Chapitre 2

Attaques et intrusions informatiques

Pr. HADRI

Chapitre 2: Attaques et intrusion réseau

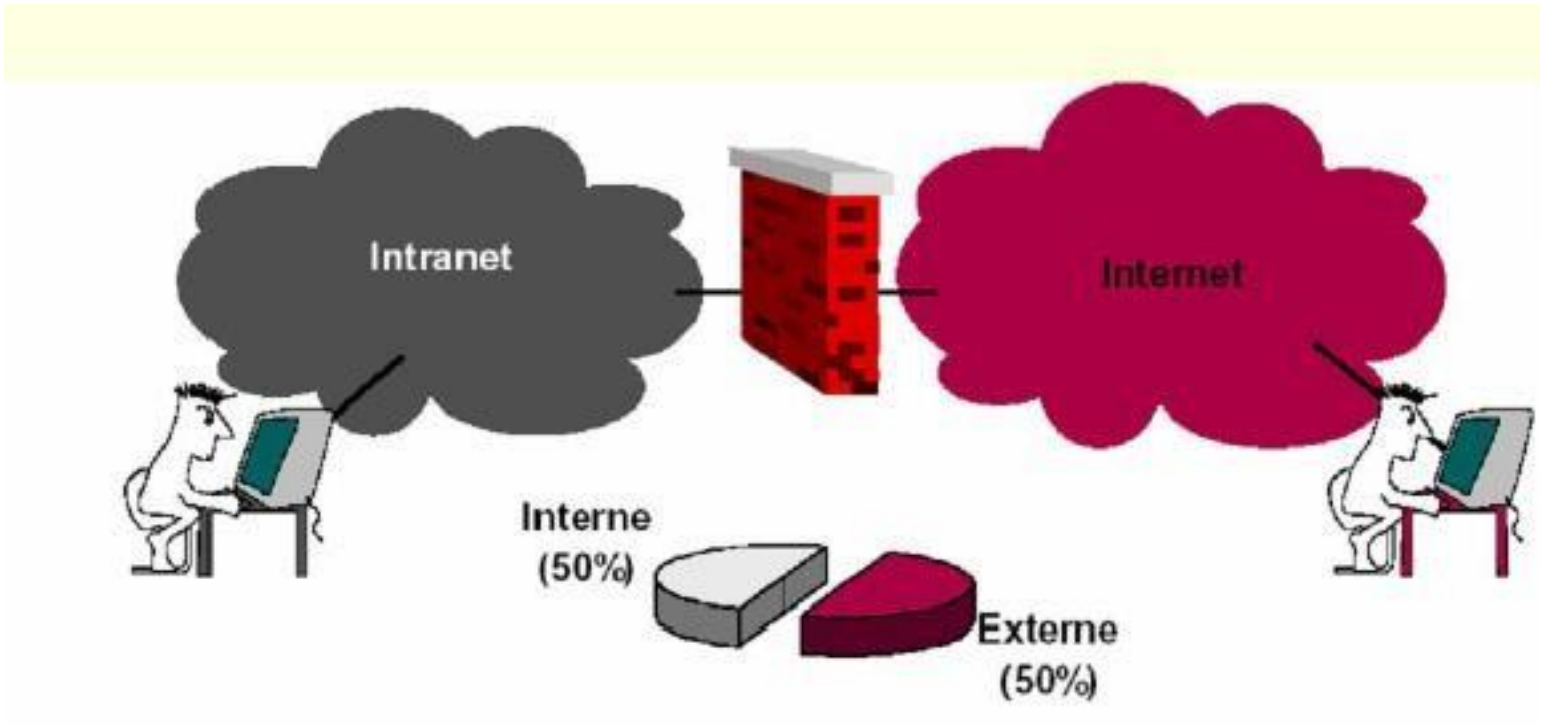
Objectifs

- Comprendre le concept de l'attaque;
- Comprendre les types de hackers;
- Comprendre le processus d'une attaque;
- Appréhender les types d'intrusion;
- Appréhender les types d'attaque et les piliers de sécurité correspondants;
- Démystifier les différentes méthodes, outils de chaque phase de l'intrusion;
- Se mettre dans la peau d'un attaquant (une personne malveillante) pour le combattre;
- Apprendre à devenir un hacker étique.

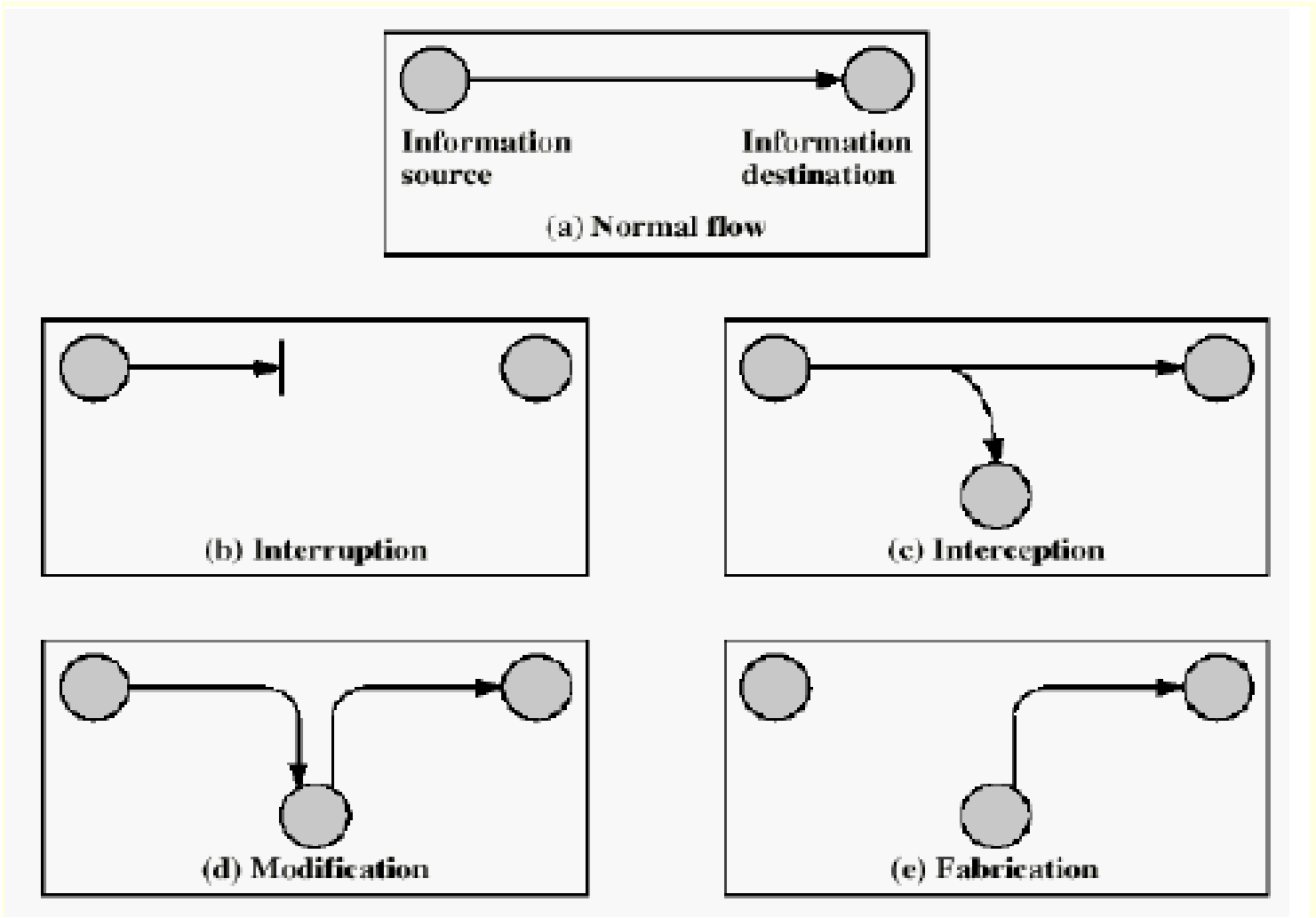
Qu’est ce qu’ une attaque?

- Une «**attaque**» est l'exploitation d'une faille d'un système d’information (système d'exploitation, logiciel ou bien même de l'utilisateur), à des fins non connues par l'exploitant du système et généralement **préjudiciables**.
- Les attaques sont plus souvent basées sur les failles et les vulnérabilités dans les systèmes.
- Afin de contrer ces attaques il est indispensable de connaître la méthodologie d’une attaque, ainsi que les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Origines d'attaques

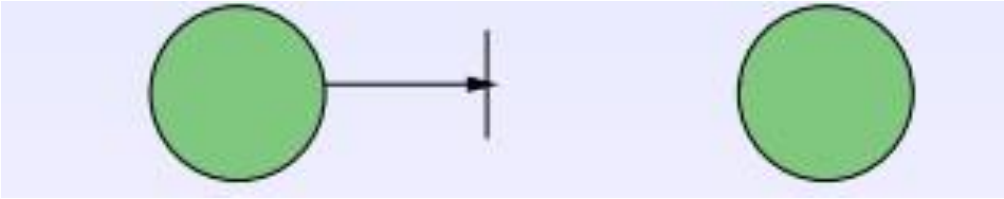


Les types d'attaques

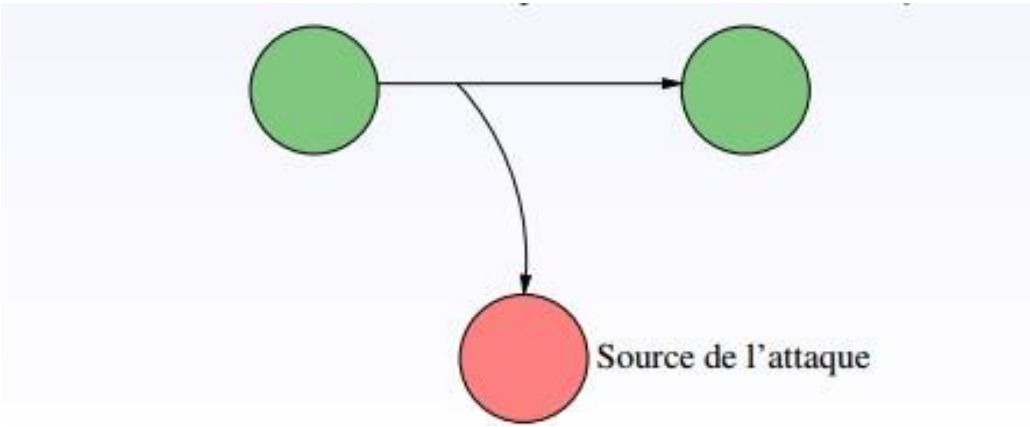


Les types d'attaques / critères de sécurité

Interruption. vise la **disponibilité** des informations (DoS, . . .)

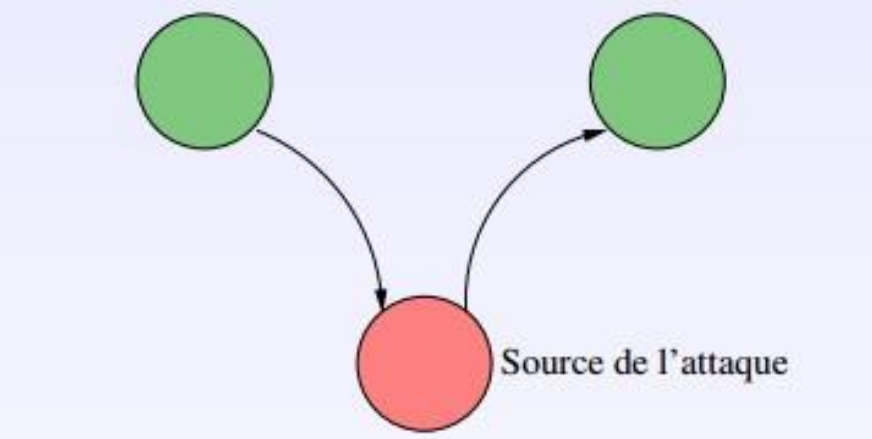


Interception. vise la **confidentialité** des informations (capture de contenu, analyse de traffic, . . .)

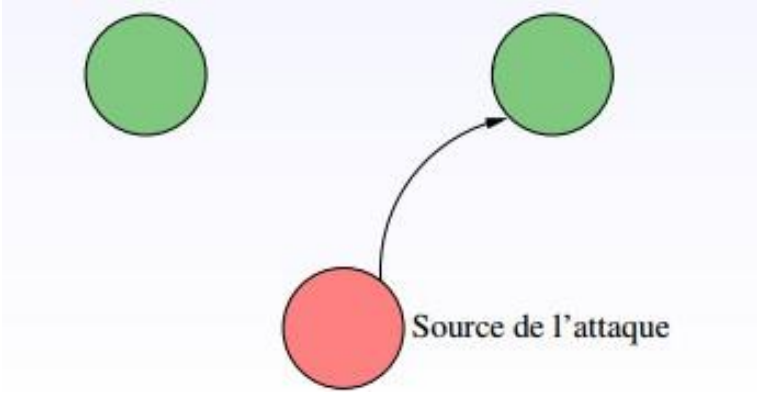


Les types d'attaques / critères de sécurité

Modification. vise **l'intégrité** des informations (modification, rejeu, . . .)



Fabrication. vise **Non répudiation**des informations (mascarade, . . .)



Hacker

- L'origine: Verbe **to hack;**
- Découper quelques chose à l'aide d'un outil;
- Découper des informations en blocs logique et les réassembler;
- Modifier le fonctionnement de quelques choses pour l'améliorer;
- **Sécurité informatique**: détourner la protection d'un système;
- Deux cas de figures: Malveillant ou bienveillant (éthique).

Hacker

- Utiliser une tasse pour maximiser l'espace utilisé dans le micro onde➔ chauffer deux bols de céréales;
- Economiser le temps et l'énergie;
- Bricoleurs;
- Bidouilleurs;
- Connaitre le fonctionnement des outils utilisés (réseaux, systèmes, programmes..)

Hacker

- Une personne passionnée par la compréhension d'un système informatique;
- Bricoler celui-ci;
- Détourner;
- Construire quelques chose de meilleur et d'utiles pour les autres personnes

Types de Hackers

Hackers principaux

- Chapeaux blanc;
- Chapeaux noirs;
- Chapeaux gris.

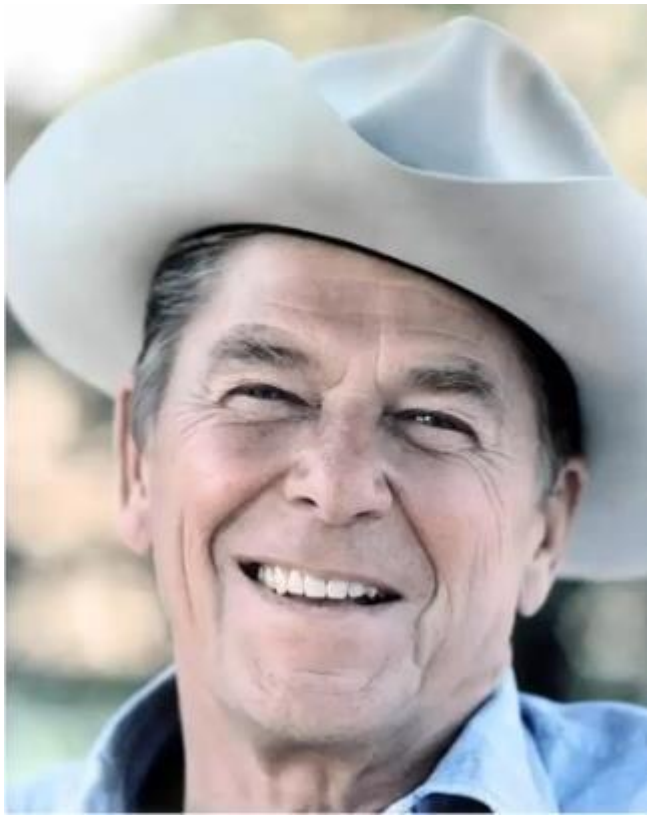
Hackers Secondaires

- Anonymous;
- Scripts kiddies;
- Phreakers

Les universitaires

Types de Hackers

Le hacker éthique (chapeau blanc)



- Hacker éthique, agit toujours en restant conforme à la loi.
- Apprendre la sécurité informatique pour se protéger, et protéger d'autres personnes;

L'objectif de ce cours c'est devenir un hacker éthique.

Types de Hackers

Le hacker malveillant(chapeau noir): pirate

- Hacker Spécialiste dans la maitrise de la sécurité informatique et des moyens de déjouer cette sécurité;
- Hacker agissant avec une intention de nuire ou pour un intérêt personnel;
- Il a les même compétences qu'un hacher étique, ce sont les intensions qui différent.

Types de Hackers

Le hacker au chapeau gris

- Entre le white hat et le black hat, il agit sans mauvaise intention ni pour des intérêts personnels mais peut occasionnellement dépasser les limites;
- Ces intensions sont plus mitigées;
- Se prend pour un justicier;
- Intrusion noble➔ sécuriser les systèmes➔ illégale.
- L'autorisation qui le différencie d'un hacker au chapeau blanc.

Types de Hackers

Hackers secondaires

(1) Anonymos

- Sous type du hacker chapeau gris;
- **Hacktivist**: hack + activist;
- But politique;
- Exemple: Mettre hors service un site web pour manifester contre quelques choses;

Types de Hackers

Hackers secondaires

(2). Scripts kiddies

- **Skript kiddy**: « gamins qui utilisent les scripts »;
- Télécharger un programme tout fait, avec le mode d'emploi;
- Utiliser ces programmes sans gênes sur les autres personnes, sans connaissance de causes, des enjeux et des dangers qui peuvent provoquer.
- Ce type est rejeté de la communié des hackers étique.

Types de Hackers

Hackers secondaires

(3). Phreakers

- **Phreakers**: **phone** et **phreak**
- Populaires en 1960, 1970;
- Personnes qui piratent les lignes téléphoniques:
  - Pour téléphoner gratuit;
  - Accéder à des fonctionnalités interdites;

Types de Hackers

Les universitaires (1/2)

- Ce sont des hackers libres;
- Mouvement Open Source du logiciel libre, comme Richard Matthew Stallman, le fondateur du projet GNU.
- Ce type est défini comme quelqu'un qui partage sa connaissance avec autrui, sur le fonctionnement d'un système, des ordinateurs et des réseaux;
- l'information est libre et n'appartient à personne. Ainsi, toute nouvelle connaissance se veut d'être partagée avec tout le monde;

Types de Hackers

Les universitaires (2/2)

- En 1984 , Steven Levy a défini cette catégorie selon les principes suivants :
  - Toute information est par nature libre et gratuite.
  - L'accès aux ordinateurs devrait être total, illimité, possible pour tout le monde.
  - La décentralisation des données doit être encouragée.
  - Les hackers devraient être jugés sur le hacking, non pas sur des hiérarchies sociales telles que le diplôme, l'âge ou le grade.
  - On peut créer de l'art et de la beauté avec un ordinateur.
  - Les ordinateurs peuvent améliorer la vie.

L’anatomie d’une intrusion (attaque)

Pourquoi faire un test d’intrusion?

- Tester les identifiants;
- Tester un nouveau service;
- Tester le personnel;
- Sécuriser son système;
- Vérifier la conformité à une norme;

Intrusion

Attaque = cible + méthode + Vulnérabilités

“Pour battre un pirate, il faut réfléchir comme un pirate”

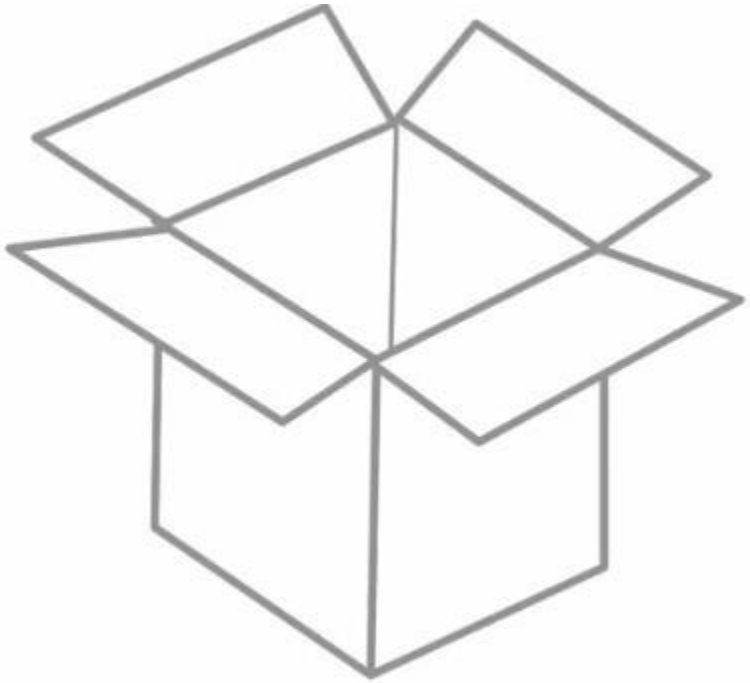
Types d’intrusions

Boite noire

- Tester un système sans son fonctionnement interne, son code source;
- Le hacker étique se passe pour un pirate;
- N’aura aucune information spécifique;
- Va essayer d’entrer dans le système.

Types d’intrusions

Boite Blanche



- Accès à tous les codes sources;
- Accès au systèmes;
- Avoir toutes les informations nécessaires;
- Accès à tous les détails.

Types d’intrusions

Boite Grise

- Accès à quelques éléments;
- Avoir quelques informations;
  - Topologie réseau;
  - Plan d’adressage.
  - Etc..

L’anatomie d’une attaque

Cible = motivation

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- glâner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond » pour une attaque ;

Le processus général d'une attaque

Une attaque est souvent décrite à l'aide des 5 « P » :

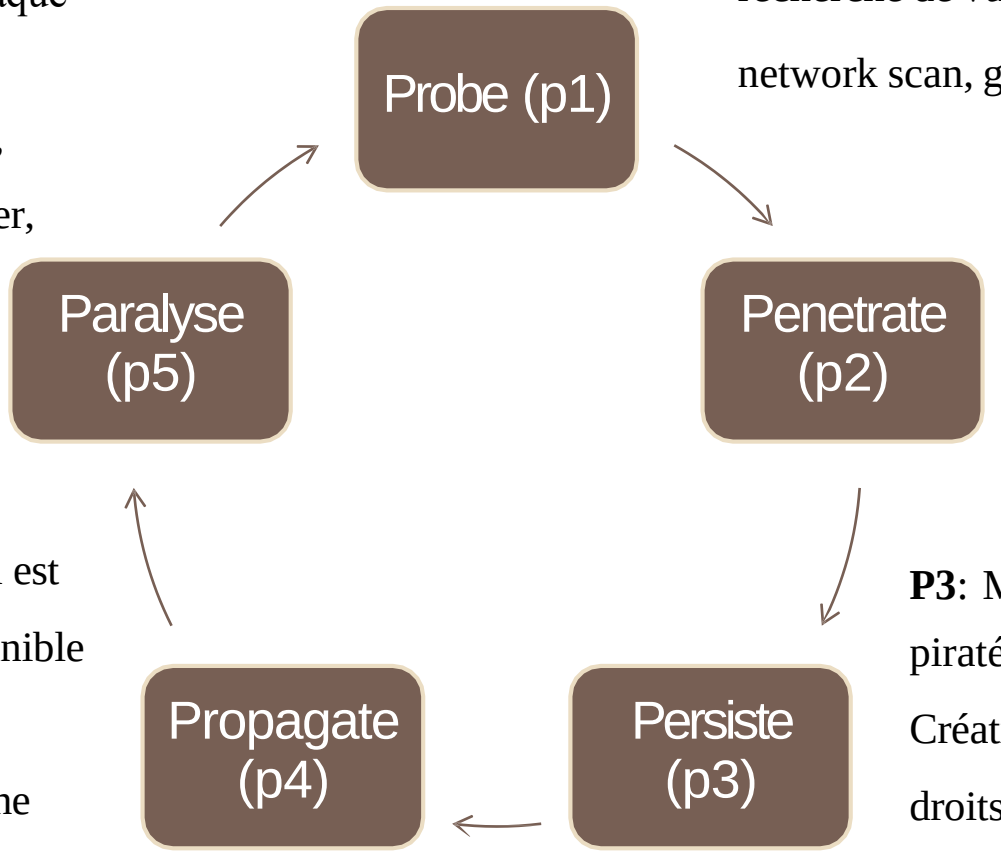
P1: la collecte d'informations et la recherche de vulnérabilités (footprinting, network scan, google hack….)

P2: exploitation des informations receuillies et des failles➔ s'introduire;

P3: Maintenir l'accès au système piraté (backdoor, rootkits). Création d'un compte avec les droits admin ou installer une appli de controle à distance.

P4: Observer ce qui est accessible et disponnible sur le réseau local. Rester anonyme et ne pas laisser de traces.

P5: creation de l'attaque ➔ debouche sur l'intrusion (Détruire, endomager, espionner, voler).



Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

- Apprendre le maximum d'information sur la cible;
- Prise de temps (quelques mois), c'est l'étape la plus longue.
- Les autres étapes se base sur la reconnaissance;
- On utilise le terme foot printing (chercher les technologies qui sont mise en place; quel serveur web,….)

Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

- Récupérer des informations de plus en plus précise sur la cible;
- Cascade d'informations: on trouve une information, on l'utilise pour trouver une autre (trouver les infos les unes après les autres);
- Reconnaissance active: se rendre sur place
- passive: Chercher sur internet (infos publiques)

Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

- Internet (les enregistrements whois, communiqués de presse;
- Whois: nom, prénom;, adresse du contact ou propriétaire du site;
- Hors ligne: catalogues, documents internes;
- Hors ligne; plus directe

Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Hors ligne; plus directe**
- ***Dumpster diving***: fouiller les poubelles de la cible;
- ***Shoulder surfing***: observer au dessus des epôles;
- ***Eavesdropping*:** Ecouter des conversions privées, se placer à coté d'une personne

Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

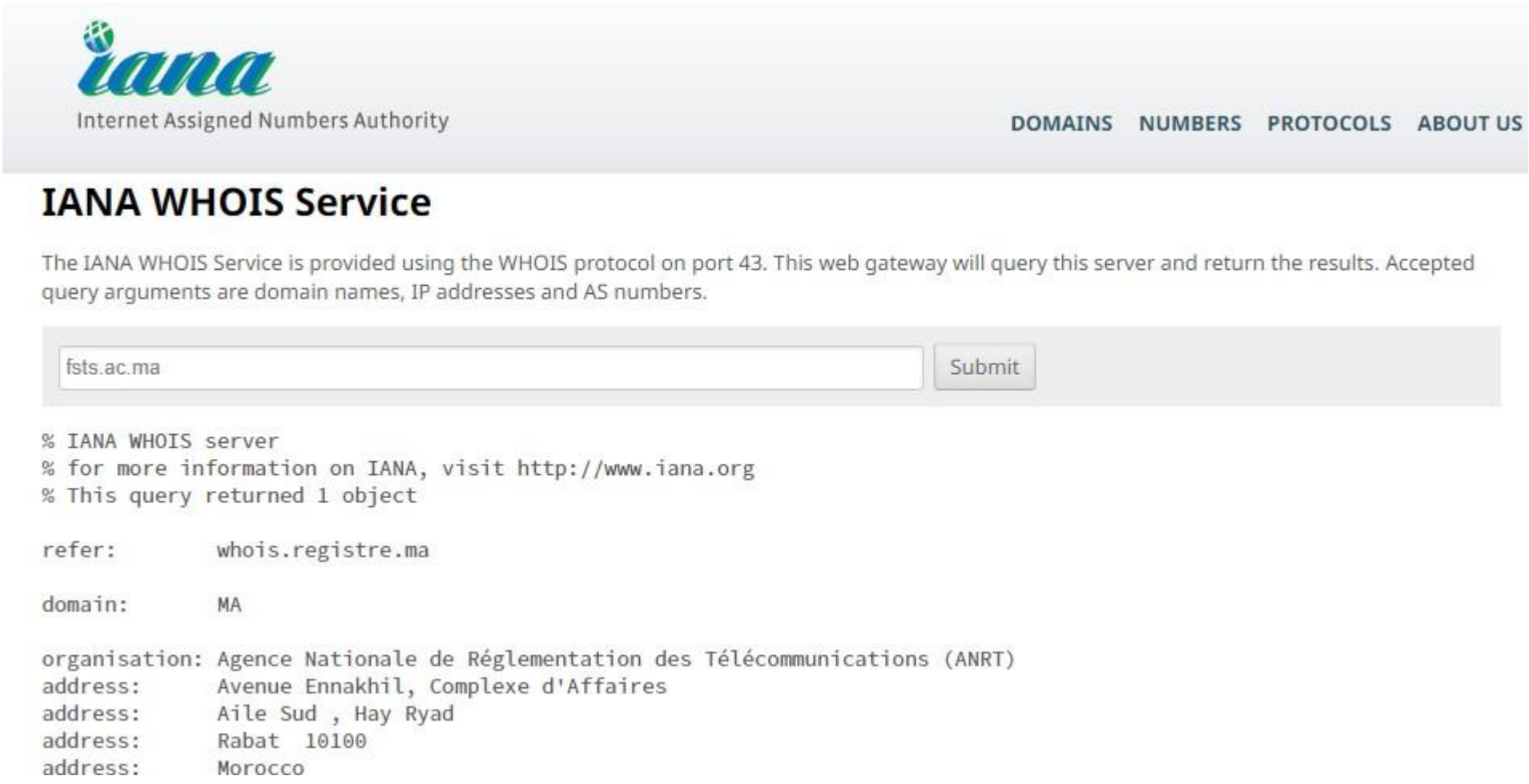
- **Whois;**
- Service permettant de récupérer des informations sur le propriétaire; Accès publique;

(P1) Probe: Collecte d'informations, phase de reconnaissance

- Les bases de données **WHOIS** sont des outils qui permettent d'interroger les informations d'une organization quant ils ont enregistré leur domaine.
- Toutes les informations disponnible sur le site IANA sont recherchées par le nom de domaine.
- L'information comprend, **l'admin du domaine**, les informations de **contact technique**…

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Exemple pour le domaine : .ma**



(P1) Probe: Collecte d'informations, phase de reconnaissance

```
contact:      administrative
name:         General Director
organisation: Agence Nationale de Réglementation des Télécommunications (ANRT)
address:      Avenue Ennakhil, Complexe d'Affaires
address:      Aile Sud , Hay Ryad
address:      Rabat  10100
address:      Morocco
phone:        +212 537 71 84 00
fax-no:       +212 537 71 64 89
e-mail:       ma@anrt.ma

contact:      technical
name:         General Director
organisation: Agence Nationale de Réglementation des Télécommunications (ANRT)
address:      Avenue Ennakhil, Complexe d'Affaires
address:      Aile Sud , Hay Ryad
address:      Rabat  10100
address:      Morocco
phone:        +212 537 71 84 00
fax-no:       +212 537 71 64 89
e-mail:       ma@anrt.ma
```

(P1) Probe: Collecte d'informations, phase de reconnaissance

```
nserver:      DNS.INRIA.FR 193.51.208.13
nserver:      NS1.REGISTRE.MA 2001:4288:1800:186:0:0:0:3 81.192.171.131 81.192.171.83
nserver:      NS2.NIC.FR 192.93.0.4 2001:660:3005:1:0:0:1:2
nserver:      NS2.REGISTRE.MA 2001:4288:1800:186:0:0:0:4 81.192.171.132 81.192.171.84
nserver:      NS3.REGISTRE.MA 2001:4288:1800:386:0:0:0:3 81.192.171.115 81.192.171.139
nserver:      NS4.REGISTRE.MA 2001:4288:1800:386:0:0:0:4 81.192.171.116 81.192.171.140
nserver:      SNS-PB.ISC.ORG 192.5.4.1 2001:500:2e:0:0:0:0:1
ds-rdata:     15319 8 2 69C0229C3B381976C0BA84B65A63C01AA7EE4F2A807354FC9C028E5C59526C86

whois:        whois.registre.ma

status:       ACTIVE
remarks:      Registration information: http://www.registre.ma

created:      1993-11-26
changed:      2018-01-20
source:       IANA
```

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Whois: exemple de site**
- **https://whois.domaintools.com/**
- **https://www.africaregistry.com/services/whoisSearchPage**
- **https://www.easywhois.com/**
- **http://whois.ma/ressources/whois**

(P1) Probe: Collecte d'informations, phase de reconnaissance

Enumération:

- Bannières systems (version des serveurs WEB, MAIL…).
- Utilisation de TELNET: **Telnet server port**

- Ex: telnet www.fsts.ac.ma 80

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Google hacking:**

  - Google offer à l'attaquant la possibilité de collecter des informations sensibles qui ne devraient pas etre disponnible à l'exterieur.
  - En utilisant des opérateurs avancés comme le montre le tableau suivant en combinaison avec des termes clès, on peut utiliser Google pour découvrir de nombreuses informations sensibles qui ne doivent pas etre révélées.

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Google hack :**

Opérateur	Description	Valaur à saisir
Filetype	Recherche des fichiers ayant une extention determinée	Une suite de caractère (doc, pdf, xls…)
Inurl	Recherche un mot dans l'URL de la page	Un mot ou une erpression entre "guillemets"
Link	Recherche des liens pointant	Une URL
InTitle	Recherche un mot dans le titre de la page	Un mot ou une expression

Ou: **https://www.google.fr/advanced_search**

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Alternative à google: Shodan (google des hackers)**

- **Shodan**: un moteur de recherche qui permet de chercher des routeurs, serveurs, cameras IP, imprimantes, Iphones et des appareils ayant une IP visible sur le net.
- Shodan se base sur l'analyse de l'entête HTTP renvoyée par l'appareil ou le serveur
- **www.shodan.io**
- Utilisation d'opérateurs de recherché: country, net, port,....

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Alternative à google:tineye**

- **Tineye**: consiste à faire de la recherche d'images inversées
- **www.tineye.com**

Le processus général d'une attaque

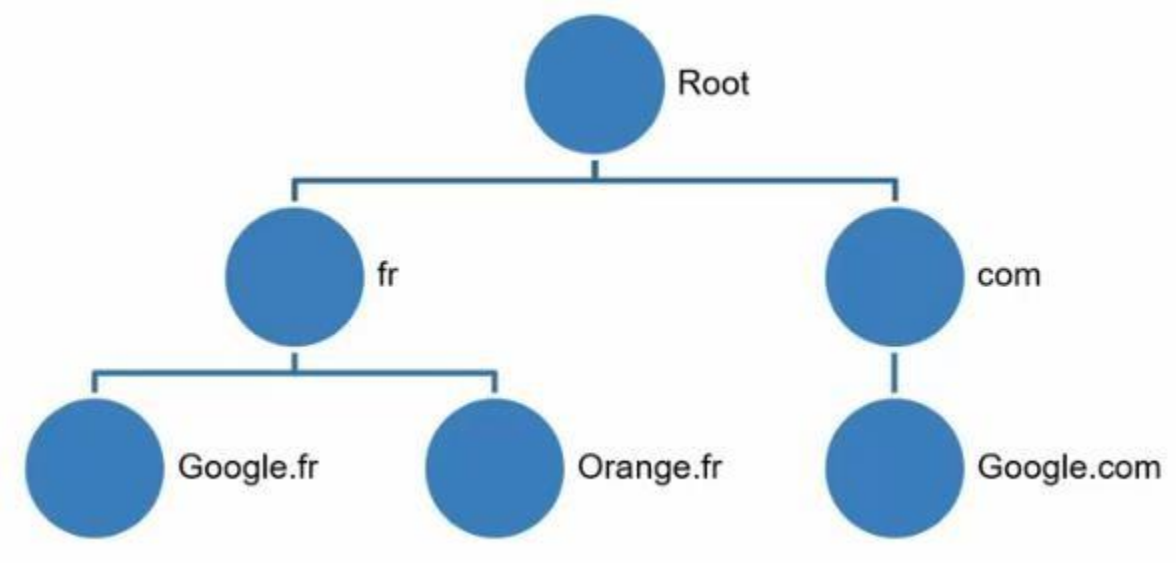
(P1) Probe: Collecte d'informations, phase de reconnaissance

- **DNS: domain Name System**
- Protocole permet de convertir un nom d'hôte/ domaine en une adresse IP;
- Port UDP 53

Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **DNS: domain Name System**



Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **DNS: enregistrements**

TYPE	FONCTION
A	Nom d'hôte vers adresse IPv4
AAAA	Nom d'hôte vers adresse IPv6
PTR	Inverse de A ou AAAA
MX	Nom de serveur mail

Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **DNS: fonctionnement**
- Un client fait une demande à un serveur DNS, en demandant l'adresse IP de fsts.ac.ma
- Le serveur DNS lui fournit l'adresse IP.

(P1) Probe: Collecte d'informations, phase de reconnaissance

Interogation du DNS:

- NSLOOKUP est utilisé pour récupérer des informations sur les serveurs de noms:
- **Procédure:**
  - Cmd ➔ nslookup entrer
  - @ du serveur
  - Set type=all
  - Nom du domaine

(P1) Probe: Collecte d'informations, phase de reconnaissance

Exemple: emi.ac.ma

```
C:\Users\mounia>nslookup
Default Server:  192.168.1.1
Address:  192.168.1.1

> set type=all
> emi.ac.ma
Server:  192.168.1.1
Address:  192.168.1.1

Non-authoritative answer:
emi.ac.ma
        primary name server = ns1.emi.ac.ma
        responsible mail addr = emiadm.emi.ac.ma
        serial  = 20180901
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
emi.ac.ma       MX preference = 10, mail exchanger = smtpgate1.emi.ac.ma
emi.ac.ma       MX preference = 10, mail exchanger = smtpgate2.emi.ac.ma
emi.ac.ma       text =
```

(P1) Probe: Collecte d'informations, phase de reconnaissance

Dig:

- Permet de récupérer des informations précieuses sur un nom de domaine
- Dig www.google.com
- Dig www.google.com mx
- Web: **toolbox.googlapps.com**

Le processus général d'une attaque

(P1) Probe: Collecte d'informations, phase de reconnaissance

- Scan de ports : **Nmap** pour déterminer la version des logiciels utilisés, les OS et les ports ouverts.
- Scan de vulnérabilités : programme **Nessus.**

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Ping et Traceroute/ tracert:**

- Pour afficher l'itinéraire que suit un paquet IP d'un hôte à l'autre.
- Nous pouvons utiliser les fonctionnalités de traceroute pour:
  - Déterminer le chemin exact que nos paquets prennent;
  - Découvrir la topologie réseau utilisée par le réseau cible;
  - Identifier les dispositifs de controle d'accès (comme un par feu) qui peuvent filtrer le traffic.

  - Sous windows on utilise la commande **TRACERT**.
  - Outil: **Visual route**

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Ping et Traceroute/ tracert:**

- **Ping**= tester la connectivité (si la machine cible fonctionne);
- **Traceroute=** voir les chemins empruntés (paquets)

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Traceroute/ tracert:**

```
C:\Users\mounia>traceroute emi.ac.ma
'traceroute' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\mounia>tracert emi.ac.ma

Tracing route to emi.ac.ma [196.200.140.2]
over a maximum of 30 hops:

  1    17 ms    27 ms    20 ms  192.168.1.1 [192.168.1.1]
  2     4 ms    80 ms    27 ms  160.178.152.1
  3    19 ms    29 ms   349 ms  adsl-186-65-192-81.adsl2.iam.net.ma [81.192.65.1
86]
  4    64 ms    90 ms    38 ms  adsl-177-65-192-81.adsl2.iam.net.ma [81.192.65.1
77]
  5    24 ms    13 ms    14 ms  adsl-42-12-192-81.adsl.iam.net.ma [81.192.12.42]

  6    42 ms    48 ms    51 ms  ae18.marsig2.mar.seabone.net [213.144.176.166]
  7    49 ms    65 ms    44 ms  ae22.parigi52.par.seabone.net [195.22.210.195]
  8    42 ms    57 ms    43 ms  vox-168-101.par.seabone.net [213.144.168.101]
  9     *        *        *     Request timed out.
 10    85 ms   149 ms   124 ms  105.73.6.138
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
```

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Géolocalisation des addresses IP:**

- Nombreux services en ligne;
- **https://www.iplocation.net/**

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Archivage des données publiques**

Remontée dans le temps

- **Organisation à but non lucratif;**
- **archive.org;**
- **Archiver le web d'une manière automatique;**
- **Véritable historique des sites web;**

(P1) Probe: Collecte d'informations, phase de reconnaissance

- **Internet**:
  - les enregistrements whois
  - Google hack;
  - shodan
- **Hors ligne**: catalogues, documents internes;
- Hors ligne; plus directe
  - *Dumpster diving*
  - *Shoulder surfing*
  - *Eavesdropping*
- **DNS**
  - Nslookup;
  - Dig;
- Traceroute/ping
- Géolocalisation;
- Archivage publique.
- .....

(P2) Penetrate: Intrusion et présence

- **Etape clé de l'intrusion;**
- Accès concret au système visé;
- utilisation des informations récoltées pour pénétrer un réseau;
- Utilisation d'une ou plusieurs vulnérabilités (Humaines / logicielles);
- **Le craquage de mot de passe**: Le craquage consiste à faire de nombreux essais jusqu'à trouver le bon mot de passe.
  - Il existe deux grandes méthodes :
    - le **brute force**
    - les **attaques par dictionnaires**.

(P2) Penetrate: Intrusion et présence

- **Attaque par force brute:** selon le degré de complexité de mot de passe;
  - Tester toutes les combinaisons possibles;
  - Puissance de calcul dans le cloud ➔ louer des service de traitement auprès d'un organisme (ex Microsoft azure, ….
- **Attaque par dictionnaire:**
  - Dictionnaires publiques conçu dans ce but.
  - Comparaison avec des listes de mots de passes;
  - le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci.

(P2) Penetrate: Intrusion et présence

- **Découverte et scan de la cible:**
- Les techniques **de scan de ports** sont utilisés pour découvrir les machines vulnérables pour les attaquer.
  - **Nmap**
- Cette phase est souvent basée sur l'exploitation des informations recueillies dans la phase « probe ».

(P3) Persist: Acquisition des privilèges administrateurs

- **Backdoors:**
- création d'un compte avec des droits de super utilisateur pour pouvoir se ré infiltrer ultérieurement.
- Une autre technique consiste à installer une application de contrôle à distance capable de résister à un reboot (ex. : un cheval de Troie) ;

(P4) Propagate: mouvement latéral

- **Elévation de privilèges**.
- cette étape consiste à observer ce qui est accessible et disponible sur le réseau local;
- Récupérer plus d'habilitations sur le système.

(P5) Paralyze: exécuter l'attaque, Mission achevée

- **L'éxécution de l'attaque**
- Cette étape peut consister en plusieurs actions, l'attaquant peut:
  - utiliser le serveur pour mener une attaque sur une autre machine
  - Détruire des données;
  - Endommager le système d'exploitation dans le but de planter le serveur.
- La finalité de l'attaque dépend de la motivation de l'attaquant.

(P5) Paralyze: exécuter l'attaque, Mission achevée

- **Attaque utilisant les exploits**:
- **Flooding (Saturation);**
- **Spoofing (Déguisement);**
- **Snifing (Ecoute).**
- **Ingénierie sociale**
- **Les malwares**

(P5) Paralyze: exécuter l'attaque, Mission achevée

Type1: Attaque utilisant les exploits

- Utiliser un exploit spécifique à une vulnérabilité ou un Framework qui regroupe plusieurs exploits connus
- Framework: **Metasploit**

(P5) Paralyze: exécuter l'attaque, Mission achevée

Type1: Attaque utilisant les exploits

Maquette à préparer

(P5) Paralyze: exécuter l'attaque

Type 2: Flooding (Saturation)

- Bloquer la disponibilité d'un service;
- En ligne: sites web
- Hors ligne: ransomwares
- Déni de service simple (DOS) Vs déni de service distribué (DDOS)
- **https://www.digitalattackmap.com/**

(P5) Paralyze: exécuter l'attaque

Type 2: Flooding (Saturation)

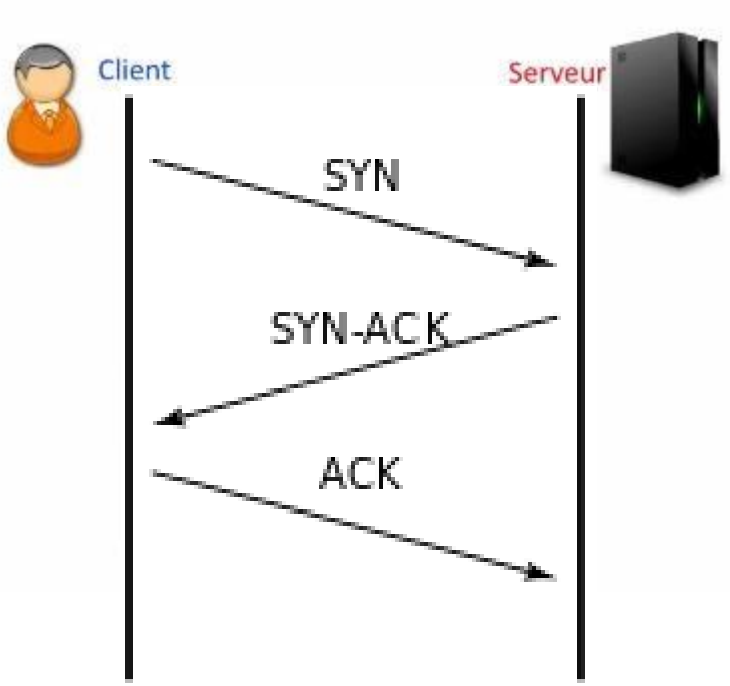
- **Attaque de type déni de service:**
- Envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra pas traiter tous les paquets et finira par se déconnecter du réseau.
- Le smurf (ICMP FLOOD): S'appuie sur le ping et les serveurs de broadcast . On falsifie d'abord son adresse IP pour se faire passer pour la machine cible.
- **TCP SYN FLOOD**;
- **UDP FLOOD;**

Outil: hping

(P5) Paralyze: exécuter l'attaque

Type 2: Flooding (Saturation)

TCP SYN FLOOD



- Saturer le serveur en envoyant une grande quantité de paquets TCP avec le flague « SYN » activé, sans répondre aux « ACK » (connexion semi-ouverte sur la machine)
- consommation des ressources (mémoire, CPU) sur le serveur jusqu'à écroulement.

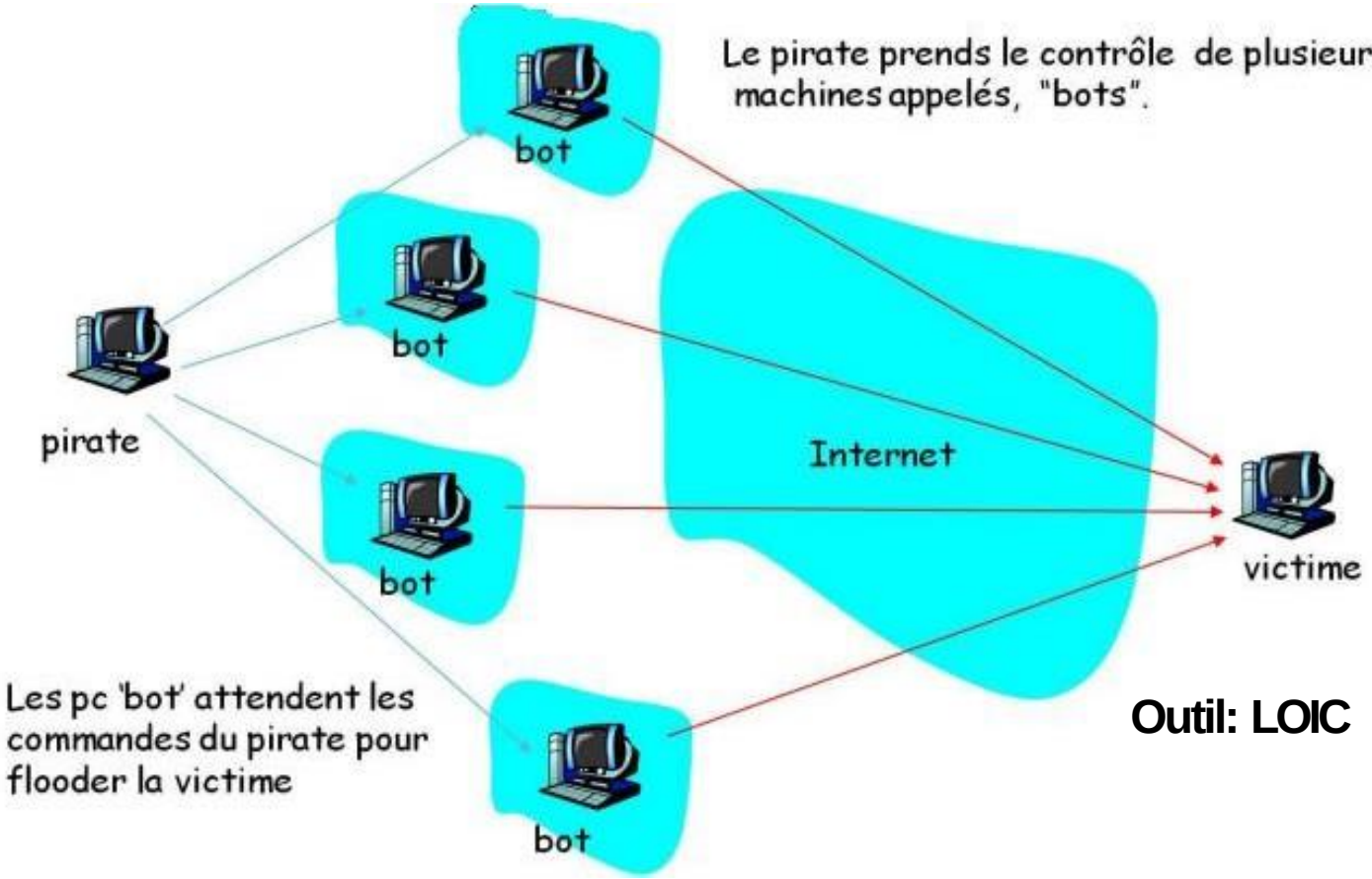
(P5) Paralyze: exécuter l'attaque

Type 2: Flooding (Saturation)

- **DDOS (distributed DOS)**
- Attaque de type déni de service;
- S'introduire sur plusieurs machines à partir des quelles l'attaquant va lancer une attaque sur une cible particulière.
- Attaque orchestrée généralement par un attaquant qui donne les commandes.

(P5) Paralyze: Distributed DOS (DDOS)

Type 2: Flooding (Saturation)



Outil: LOIC

(P5) Paralyze

Type3: Sniffing (écoute)

- L'attaquant doit se trouver au sein du réseau à écouter.
- **Pré-requis**:
  - Le PC de l'attaquant est connecté au réseau local;
  - La carte réseau doit être en mode ***« promisuous mode »***
    - C-à-d qu'elle peut voir même les trames Ethernet qui ne lui sont pas destinées.
- Un sinfer procède en deux ètapes:
  - Capture des paquets;
  - Analyse des paquets.

(P5) Paralyze

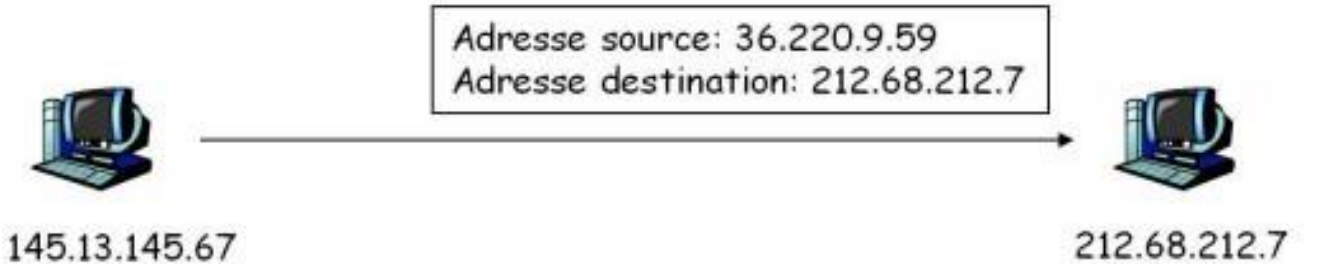
Type3: Sniffing (écoute)

- Sniffers populaires:
  - Wireshark (ethreal);
  - Tcpdump;
  - Snort (détecteur d'intrusion, contenant un composant du sniffing, fait l'objet de l'atelier 2 de ce module)

(P5) Paralyze

Type4: Attaques par spoofing:

- Principe: modifier l'identité de l'attaquant (déguisement);



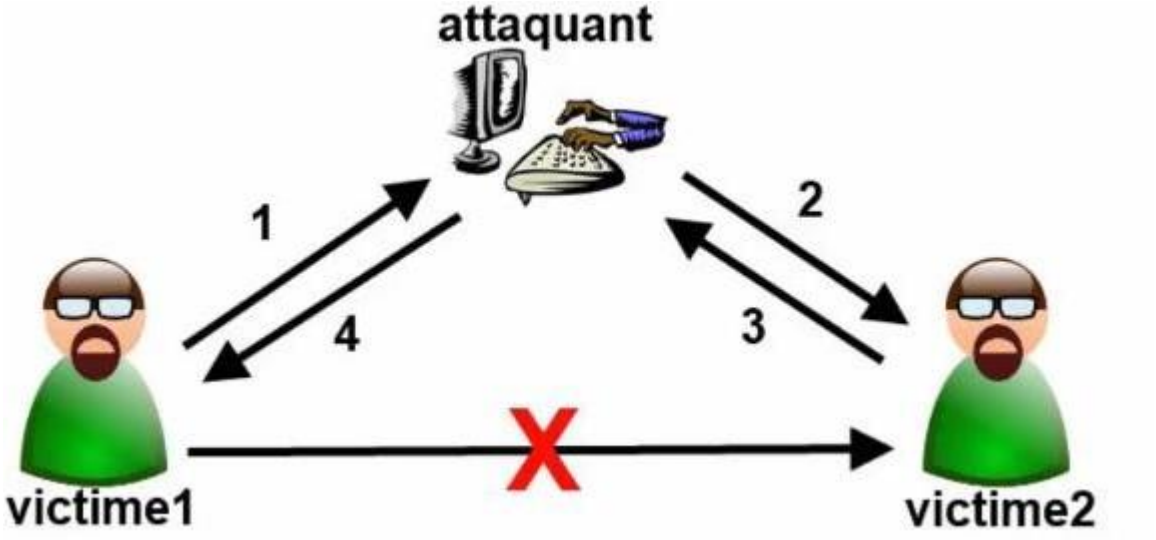
- L'attaquant envoie un datagramme IP en changeant l@ source et en la remplaçant par l@ source d'une autre machine.
- Lorsque l'attaquant ne veut pas être tracé.
- Possibilité de changer l'@ IP source dans Windows ou linux.

(P5) Paralyze

Type4: Attaques par spoofing:

L'homme au milieu (men in the midle):

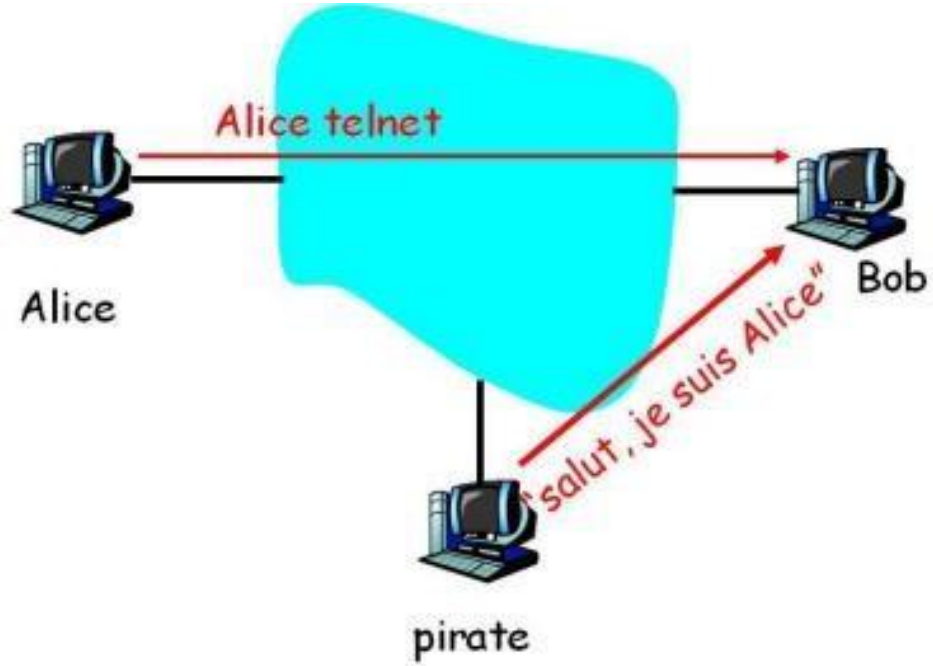
- Le but est d'intercepter les communications entre deux parties;
- L'attaquant sert de l'intermédiaire, il intercepte et renvoie le trafic.



(P5) Paralyze

Type4: Attaques par spoofing:

- **session hijcking**
- Prendre la contrôle d'une connexion tcp déjà établie;
- Combine des techniques de sniffing et de spoofing;
- Outils: **Hunt, hamster.**



(P5) Paralyze

Type4: Attaques par spoofing:

- **Le IP spoofing**: se faire passer pour une autre machine en falsifiant son adresse IP.
- Il existe des variantes, spoofer aussi des adresses e-mail, des serveurs DNS.

(P5) Paralyze

Ingénierie sociale

- Manipuler une personne pour obtenir quelques choses d'elle;
- Se base sur les interactions humaines et sur l'influence;
- **Faille humaine**: clé de réussite des piratages;
- Difficile à repérer techniquement;
- **Plusieurs formes**: Téléphone, en ligne, dumpster diving (faire les poubelles), shoulder surfing ();

(P5) Paralyze

Ingénierie sociale

Phases d'une attaque d'ingénierie sociale

(P5) Paralyze

Ingénierie sociale: compétences de l'attaquant

- Fait des prétextes;
- Demande directe d'informations (pressé);
- Story telling (émotions);
- Usurpation d'identité;
- Communication non verbale;
- Utiliser un partenaire;
- Exemple classique: un pirate se fait passer pour le support et appelle la secrétaire de l'entreprise;

(P5) Paralyze

Ingénierie sociale: fishing ou hamçonage

- Est une technique d'Ingénierie Sociale qui consiste à:
  - Récupérer des données personnelles auprès d'une ou plusieurs victimes;
  - Se faire passer pour une personne, un site ou un service;

(P5) Paralyze

fishing ou hamçonage: exemple

(P5) Paralyze

Ingénierie sociale

- **Le Spear phishing (attaque ciblée)**: personnaliser la victime;
- **Le pharming**: redirection du trafic depuis un site connu vers un site pirate;
- **Le E-Whorning en image**: Se faire passer pour une belle fille ou une femme attirante sur internet;
  - le but est d'échanger des photos et des védios à de potentiels victimes en échanges de grosses sommes d'argents;
  - La victime paye pour recevoir plus d'images ou plus de vidéos d'une personne que ce n'est pas celle qui prétend être (truquée);

(P5) Paralyze

Les malwares

- « **Malware** » signifie logiciel malveillant et sert de terme générique pour désigner un virus, un spyware, un ver, etc.
- Un malware est conçu pour causer des dommages à un ordinateur autonome ou un ordinateur en réseau.
- Dès lors que le terme « malware » est utilisé, il désigne un programme conçu pour nuire à votre ordinateur, qu'il s'agisse d'un virus, d'un ver ou d'un cheval de Troie.

(P5) Paralyze

Les malwares

- Virus/Vers
- Trojan
- Ransomware/ cryptolockers
- Spyware/ adware

(P5) Paralyze

Les malwares: virus, vers

- **Virus:** Est un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs. .
- Les dégâts causés vont du simple programme qui affiche un message à l'écran au programme qui formate le disque dur après s'être multiplié.
- Un virus informatique est plus dangereux qu'un ver informatique car il modifie ou supprime les fichiers alors qu'un ver ne fait que se répliquer, sans apporter de changements aux données.

Exemple de virus:

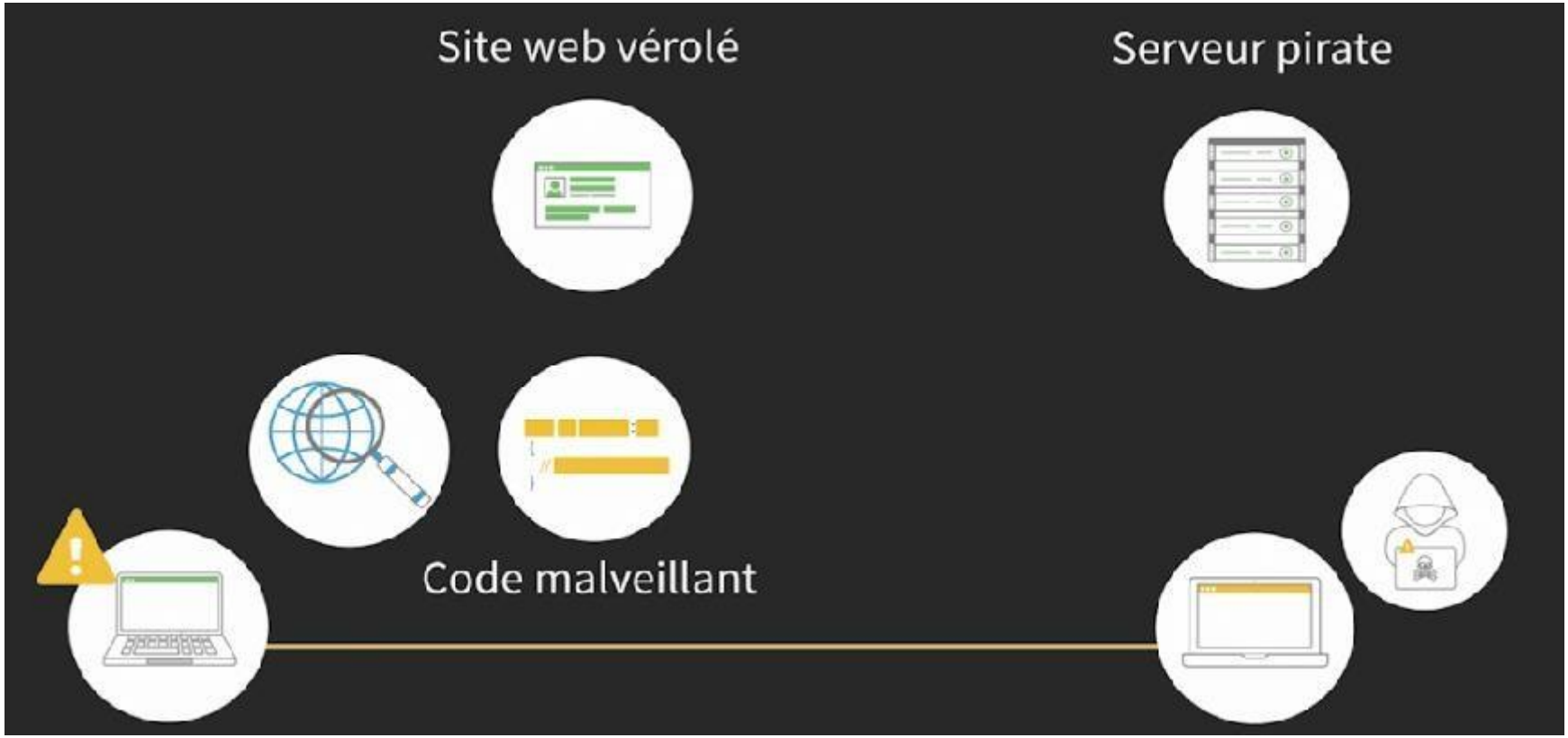
W32.Sfc!mod

ABAP.Rivpas.A

Accept.3773

(P5) Paralyze

Les malwares: Scénario



(P5) Paralyze

Les malwares: virus / vers

- **vers :** est un programme malveillant ayant la capacité de se répliquer eux-mêmes sans cesse sur un disque local, des partages réseau, etc.
- Le seul objectif d'un ver est de se répliquer encore et encore.
- Il n'altère aucune donnée ou aucun fichier sur l'ordinateur. À l'inverse d'un virus, il n'a pas besoin de se fixer sur un programme existant.
- Les vers se propagent en exploitant les vulnérabilités des systèmes d'exploitation.

Exemples:

W32.SillyFDC.BBY

Packed.Generic.236

W32.Troresba

Stuxnet

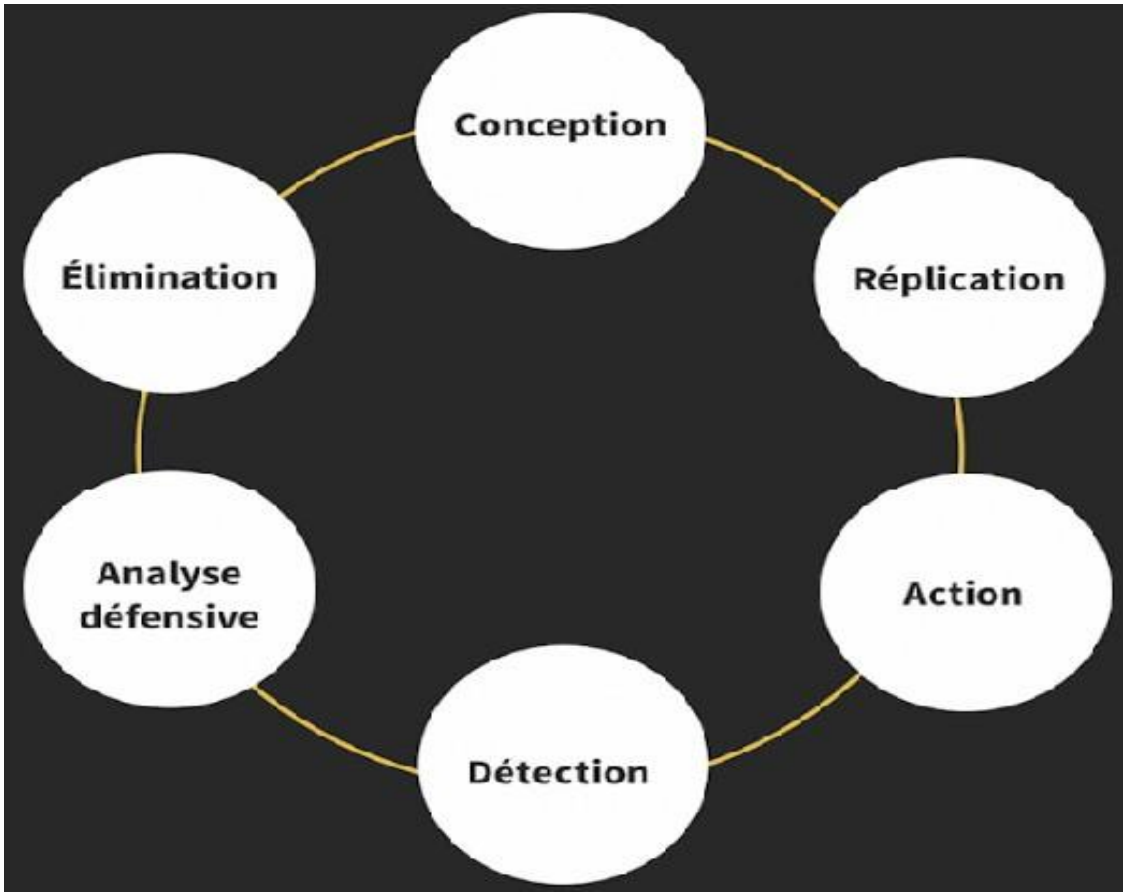
(P5) Paralyze

Les malwares: virus/ vers

- **Vers:**
- En raison de sa faculté à se répliquer, il occupe beaucoup d'espace sur le disque dur et consomme plus de ressources de processeur
- ce qui rend l'ordinateur plus lent.
- Il consomme aussi plus de bande passante sur un réseau.

(P5) Paralyze

Les malwares: cycle de vie d'un virus



(P5) Paralyze

Les malwares: Les trojans (Chauveau de Troie)

- **Cheval de Troie**: Sont des programmes informatiques cachés dans d'autres programmes. Ce nom vient de la légende grecque de la prise de Troie à l'aide d'un cheval en bois rempli de soldats qui attaquèrent la ville une fois à l'intérieur.
- Le but d'un cheval de Troie est de créer une porte dérobée (backdoor) pour qu'un attaquant puisse ensuite accéder facilement l'ordinateur ou le réseau informatique.
- Il peut aussi voler des mots de passe, copier des données, exécuter des actions nuisibles.
- **Exemple** : JS.Debeski.Trojan

(P5) Paralyze

Les malwares : Les spaywares /adwares

- **Les spaywares**: Sont des logiciels espion;
- PMAD: enregistrer les moindres faits et gestes de l'utilisateur;
  - Site internet visité;
  - Déclenchement de la webcam à distance;
  - Enregistrement de tout ce qui est tapé au clavier;
  - Liste des sms et numéros appelés (l'attaque cible un tél mobile).

(P5) Paralyze

Les malwares : Les spaywares /adwares

- **Les adwares:** sont des logiciels indésirables conçu pour afficher des publicités intempestives sur l'écran de la victime;
- la finalité n'est pas automatiquement de nuire à la victime;
- Afficher des publicités ciblés lors du navigation de la victime;
- Modifier les pages d'accueil du navigateur de la victime.

(P5) Paralyze

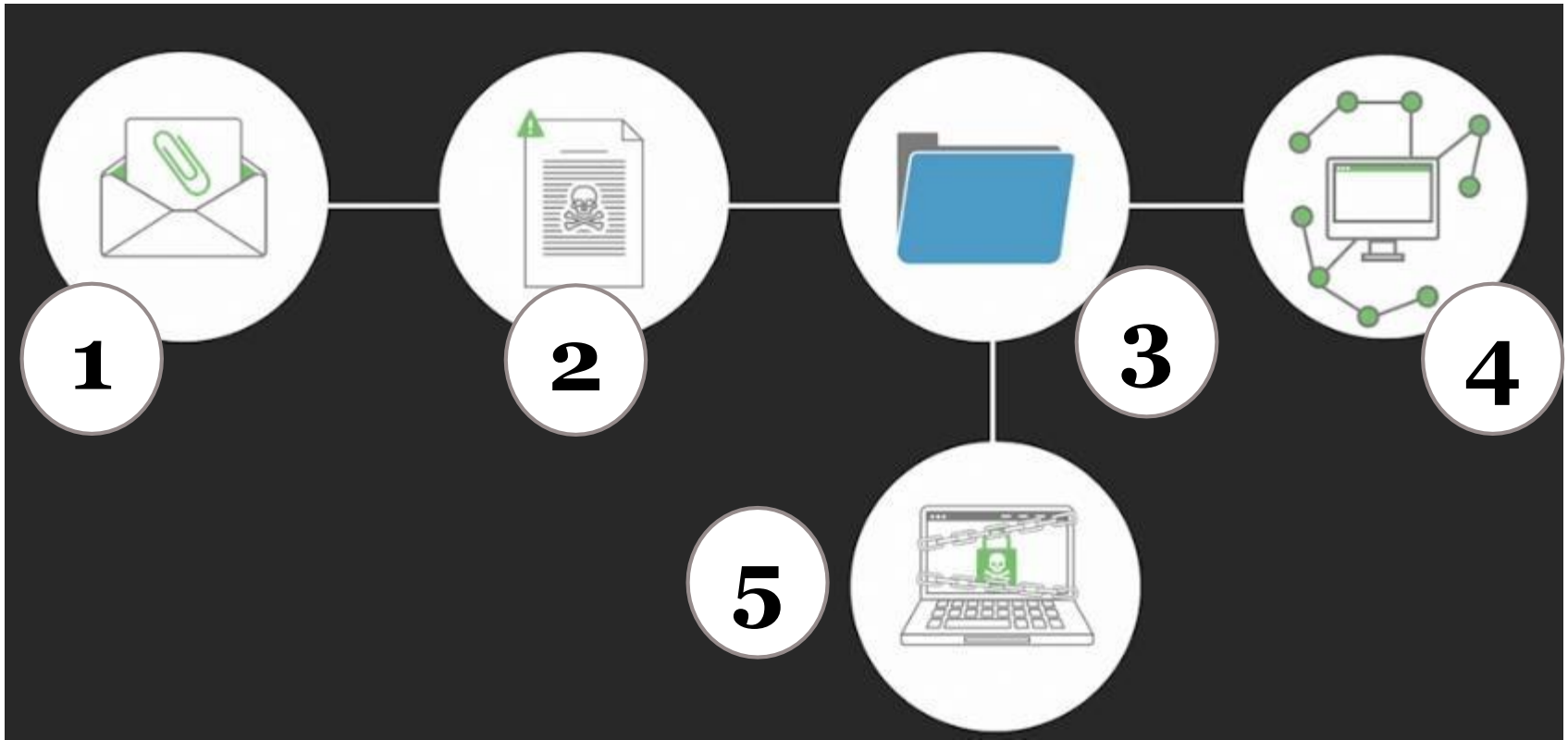
Les malwares : Les ransomwares /cryptolockers

- **Rançon** à verser aux pirates;
- Le but est de gagner rapidement de l'argent, en prenant en otage la machine attaquée, précisément, ces fichiers;
- Cette rançon correspond au versement d'une somme d'argent directement au pirate;
- Paiement en cryptomonaie (le bitcoin), ne permet pas de remonter à l'identité réelle du pirate➔ garantit l'anonymat;

(P5) Paralyze

Les malwares : Les ransomwares/ cryptolockers

- **Exemple de Scénario d'un cryptoloker**



Synthèse

Type d'attaques	Types d'attaque	Pilier visé	Exemples	explications
Par exploits	Modification	Integrité	• Virus • Vers • Chevaux de troie • CVE et exploit	
Flooding	Saturation (interruption)	Disponibilité	• Smurf; • Dos; • DDOS.	
Spoofing	Usurpation (Déguisement et fabrication)	Non-répudiation	• IP-spoofing • ARP-spoofing	
Sniffing	Accès (écoute et interception)	confidentialité	• Snifing; • Portes dérobées; • crakage de mot de passe	• Dictionnaire • Brute force

Les types d'attaques

Exercice

Donner pour chaque type d'attaque, le pilier de sécurité touché.

- Interruption
- Interception
- Modification
- Fabrication

Attaques et critères de sécurité

Exercice: **Pour chaque critère choisissez une attaque correspondante parmi les attaques**

Critère	Attaque correspondante	Attaque
Intégrité		Interception d'information
Confidentialité		Interruption de service
Authenticité		Modification d'information
Disponibilité		Usurpation d'dentité

Les défis d'une attaque

- **Attaque passive** : c'est la moins dangereuse
  - Ne modifie pas l'information;
  - Consultation de l'information.
- **Attaque active** : ce type d'attaque est dangereux
  - Modifie l'état d'une information, d'un serveur ou d'une communication;
  - Connexion frauduleuse à un host ou un réseau;
  - Altération des messages en transit sur un réseau (Denis de service).