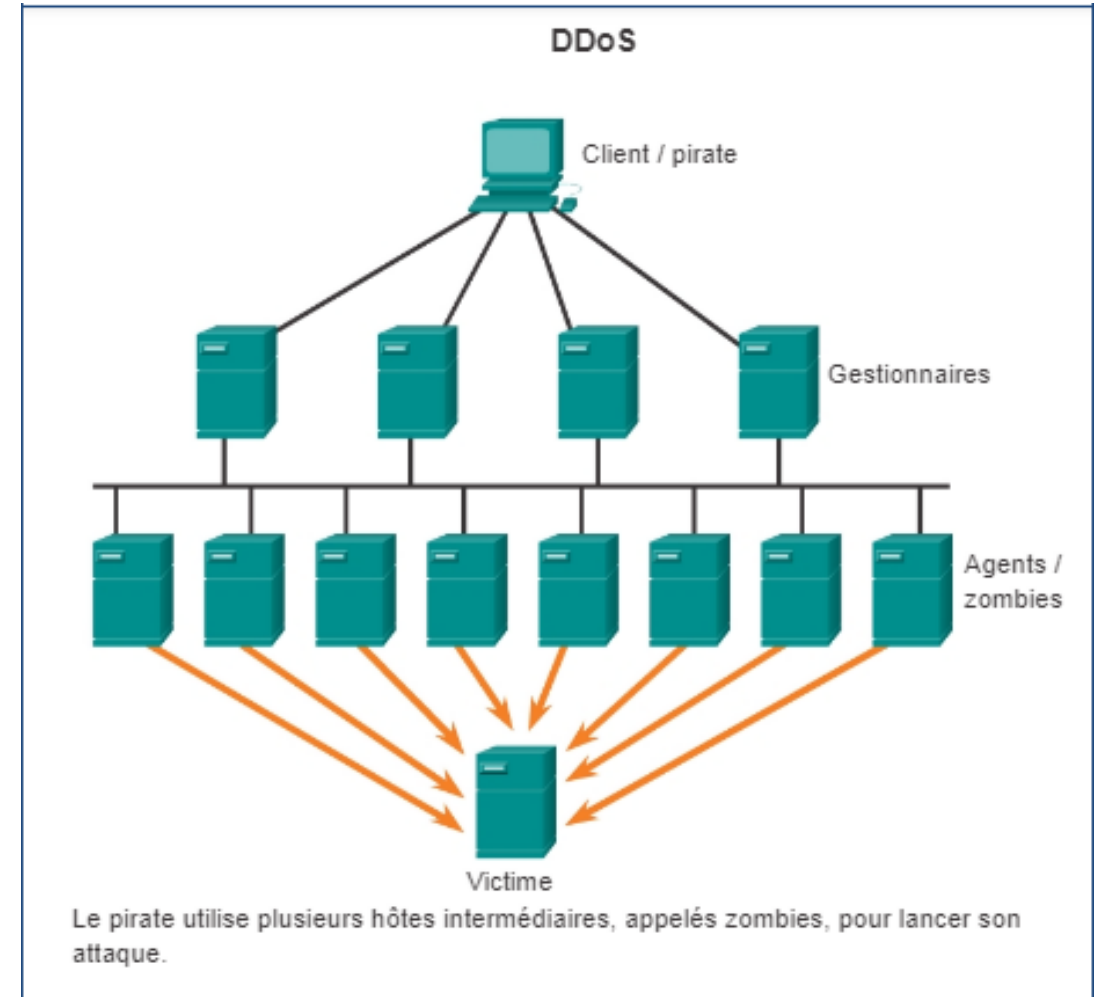
Attaques d'intrusion

Attaque DoS émise depuis **plusieurs** origines distinctes (réseau de zombies - **Botnet**) contrôlées par l'attaquant ;

Inonder la cible (épuiser ses ressources) par grand nombre de requêtes.

⇒ Complexe à bloquer (difficile de différencier entre une vraie requête d'une requête DDoS).

Botnet (robot network) : réseau d'ordinateurs (Milliers ou millions) infectés et contrôlés par l'attaquant sans leur attention.



Attaques de déni de service (Denial of Service – DoS)

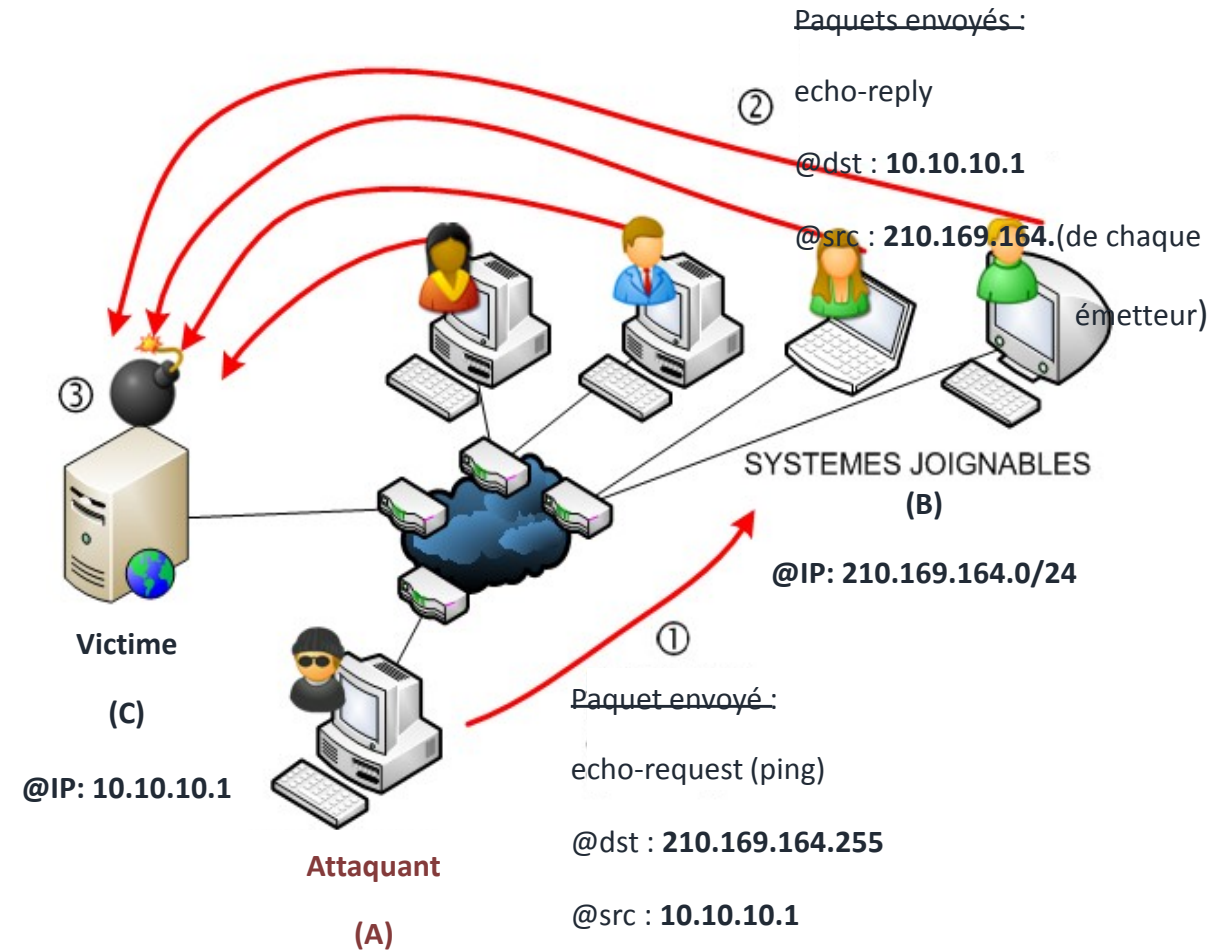
Smurfing (par réflexion)

Attaque DDoS ;

Grand nombre de paquets ICMP echo (**echo-request**) avec l'@ IP source usurpée (spoofed) de la victime sont diffusés (en broadcast) sur un réseau informatique,

⇒ Inonder la cible par réflexion des paquets ICMP reply (**echo-reply**).

Cela conduit à **une saturation de la bande passante** du réseau.



Attaques d'intrusion

Ingénierie sociale (Social engineering)

C'est l'art de la manipulation mentale (psychologique) des gens, afin qu'ils révèlent des informations confidentielles nécessaires à accéder au système (atteindre l'objectif).

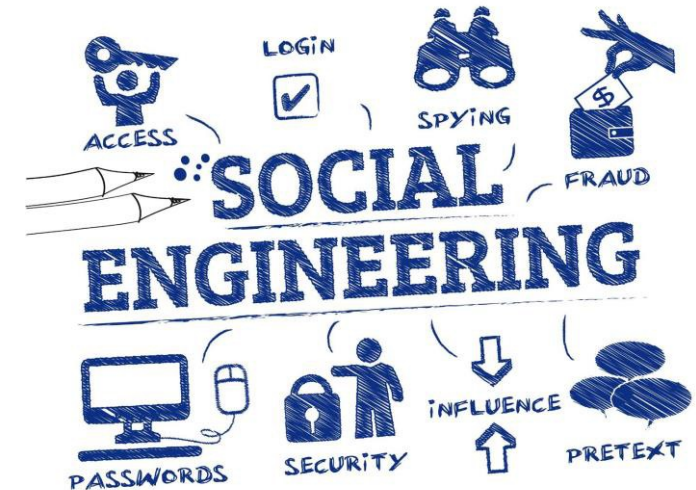
Elle exploite les faiblesses humaines (altruisme, confiance, peur, etc.).

Outils : Téléphone, internet, email, lettre, etc.

Exemple:

Hameçonnage (Phishing) à travers une page factice d'un site bancaire ou de e-commerce pour amène les internautes à révéler leurs informations personnelles (nom, mots de passe ou des informations de carte de paiement).

(3)



Attaques d'intrusion

Ingénierie sociale (Social engineering)

(Type)

(3)



Phishing



Tentative frauduleuse pour obtenir des informations sensibles

Spear Phishing



S'adresse à un groupe spécifique ou à un individu

Whaling Phishing



S'adresse aux personnes riches et éminentes

Attaques d'intrusion

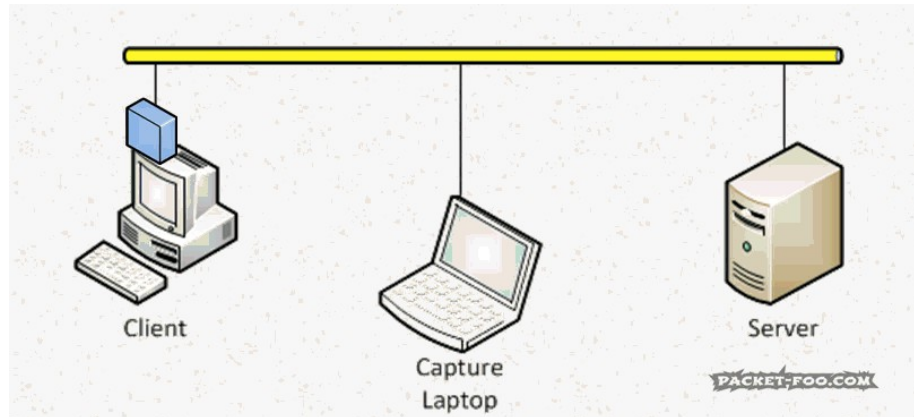
Attaques réseaux (Sniffing)

(3)



Technique permettant de récupérer toutes les informations transitant sur un réseau (sur le lien de communication) en utilisant un sniffer (Wireshark, Siphon, Dsniff, tcpdump, windump, etc.):

- ⇒ Identifier les machines communicants sur le réseau,
- ⇒ Identifier les connections entre ces machines,
- ⇒ Récupérer les mots de passe, etc.



Sniffing est l'utilisation d'une fonction standard d'**Ethernet** : le mode « **promiscuous** » (Intercepter tous les données).

Sur Windows: activer le mode **promiscuous** avec le module python « **libpcap** ».

Attaques d'intrusion

Attaques réseaux (Sniffing)

Wireshark

(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion

eth1 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
8	0.008705	192.168.1.22	212.27.63.3	TCP	74	38834 > ftp [SYN] Seq=1416128761 Win=1
9	0.036853	212.27.63.3	192.168.1.22	TCP	60	ftp > 38834 [SYN, ACK] Seq=801175440 A
10	0.036897	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128762 Ack=8
11	0.062993	212.27.63.3	192.168.1.22	FTP	140	Response: 220 Serveur de mise a jour d
12	0.063054	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128762 Ack=8
13	3.292595	192.168.1.22	212.27.63.3	FTP	74	Request: USER gildas.avoine
14	3.319677	212.27.63.3	192.168.1.22	TCP	60	ftp > 38834 [ACK] Seq=801175527 Ack=14
15	3.326153	212.27.63.3	192.168.1.22	FTP	96	Response: 331 Password required for gi
16	3.326259	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128782 Ack=8
17	5.462989	b8:26:6c:07:d5:b4	Broadcast	ARP	60	Who has 192.168.1.11? Tell 192.168.1.
18	5.511446	b8:26:6c:07:d5:b4	Broadcast	ARP	60	Who has 192.168.1.15? Tell 192.168.1.

▶ Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Offset	Hex	ASCII
0000	b8 26 6c 07 d5 b4 d4 be d9 5d b5 b5 08 00 45 10	.&l..... .]....E.
0010	00 3c 3d d0 40 00 40 06 27 ff c0 a8 01 16 d4 1b	.<=.@.@. '.....
0020	3f 03 97 b2 00 15 54 68 68 fa 2f c0 f7 e7 50 18	?.....Th h./...P.
0030	39 08 d5 0b 00 00 55 53 45 52 20 67 69 6c 64 61	9.....US ER gilda
0040	73 2e 61 76 6f 69 6e 65 0d 0a	s.avoine ..

Attaques d'intrusion

Attaques réseaux (Sniffing)

(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion

Scénario normal :

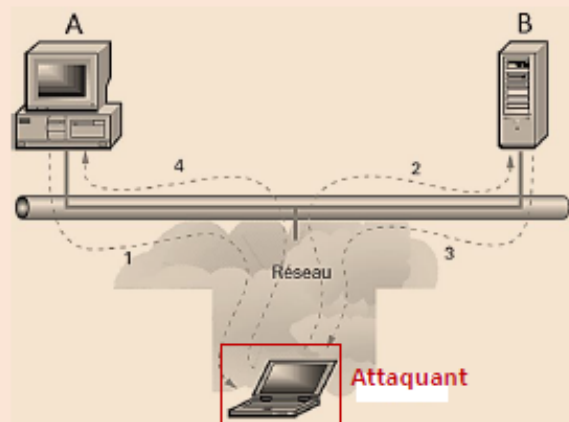
L'interface **Ethernet** n'écoute que les données qui lui sont destinées (selon @MAC& @IP).

Scénario d'attaque :

Le mode **promiscuous** est activé : l'interface Ethernet s'intéresse à toutes les données en transit sur le lien.

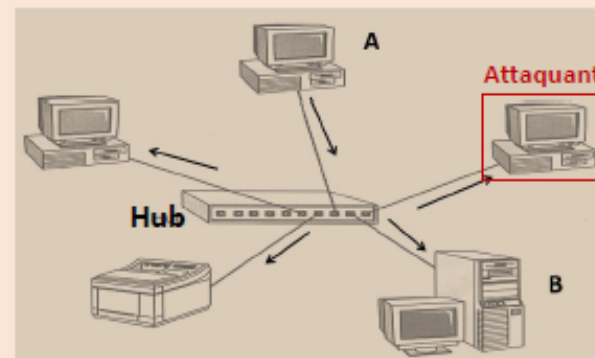
Topologie en bus

Les données sont déposées sur le bus
=> Voit l'intégralité des données.

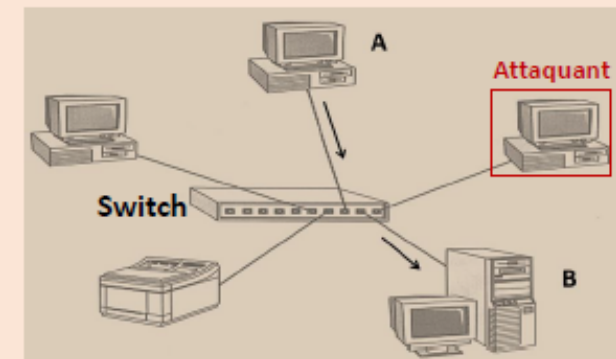


Topologie en étoile

Quel que soit le port de la machine
écoutant le réseau,
=> Voit l'intégralité des données.



les données se transigent entre A et B
seulement,
=> Ne voit pas les données.



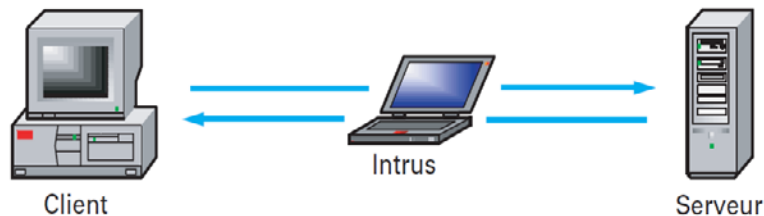
Attaques d'intrusion

Attaques réseaux (Man In The Middle – l'homme au milieu)

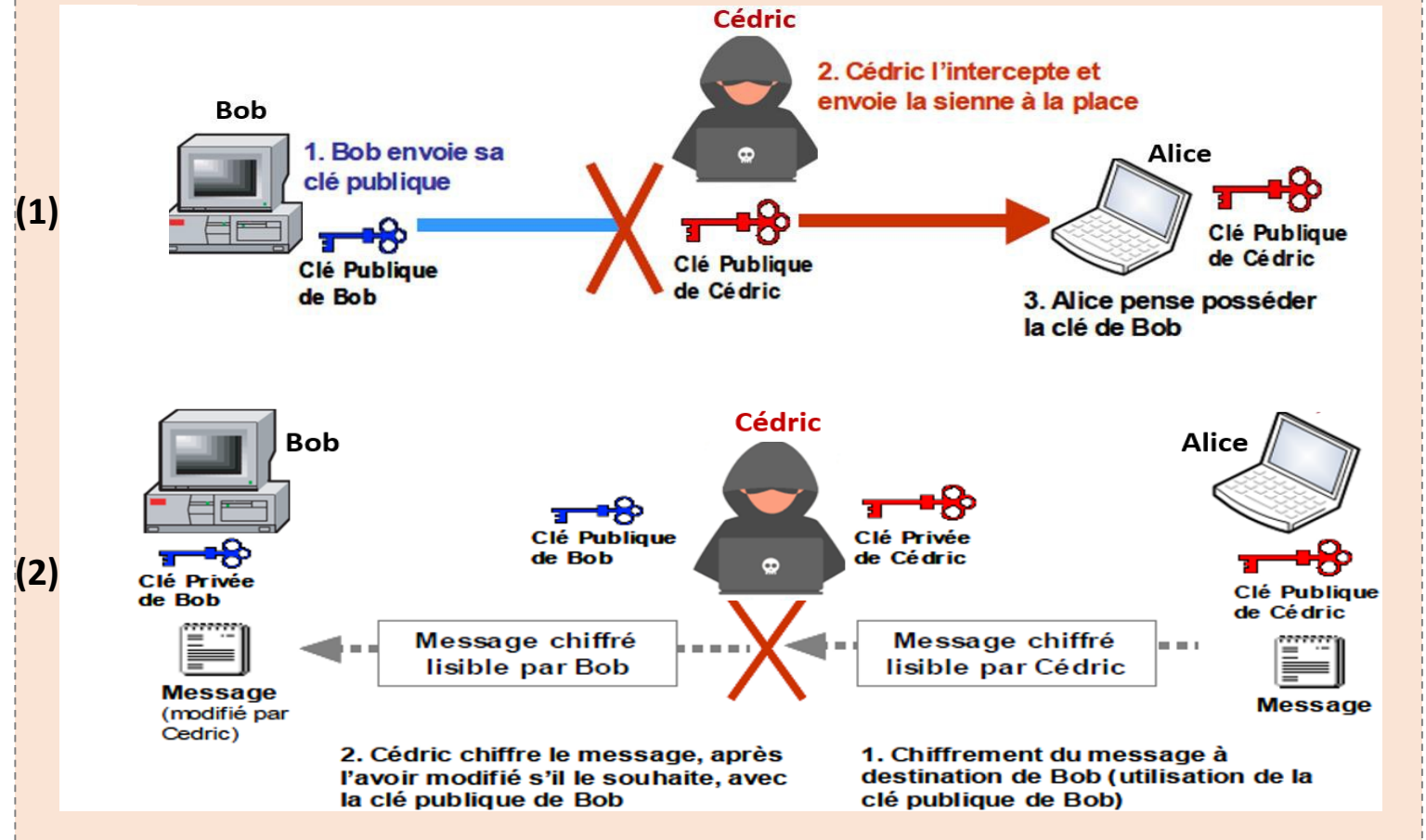
Une attaque où une tierce personne s'interpose de manière transparente (sans se faire remarquer) dans une connexion,

⇒ Ecoute passive

⇒ Ecoute active.

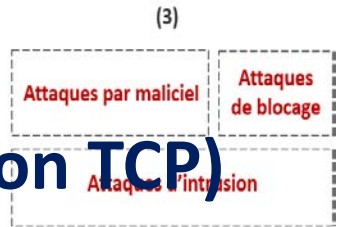


Scénario d'une attaque :



Attaques d'intrusion

Attaques réseaux (TCP Session Hijacking – Détournement de session TCP)

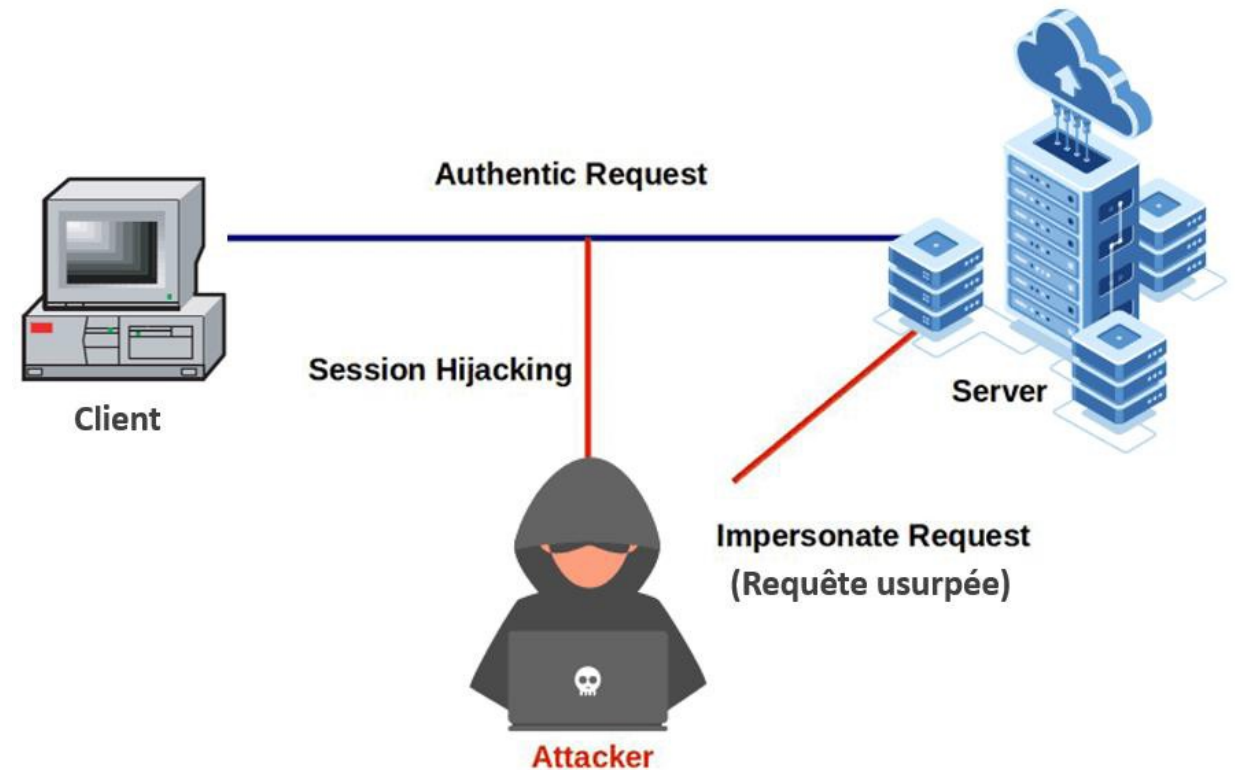


Consiste à **intercepter** une session TCP **initée** entre deux machines (client et serveur) puis la **détourner**,

- ⇒ **Prendre possession** de la connexion (sans authentification),
- ⇒ **Continue** la session (qui avait été ouverte par le client).

Le contrôle d'authentification des protocoles application (telnet, FTP, HTTP, etc.) s'effectue à l'ouverture de la session,

- ⇒ Au lieu de voler un mot de passe (telnet), le pirate attend qu'un utilisateur s'authentifie puis voler sa session.



Attaques d'intrusion

Attaques réseaux (IP spoofing – Usurpation d'IP)

Consiste à remplacer l'@IP de l'expéditeur d'un paquet IP (attaquant) par l'@IP d'une autre machine de confiance (trusted host).

- ⇒ Passer sur le réseau sans être détecté par le système de filtrage de paquets (pare-feu).
- ⇒ Réaliser à la cible ce que la machine de confiance peut réaliser.

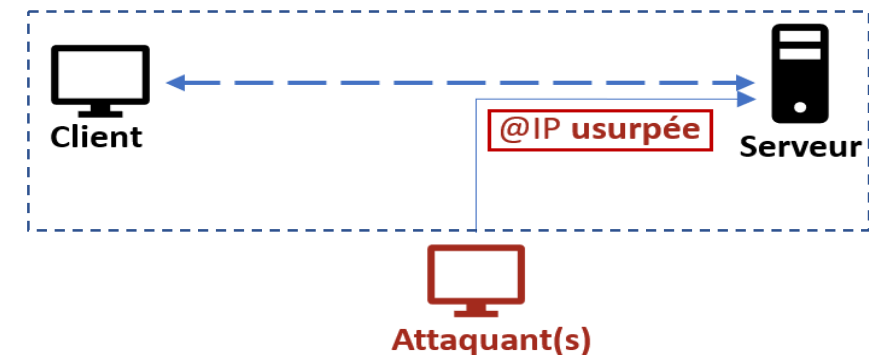
L'IP spoofing est utilisée lorsque deux hôtes sont en relation de confiance grâce à leurs @ IP, c'est-à-dire que l'authentification au niveau du serveur consiste en une vérification de l'adresse IP du client (services tels que **rlogin**, **ssh**, ...).

Exemple: **hping2**

(3)



Version	Header Length	Type of service	Total Packet Length (in Bytes)			
Identification			x	D	M	Fragment Offset
Time to Live (TTL)		Protocol	Header Checksum			
Source Address						
Destination Address						
Options (if any)						
Payload						



Attaques d'intrusion

Attaques réseaux (IP spoofing – Usurpation d'IP)

(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion

Exemple d'attaque :

```
#hping3 -S <target IP> -a <spoofed IP> -c 3
```

s: SYN a: adresse IP usurpée c: nombre de requêtes SYN

```
(root@kali)-[~]
# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.44.2   0.0.0.0         UG    100    0      0 eth0
192.168.44.0     0.0.0.0        255.255.255.0   U     100    0      0 eth0
```

```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.44.128 netmask 255.255.255.0 broadcast 192.168.44.255
```

```
(root@kali)-[~]
# hping3 -S 192.168.44.2 -a 192.168.44.100 -c 3

HPING 192.168.44.2 (eth0 192.168.44.2): S set, 40 headers + 0 data bytes

— 192.168.44.2 hping statistic —
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

hping3 : outil réseau capable d'envoyer des paquets TCP/IP sur commande.



Attaques d'intrusion

Attaques réseaux (ARP spoofing/poisoning – Empoisonnement ARP)

(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion

Le protocole **ARP** (Address Resolution Protocol) a pour rôle de faire la correspondance entre une @IP et une @ physique (**MAC**).

Si un attaquant envoie un message de réponse ARP (*ARP reply*) avec son **@MAC** correspondant à l'@IP du récepteur, tout le flux IP dirigé vers le récepteur sera redirigé vers l'attaquant. On dit qu'il a **empoisonné le cache ARP** du récepteur.

Attaque a pour but de **corrompre** la **table ARP** (Address Resolution Protocol) d'un **commutateur** à travers deux méthodes :

- l'envoi de fausses réponses à des requêtes ARP (ARP request),
- l'envoi de paquets avec @IP usurpée / réponses ARP gratuites avec @IP usurpée.

👉 Exemple: **ARPspooof**

Attaques d'intrusion

Attaques réseaux (ARP spoofing/poisoning – Empoisonnement ARP)

(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion

Fonctionnement (protocole ARP) :

(A) Veut envoyer des données à (B) :

(1) Si la **table ARP** de (A) ne contient pas **@MAC(B)**, envoie **requête ARP** (ARP request) en **broadcast**.

(2) **Commutateur** ajoute l'**@MAC(A)** dans sa **table ARP**,
Si la **table ARP** du **commutateur** ne contient pas **@MAC(B)**, envoie **requête ARP** (ARP request) aux autres ports.

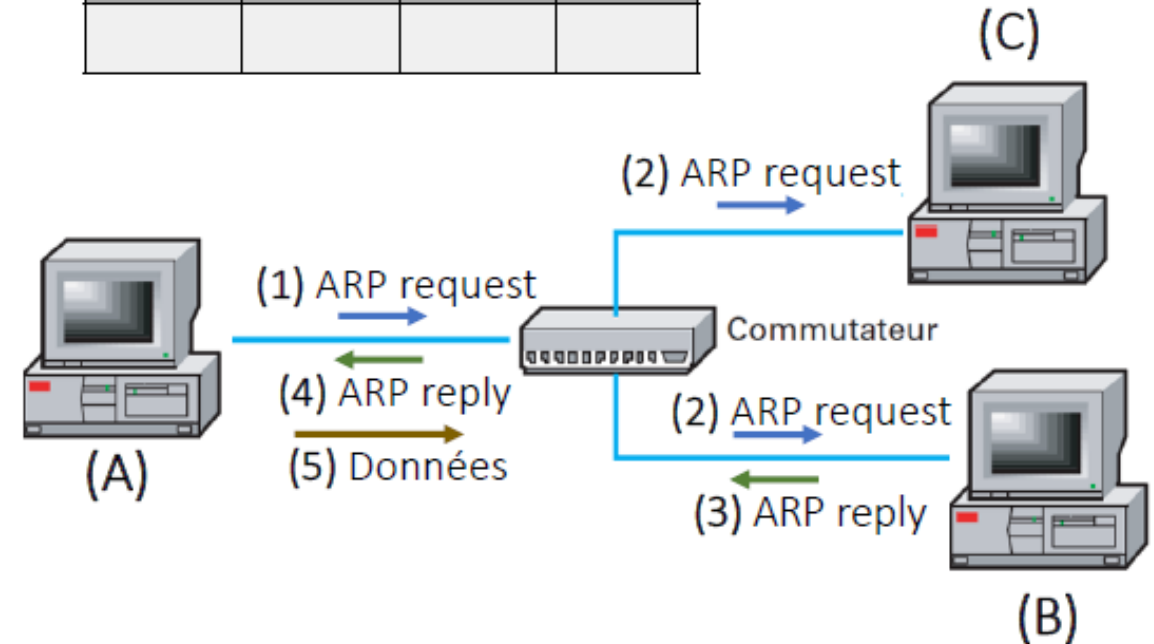
(3) (B) ajoute l'**@MAC(A)** dans sa **table ARP**, (B) envoie **réponse ARP** (ARP reply),

(4) **Commutateur** ajoute l'**@MAC(B)** dans sa **table ARP**, renvoie la **réponse ARP** (ARP reply) à (A).

(5) (A) envoie les données à (B).

Table ARP (switch)

@IP	@MAC	N°port	...



Attaques d'intrusion

Attaques réseaux (ARP spoofing/poisoning – Empoisonnement ARP)

(3)

Attaques par maliciel

Attaques de blocage

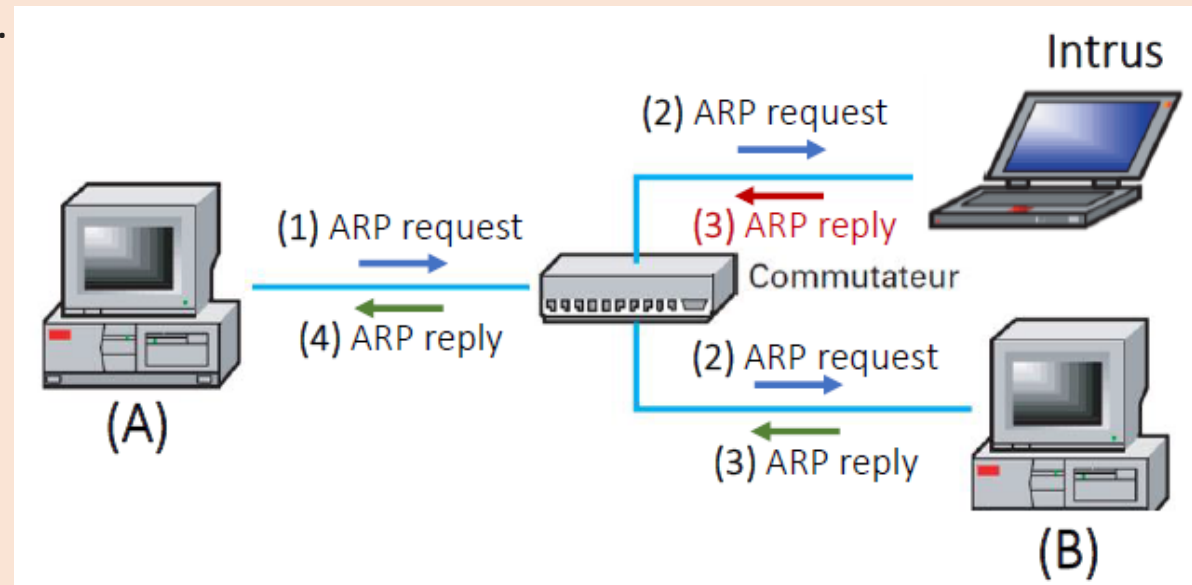
Attaques d'intrusion

1. Envoi de fausses réponses ARP aux requêtes ARP :

⇒ Recevoir des paquets destinés à une autre machine.

(3) L'intrus réponds par **ARP reply** contenant son **@MAC** (disant qu'il le propriétaire de **@IP dest**),

(4) Selon le modèle du **commutateur**, il peut ajouter l'**@MAC(Intrus)** et l'**@MAC(B)** dans sa **table ARP** puis renvoie la **réponse ARP** (ARP reply) à (A) **OU** ignorer la réponse du port suspect.



Attaques d'intrusion

Attaques réseaux (ARP spoofing/poisoning – Empoisonnement ARP)

(3)

Attaques par maliciel

Attaques de blocage

Attaques d'intrusion

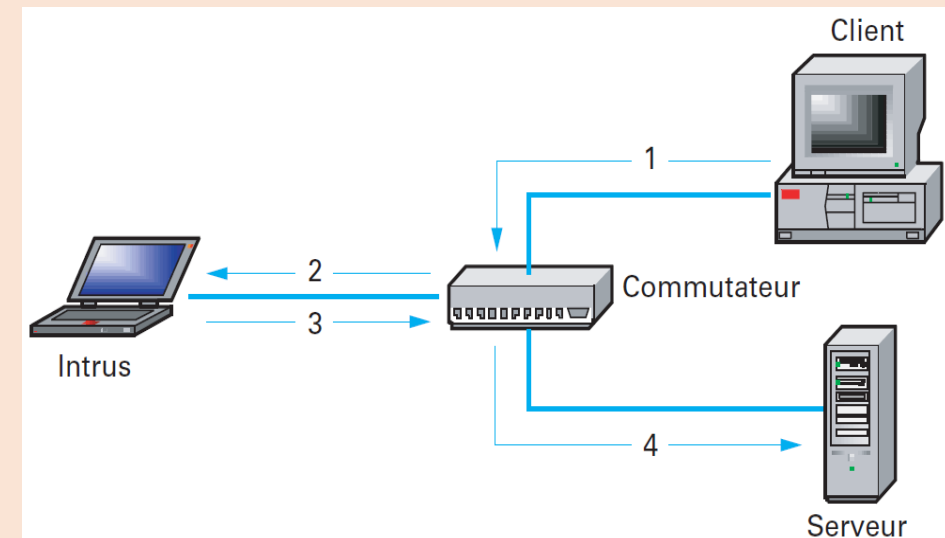
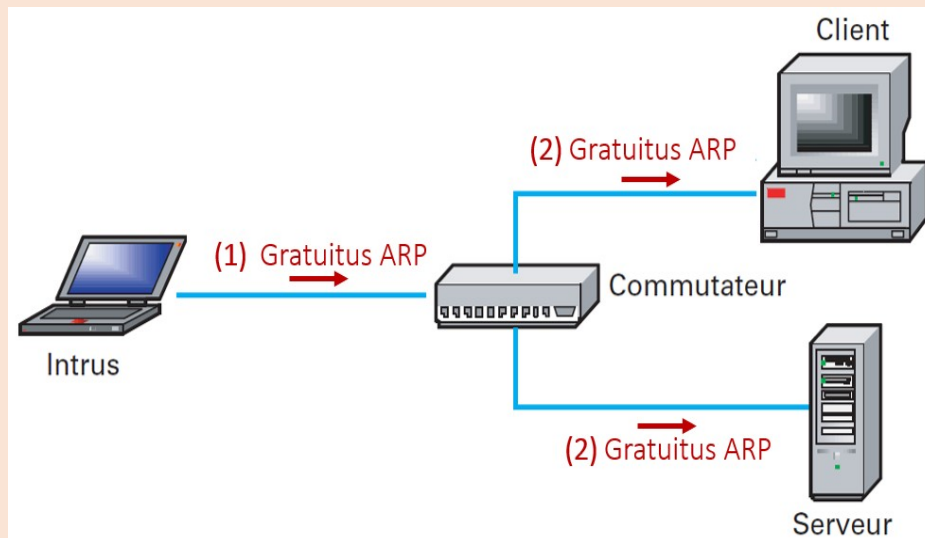
2. Envoi de paquets ARP gratuits (de mise à jour) avec @IP usurpée :

⇒ Pour que le trafic passe par l'attaquant.

(1) L'intrus broadcast un paquet **ARP** gratuite contenant son **@MAC** et **@IP(serveur/passerelle)**,

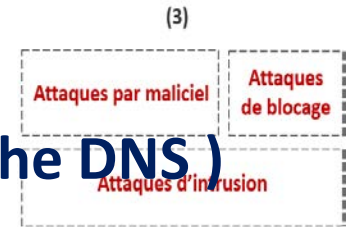
(2) **Commutateur** met à jour sa **table ARP** en associant l'**@MAC(Intrus)** avec **@IP(serveur/passerelle)**. Par la suite, les autres machines mettent à jour leurs **table ARP**.

⇒ Le trafic du **client** doit passer par l'**intrus** avant d'atteindre le **serveur**.



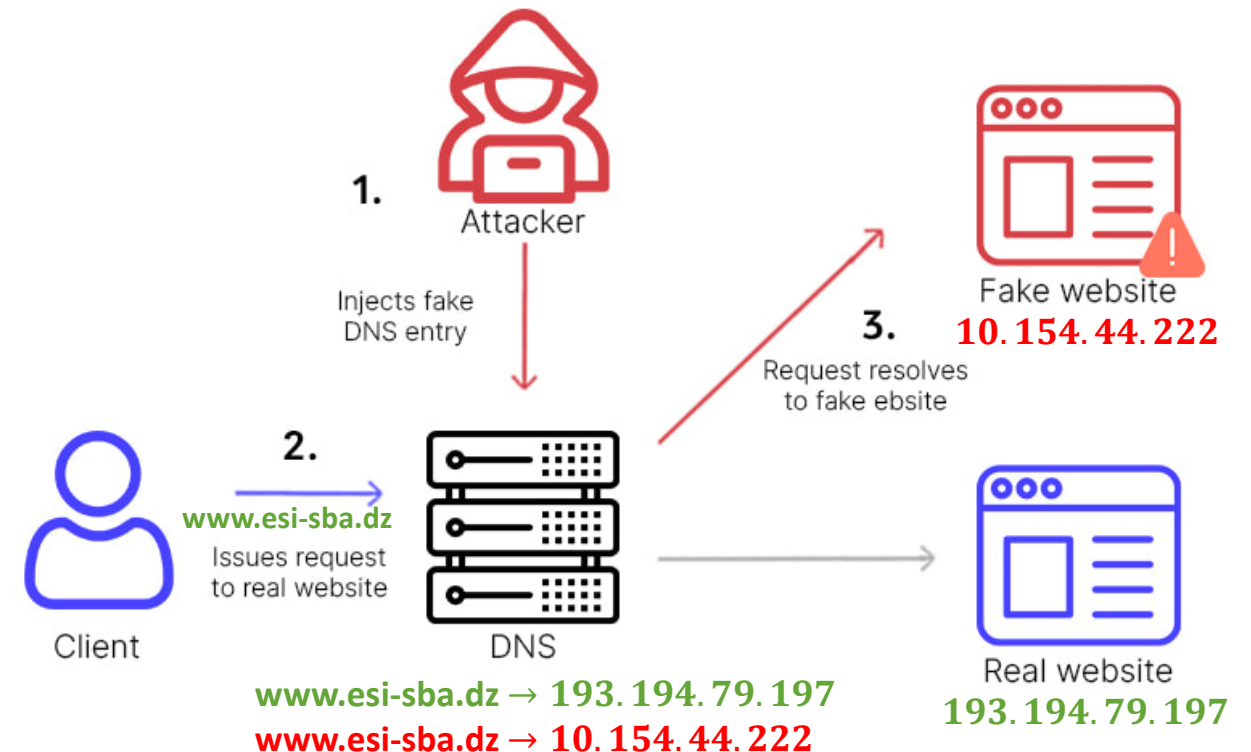
Attaques d'intrusion

Attaques réseaux (DNS Spoofing/Usurpation DNS – Empoisonnement du cache DNS)



Le protocole **DNS** (Domain Name System) a pour rôle de **convertir** un **nom de domaine** (par exemple www.esi-sba.dz) en son **@IP** (par exemple 193.194.79.197) et réciproquement. Cette attaque consiste à faire parvenir de **fausses réponses** aux **requêtes DNS** émises par un **client DNS** (victime) au **serveur DNS**:

⇒ Renvoyer une **@IP incorrecte**, détournant le trafic vers une autre machine (souvent celui d'un attaquant).



Attaques d'intrusion

Attaques applicatives (SQL Injection)

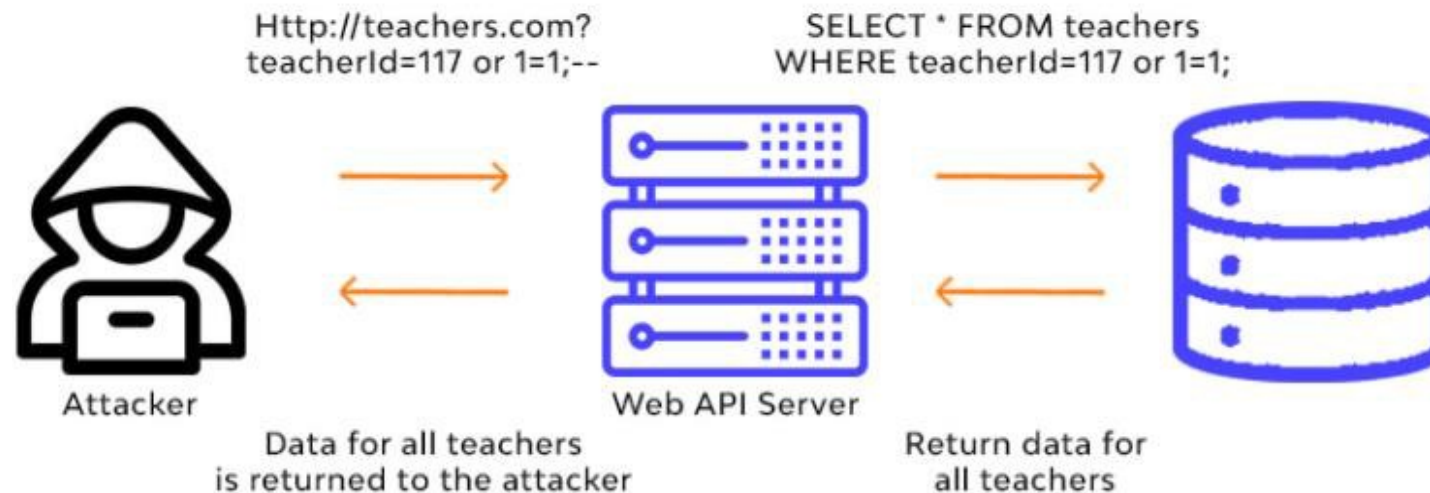
(3)



Permet à un **intrus** d'**interagir directement** avec la **BDD** d'un site web (où l'accès à la base est **interdite**),

Consiste à **détourner** la **requête SQL** et -en fonction du contexte- **créer** sa propre **requête SQL malveillante** :

- ⇒ **Contourner** le mécanisme d'authentification,
- ⇒ Accéder/modifier **frauduleusement** les données confidentielles de la base (mots de passe, n°tel, etc.).



Attaques d'intrusion

Attaques applicatives (SQL Injection)

(3)

Attaques par maliciel

Attaques
de blocage

Attaques d'intrusion

Formulaire WEB :

Entrez votre identifiant et mot de passe puis cliquez sur Connexion

Identifiant

Mot de passe

Connexion

Scénario normal :

Identifiant : Ahmed

Mot de passe : 12dg4

Exemple de requête légitime :

```
Select count(*) from user  
where user= 'Ahmed' and  
pw='12dg4';
```

↓
\$user contient le login renseigné dans le formulaire par l'utilisateur.

\$pw contient le mot de passe.

↓
Une requête SQL permettant de vérifier le login et le password:

```
Select count(*) from user  
where user='$user' and pw='$pw';
```

Scénario d'attaque :

Identifiant : azerty

Mot de passe : abcd' or 1=1;/*

La requête SQL sera :

```
Select count(*) from user  
where user= 'azerty' and  
pw='abcd' or 1=1;/*;
```

Cette condition est toujours vraie !

⇒ La requête est donc toujours **valide**, quel que soit le mot de passe renseigné par l'attaquant !