Introduction à la CyberSécurité

Houssem MAHMOUDI
houssem.mahmoudi@ensicaen.fr

Chapitre 2

Les Menaces Informatiques

Plan

Introduction aux Menaces Informatiques

I. Introduction aux Menaces Informatiques

1. Définition

- Une menace informatique désigne tout événement ou action susceptible de causer des **dommages** ou des interruptions aux systèmes informatiques, aux réseaux, aux applications, aux données ou aux utilisateurs.
- Une menace permet d'exploiter une vulnérabilité pour compromettre le système.
- Il peut y avoir plusieurs menaces pour chaque vulnérabilité
- La connaissance des différents types de menaces peut aider à déterminer leurs dangerosité et à mettre en place des contrôles adaptés permettant de réduire leur impact.

I. Introduction aux Menaces Informatiques

2. Evolution des menaces

- L'évolution des menaces informatiques est étroitement liée à l'évolution des technologies de l'information et de la communication. On peut distinguer plusieurs phases clés :
  - **Années 1970-1980** : Apparition des premiers **Virus** informatiques, principalement comme expériences académiques ou blagues.
  - **Années 1990** : Propagation des malwares avec l'avènement d'Internet et des e-mails. Émergence des premiers **Vers** informatiques capables de se propager rapidement.
  - **Années 2000** : Sophistication des attaques avec l'apparition de **Botnets**, de **Rootkits** et d'exploits **Zero-day**. Les motivations deviennent de plus en plus financières.

I. Introduction aux Menaces Informatiques

2. Evolution des menaces

- **Années 2010** : Montée en puissance des **Ransomwares**, des attaques ciblées (**APT** - **A**dvanced **P**ersistent **T**hreats) et des menaces sur les appareils mobiles. Apparition des **Cyberattaques** commanditées par des États (**Cyberguerres**).
- **Les années 2020** : Augmentation des menaces liées à l'Internet des objets (**IoT**), à l'intelligence artificielle (IA) et au Cloud Computing. Intensification des attaques et utilisation de techniques d'évasion avancées.

I. Introduction aux Menaces Informatiques

3. Importance de la Cybersécurité

- Face à la sophistication des menaces informatiques, la Cybersécurité est devenue un enjeu crucial pour l'État, les organisations et les individus. Son importance se manifeste à plusieurs niveaux :
  - Economique.
  - Stratégique.
  - Juridique et réglementaire.
  - Réputation (image de marque).

Types de menaces informatiques

II. Catégories de menaces informatiques

1. Menaces internes

- menaces provenant de l'intérieur d'une organisation, généralement de la part de ses employés, partenaires ou personnes ayant accès aux systèmes et informations.
- Ces menaces peuvent être intentionnelles (fraude, sabotage) ou accidentelles (erreurs humaines).

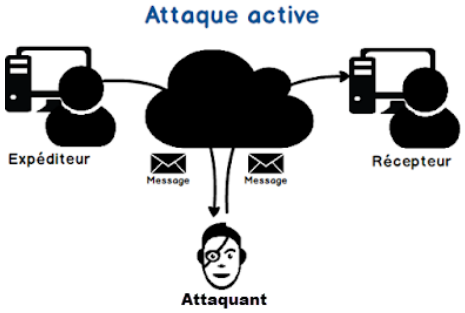
2. Menaces externes

- menaces provenant de l'extérieur de l'organisation, comme des hackers, des cybercriminels ou des groupes d'attaquants.
- Elles incluent des attaques comme les virus, les ransomwares, ou les attaques par déni de service (DDoS)

II. Catégories de menaces informatiques

3. Menaces actives

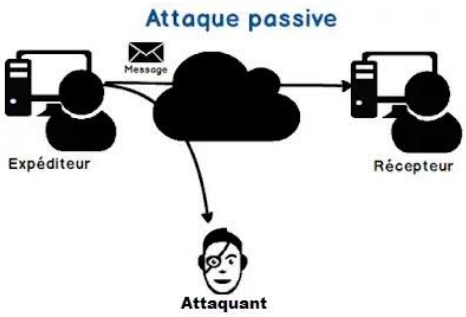
- L'attaquant intercepte le trafic transitant dans le réseau, modifie les informations et ré-envoi le trafic.
- Le pirate à le pouvoir de rediriger le trafic vers une autre interface, modifie les informations, insérer un malware, etc.



II. Types de menaces informatiques

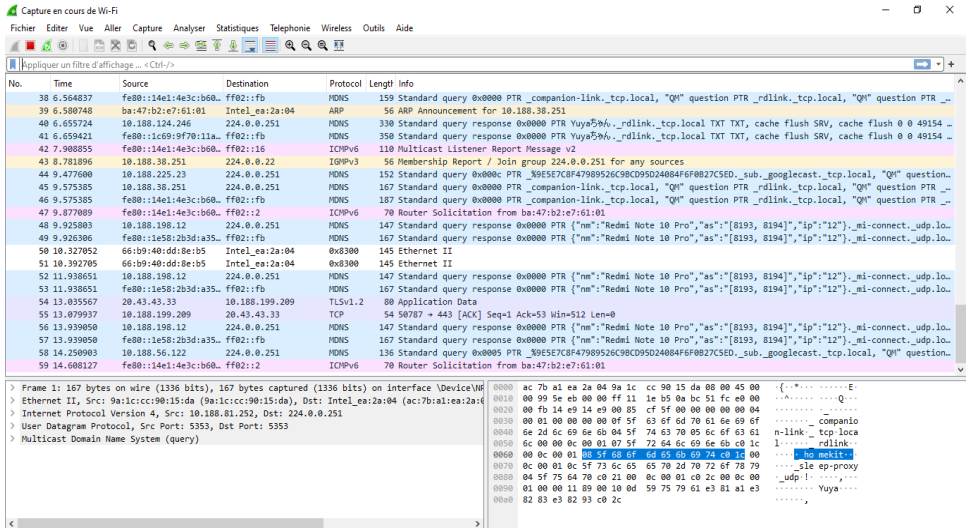
4. Menaces passives

- L'attaquant réalise une écoute du trafic réseau (**Sniffing**) avec l'intention de lire et analyser seulement les informations.
- Un Sniffer (renifleur) est un logiciel capable d'écouter le trafic réseau.



II. Types de menaces informatiques

2. Menaces passives



II. Types de menaces informatiques

3. Application

a. Quelle est l'attaque la plus dangereuse entre interne et externes ?

b. Compléter le tableau ci-dessous :

	Attaque active	Attaque passive
Définition		
Nuire au système		
Modification de l'information		
Menace à CID		

II. Types de menaces informatiques

3. Application

a. L'attaque interne est plus dangereuse : Connaissance du système, difficulté de détection, Confiance, Motivations variées.

b. Compléter le tableau ci-dessous :

	Attaque active	Attaque passive
Définition	Intercepte le trafic et le modifie	Intercepte le trafic et l'analyse
Nuire au système	Endommage le système	N'endommage pas le système
Modification de l'information	Oui	Non
Menace à CID	Confidentialité, Intégrité, Disponibilité	Confidentialité

Les techniques d'attaques par Malware

III. Les techniques d'attaques par Malware

1. Virus

- Code malveillant dont l'objectif est de perturber le fonctionnement du système, détruire les fichiers locaux de la machine et de se propager dans le corps d'un autre programme.
- Différents types de virus :
  - Virus boot
  - Virus dissimulé dans les exécutables
  - Macro-virus
- Différentes contaminations possibles:
  - Échange des clés USB
  - Pièces jointes au courrier électronique
  - Exécutables téléchargé de l'Internet

III. Les techniques d'attaques

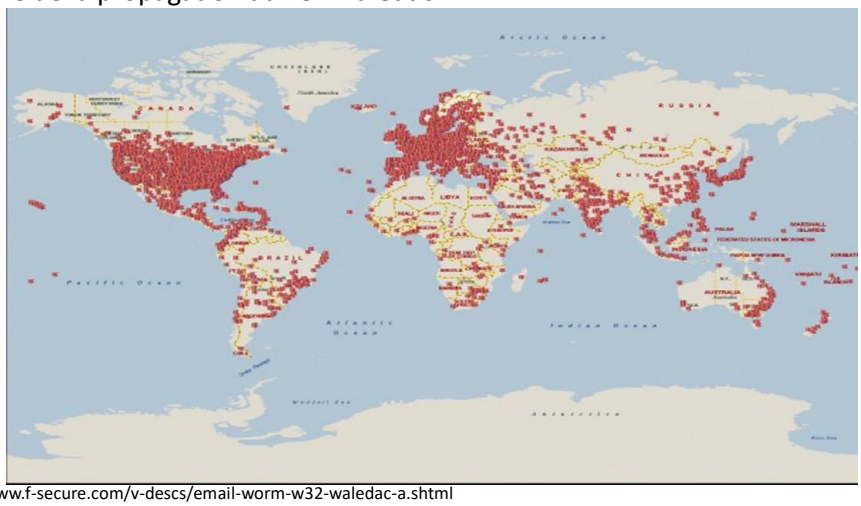
2. Vers

- Programme autonome capable de se propager sur d'autres ordinateurs à travers le réseau.
- Exploite les communications réseaux d'un ordinateur afin d'assurer sa reproduction sur d'autres ordinateurs
- Quelques exemples :
  - Code Red : utilisation d'une faille des serveurs IIS et défiguration des sites
  - Blaster : utilisation d'une faille du protocole windows DCM RPC
  - I Love you : déni de service sur les serveurs web

III. Les techniques d'attaques

2. Vers

- Cartographie de la propagation du ver **Waledac**



Source : https://www.f-secure.com/v-descs/email-worm-w32-waledac-a.shtml

III. Les techniques d'attaques

2. Vers : Parade

- Mettre à jour le système d'exploitation.
- Mettre à jour les applications qui communiquent via le réseau.
- Utilisation d'un pare feu est indispensable pour empêcher les non autorisés.
- Ne pas ouvrir des fichiers récupérés par e-mail.

III. Les techniques d'attaques

3. Cheval de Troie

- Appelé ausii Trojan, c'est un programme à apparence légitime contient un code nuisible qui exécute des fonctions non légitime sans l'autorisation de l'utilisateur.
- Permet d'ouvrir une porte dérobée (**Backdoor**) pour permettre au pirate de s'introduire au système infecté afin d'en prendre le contrôle.
- Un cheval de Troie peut :
  - Voler des mots de passe
  - Copier des données sensibles
  - Exécuter toute autre action nuisible

- Les chevaux de Troie sont généralement propagés par l'ingénierie sociale.

III. Les techniques d'attaques

3. Cheval de Troie : Parade

- Évitez de cliquer sur les pièces jointes suspectées.
- Bloquer les ports inutilisés.
- Évitez de télécharger les fichiers à partir d'une source non fiable.
- Analyser les supports amovibles avant utilisation.
- Configurer le pare feu pour bloquer des connexions non autorisés.
- Equipez votre machine par une solution de protection comprenant un antivirus professionnel, un anti-malware,…

III. Les techniques d'attaques

4. Spyware

- Programme espion, chargé de collecter des informations sur l'utilisateur de l'ordinateur dans laquelle il est installé.
- La collection d'informations peuvent être :
  - Des adresses web URL des sites visités.
  - Les mots clés saisis dans les moteurs de recherche.
  - Analyse des achats réalisés via Internet.
  - Des informations personnelle.

III. Les techniques d'attaques

4. Spyware : Parade

- Les outils :
  - Antispywares (Spybot, Windows defender, …)
- L'éducation
  - Sensibiliser les utilisateurs sur les risques liés à l'installation de logiciels non directement utiles (Extention dans la barre dans les navigateurs, codec DivX, …)
  - Ne pas consulter des sites douteux.
  - Inciter les utilisateurs à signaler l'infection de leurs machines par un spyware.

III. Les techniques d'attaques

5. Spam

- On appelle spam (pourriel, courrier indésirable ou junk mail) l'envoi massif des courriers électronique, souvent de nature publicitaire, à des destinataires ne l'ayant pas solliciter.
- La liste des adresses électroniques des destinataires est collectée depuis Internet grâce à des logiciels robots (forum, groupe de discussion,…).
- Les spammeurs lancent une application permettant l'envoi successive du message publicitaire à chaque adresse.

III. Les techniques d'attaques

5. Spam

Les Spams en quelques chiffres :

- ❑ 160 milliards de courriels envoyés par jour dans le monde
- ❑ 96,8 % des personnes ont reçu des messages de spam
- ❑ En 2023, plus que 58 % du trafic mondial des e-mails est considéré comme du spam

Sources :

- https://www.emailtooltester.com/en/blog/spam-statistics/
- https://worldmetrics.org/spam-statistics/

III. Les techniques d'attaques

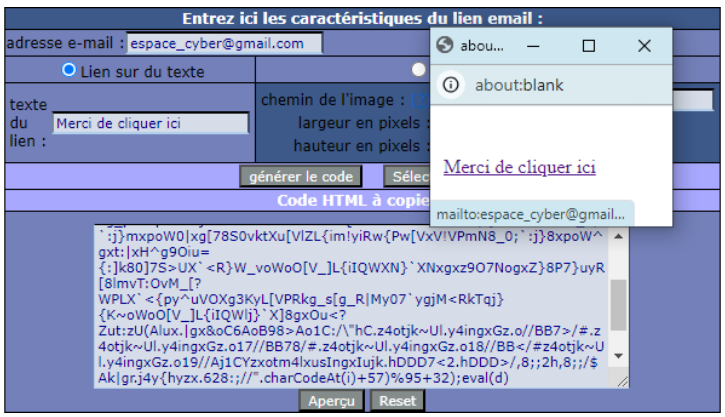
5. Spam : Parade

- Ne jamais acheter un produit ou un service dont la publicité a été réalisée par un SPAM.
- Ne jamais répondre à un SPAM.
- Sur les forums, blogs et tout formulaire non administratif, utiliser une autre adresse mail ou créer des adresses jetables.
- Utiliser les filtres anti spam des clients de messagerie pour séparer les vrais courriers des spams.

III. Les techniques d'attaques

5. Spam : Parade

- Ne jamais mettre une adresse électronique en clair sur une page web (utiliser un site comme « *www.caspam.org* » pour la masquer.



III. Les techniques d'attaques

6. Keylogger

- Un Keylogger est un malware chargé d'enregistrer les frappes de touche du clavier à l'insu de l'utilisateur.
- Les keyloggers sont invisibles, indétectables et se lance pendant le démarrage du système d'exploitation.
- Les keyloggers exploitent une fonction système pour surveiller toutes les frappes du clavier.
- Les keyloggers sont capables de sauvegardés les URL visités, les courriers électroniques, scanner les cookies stockés,…
- Il existe deux types de keyloggers : les matériels et les logiciels.
- Le Keylogger envoi les données collectées au pirate.

III. Les techniques d'attaques

6. Keylogger : Parade

- La meilleure façon de se protéger est la vigilance.
- Ne pas installer de logiciels dont la provenance est douteuse.
- Il est conseillé de ne pas se connecter à des sites sécurisés depuis un Cybercafé à partir d'un ordinateur tiers (Accès à un compte bancaire).

III. Les techniques d'attaques

7. Phishing

- Appelé aussi Hameçonnage, technique d'ingénierie sociale utilisée par des arnaqueurs (**Scammers**).
- Le phishing constitue une attaque de masse qui vise à abuser de la naïveté des clients ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire…

III. Les techniques d'attaques

7. Phishing

1. Réception d'un mail utilisant le logo et les couleurs de l'entreprise.
2. Demande pour effectuer une opération comme la mise-à-jour des données personnelles ou la confirmation du mot de passe.
3. Connexion à un faux-site identique à celui de l'entreprise et contrôlé par l'attaquant.
4. Récupération par l'attaquant des identifiants/mots de passe (ou tout autre donnée sensible) saisie par le client sur le faux site.

III. Les techniques d'attaques

7. Phishing – Exemple 1

De: "@ADMIN ZIMBRA" <pauline.videau@thouars-communaute.fr>
Envoyé: Jeudi 1 Septembre 2016 13:27:48
Objet: Mise à jour importante

Chers utilisateur Léo

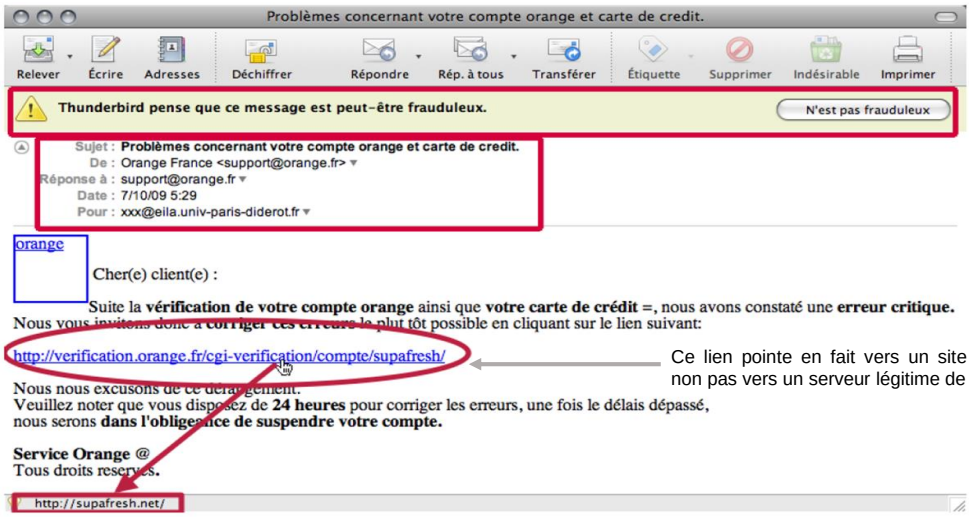
Nous avons réalisé que votre compte de messagerie web est accessible depuis une autre IP pour éviter la désactivation, cliquez sur le lien ci-dessous pour vérifier les informations de votre compte.

CLICK HERE

Merci et Désolé pour le dérangement
Admin - Webmaster

III. Les techniques d'attaques

7. Phishing – Exemple 2



Ce lien pointe en fait vers un site frauduleux et non pas vers un serveur légitime de l'entreprise

III. Les techniques d'attaques

7. Phishing – Exemple 3

III. Les techniques d'attaques

8. Ingénierie sociale

- L'ingénierie sociale constitue une attaque ciblée qui vise à exploiter la naïveté des employés de l'entreprise :
  - Pour détourner directement des informations confidentielles,
  - Pour introduire des logiciels malveillants dans le système d'information de la banque.

par téléphone

par réseaux sociaux

par e-mail

- les scénarios d'ingénierie sociale sont illimités, elle se basent sur l'imagination des attaquants et la naïveté des victimes…

III. Les techniques d'attaques

9. Scam

- Réception d'un courrier électronique du descendant d'un riche proche décédé dont il faut transférer les fonds.
- Beaucoup de déclinaisons connues (loterie, arnaque aux offres d'emplois, …)

III. Les techniques d'attaques

10. Ransomware

- Malware permet le chiffrement des données contenues sur les disques durs connectés à la machine.
- Envoi de la clé de déchiffrement contre rémunération.

III. Les techniques d'attaques

10. Ransomware – Parade

- Mettre en place des filtres des emails pour bloquer les pièces jointes suspectes et les liens malveillants.
- Former les employés à reconnaître les tentatives de phishing et des techniques d'ingénierie sociale utilisées pour diffuser les ransomwares.
- Utiliser des solutions de protection des endpoints pour surveiller et protéger les terminaux contre les attaques.
- Installer les correctifs pour combler rapidement les vulnérabilités connues.
- Mettre une stratégie de sauvegarde des données (Backup) (complète, incrémentielle, continue,…)

III. Les techniques d'attaques

11. Rootkits

- Un Rootkit est un type des malwares conçu pour permettre à des pirates informatiques d'accéder à une machine victime et la contrôler.
- Les Rootkits sont capables de dissimuler leurs présences, mais bien qu'ils restent masqués, ils sont toujours actifs. Ils se chargent avec le système d'exploitation !
- les Rootkits permettent aux cybercriminels de voler des données à caractère personnel et des informations financières, d'installer des logiciels malveillants ou d'utiliser les ordinateurs dans le cadre d'un botnet.
- **Exemple** : Stuxnet, Flame, Necurs, ZeroAccess.

III. Les techniques d'attaques

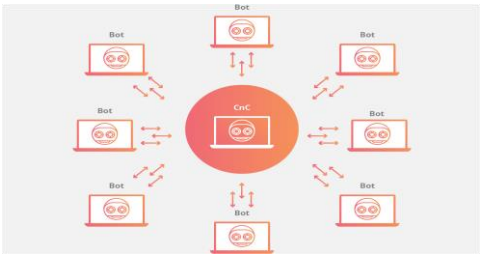
11. Rootkits – Parade

- Mettre le système à jour.
- Se méfier des attaques d'ingénierie sociale.
- Eviter des emails suspects contenant des pièces jointe (PDF, fichier Word, etc...) ou des liens vers des sites web malveillants.
- Développer et tester régulièrement des plans de réponse aux incidents pour être prêt à réagir efficacement en cas d'attaque.
- Télécharger les fichiers provenant des sources fiables.

III. Les techniques d'attaques

12. Botnets

- Type de virus se propagent silencieusement dans Internet sans y commettre le moindre dégât.
- L'ensemble des ces virus déployés est appelé botnet. (Ro**bot Net**work).
- Les machines infectées par ces virus sont nommés **Zombies**. Ces appareils peuvent être des ordinateurs, serveurs, smartphones, caméra IP ou des objets connectés.
- Ces appareils compromis sont contrôlés et commandés à distance par un master.



III. Les techniques d'attaques

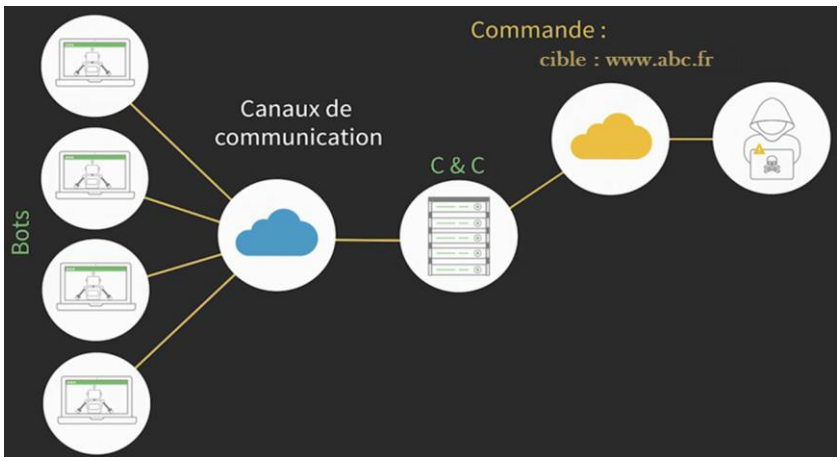
12. Botnets

- Les objectifs des Botnets :
  - Réalisé une attaque de Déni de service : saturé la ressource afin quelle soit non disponible.
  - Génère des envois massives des spams.
  - Utilise la puissance de calcul de la machine victime pour miner de la Cryptomonnaie.
  - Botnet as a Service : le pirate peut loué son réseau de botnet à d'autres pirates (Cyber arme).
- Exemple de Botnet :
  - Botnet Zeus : vole des informations bancaire
  - Botnet Mirai : réalise des attaques DOS

III. Les techniques d'attaques

12. Botnets

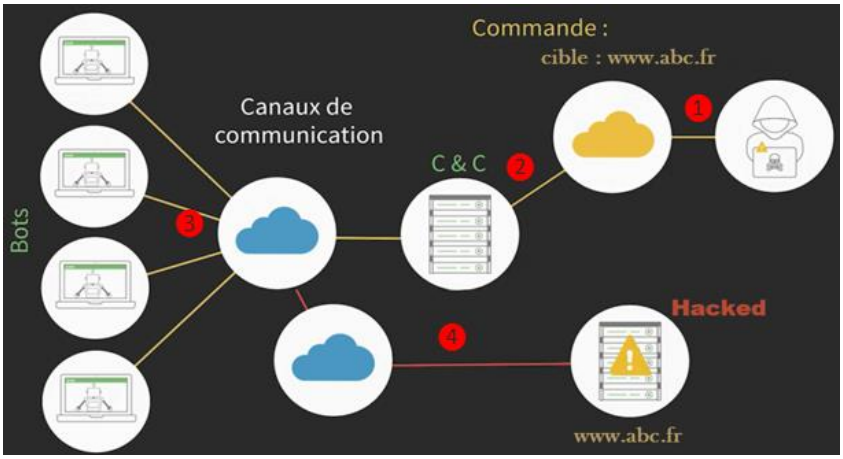
- Fonctionnement des Botnets



III. Les techniques d'attaques

12. Botnets

- Fonctionnement des Botnets



Les attaques sur les réseaux

IV. Les attaques sur le réseau

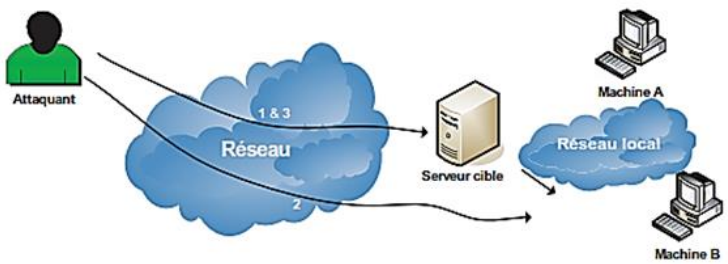
1. Sniffing

- Sniffing ou renifleurs des paquets est un Software ou hardware permettant d'écouter et analyser le trafic qui transite sur le réseau.
- Les données analysées sont : paquets IP, segments TCP/UDP, protocoles applicatifs qui permet à un :
  - Administrateur réseau : Détecter les problèmes de congestion et les accidents qui peuvent arriver.
  - Pirate : Savoir des informations clés (Adresse source, numéro de séquence, données non chiffrées…)
- Plusieurs outils permettant de réaliser l'attaque de sniffing : Wireshark, TCPDump

IV. Les attaques sur le réseau

2. IP Spoofing

- La technique Spoofing ou usurpation d'identité permet à un pirate de s'infiltrer dans un réseau en se faisant passer pour un autre de confiance.
- L'attaque IP Spoofing consiste à se faire passer pour une autre machine en utilisant son adresse IP comme adresse IP source.



IV. Les attaques sur le réseau

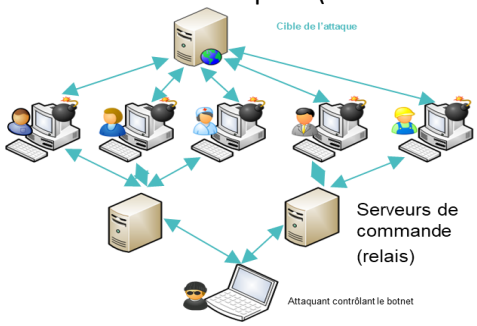
3. Déni de service : DOS

- L'attaque de type « Denial Of Service » a pour but de rendre un service, un ordinateur, un routeur ou un réseau non opérationnel.
- C'est une attaque très facile à mettre en place et très difficile à empêcher.
- Une attaque DOS permet à un attaquant de :
  - Récupérer un accès : Obtenir le contrôle d'une machine ou d'un réseau.
  - Masquer les traces : Ce type d'attaque permet également de crasher une station (**serveur de journalisation**) qui contient des traces du passage d'un pirate.

IV. Les attaques sur le réseau

4. Déni de service distribué : DDOS

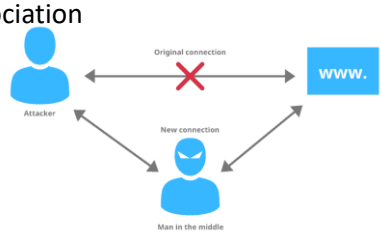
- L'attaque DDOS (Distributed Denial Of Service) est une sorte d'attaque DOS provoquée simultanément par plusieurs machines vers la victime. L'objectif est de faire tomber un système ou de saturer la bande passante de la victime.
- Nécessite un grand nombre de machines corrompues (incluant les objets connectés).



IV. Les attaques sur le réseau

5. Man in the Middle : MITM

- L'attaque de l'homme du milieu ou Man in The Middle (MITM) est une technique où l'attaquant intercepte, d'une manière invisible, la communication entre deux ordinateurs, pour écouter, altérer ou détruire les informations transmises.
- L'attaque a pour but de falsifier la relation **Adresse MAC/Adresse IP** sur les ordinateurs du réseau afin de pouvoir recevoir et retransmettre les données.
- Cela est possible grâce à la table ARP qui met en cache cette association

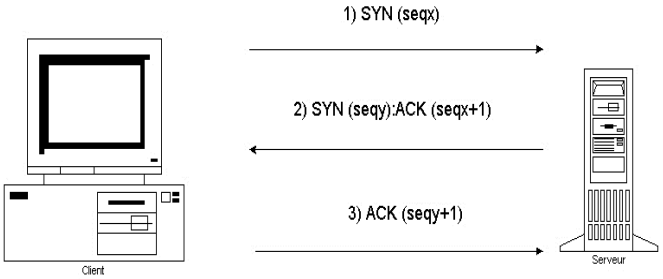


IV. Les attaques sur le réseau

6. SYN Flooding

Rappels – établissement d'une connexion TCP

- Connexion en 3 temps (Three Way Handshake) : c'est la phase **d'établissement de connexion**, elle est obligatoire entre un client et un serveur qui utilise le protocole TCP.

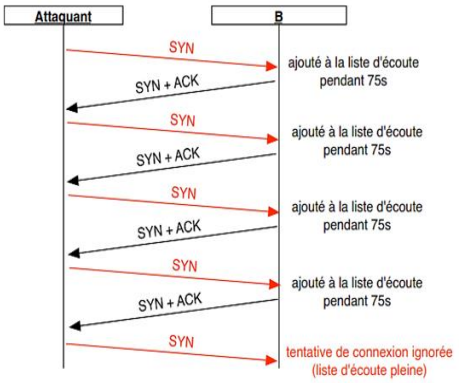


Après la phase d'établissement de connexion, la phase d'échange des données commence.

IV. Les attaques sur le réseau

6. SYN Flooding

- L'attaque SYN Flooding consiste à demander plusieurs connexions et ne pas terminer la connexion.
- Lors d'une demande de connexion, le serveur est en attente et bloque une partie de ses ressources pour cette nouvelle connexion pendant un certain temps.
- Le but de l'attaquant est d'envoyer plus de demande de connexion que le serveur ne peut pas les traiter tous ensembles dans un temps donné.



IV. Les attaques sur le réseau

7. Zero-day attaque

- Une attaque zero-day (vulnérabilité zero-day) est une cyberattaque qui exploite une vulnérabilité dans un logiciel/application/système avant que les développeurs ne la détectent.

Caractéristiques principales :

- Exploite une vulnérabilité inconnue ou non corrigée dans un logiciel.
- Très difficile à détecter et à contrer car la faille n'est pas encore connue publiquement.
- Peut causer des dommages importants avant qu'un **correctif** (patch) ne soit disponible.

IV. Les attaques sur le réseau

7. Zero-day attaque

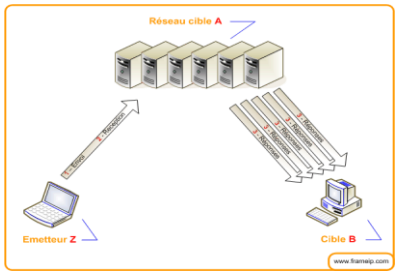
Les mesures de protection

- Pour se protéger contre les attaques zero-day, il est recommandé de :
  - Maintenir tous les logiciels et systèmes à jour.
  - Limiter le nombre d'applications installées.
  - Utiliser un pare-feu et un VPN.
  - Former les utilisateurs aux bonnes pratiques de sécurité.
  - Utiliser une solution antivirus complète.

IV. Les attaques sur le réseau

8. Attaque Smurf

- Attaque se base sur le protocole ICMP (Internet Control Message Protocol).
- L'attaque smurf est une attaque par déni de service distribué, consiste à noyer la victime par un flux de réponse ICMP.
- Le pirate inscrit **l'adresse IP de la cible** comme adresse source dans le paquet ICMP *echo request* qu'il envoie à une destination (pour amplifier l'attaque le pirate envoie la requête à une adresse de diffusion).



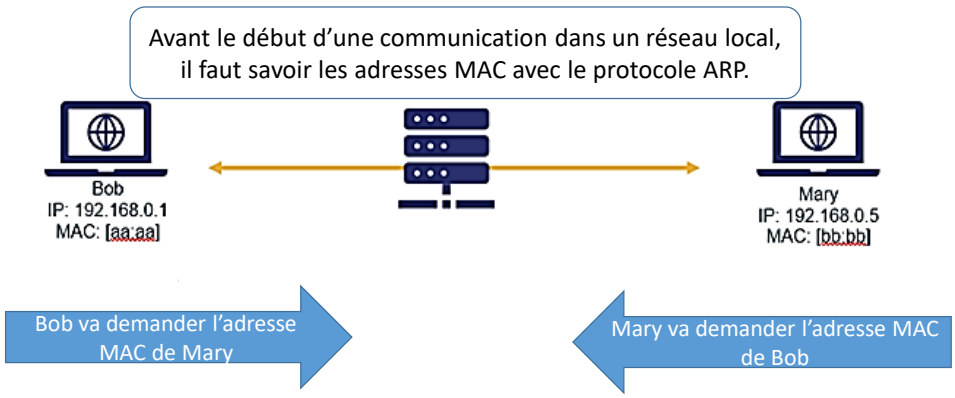
IV. Les attaques sur le réseau

9. ARP Spoofing

- Le protocole **ARP** « **A**ddress **R**esolution **P**rotocol » est un protocole qui implémente le mécanisme de traduction d'une adresse IP (32 bits) en une adresse MAC (48 bits).
- ARP Spoofing ou « ARP cache poisoning » est une technique utilisée pour attaquer tout **réseau local** utilisant le protocole ARP.
- Consiste à empoisonner les tables de correspondance <**adresse IP : adresse MAC**> (Table ARP) de tous les équipements informatiques d'un réseau pour rediriger le trafic réseau d'une machine victime vers la machine pirate.
- Le Hacker envoie des paquets **ARP réponse** au victime indiquant que la nouvelle adresse MAC de la passerelle est la sienne.

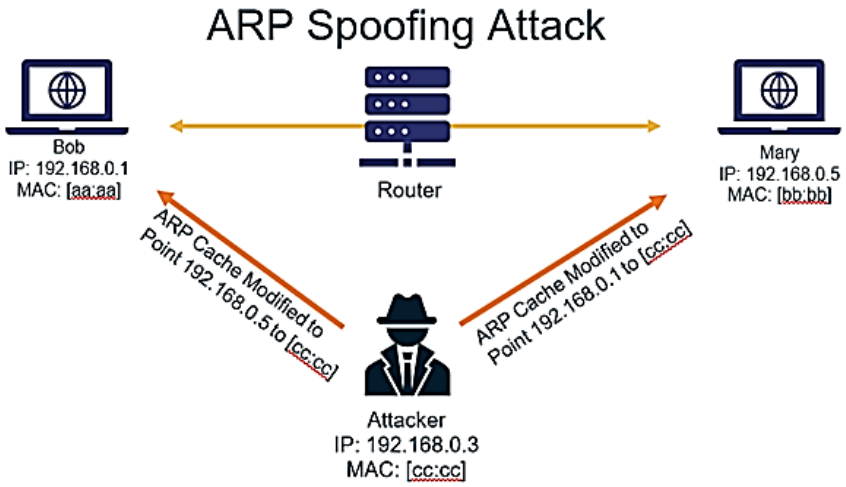
IV. Les attaques sur le réseau

9. ARP Spoofing



IV. Les attaques sur le réseau

9. ARP Spoofing – Démo



IV. Les attaques sur le réseau

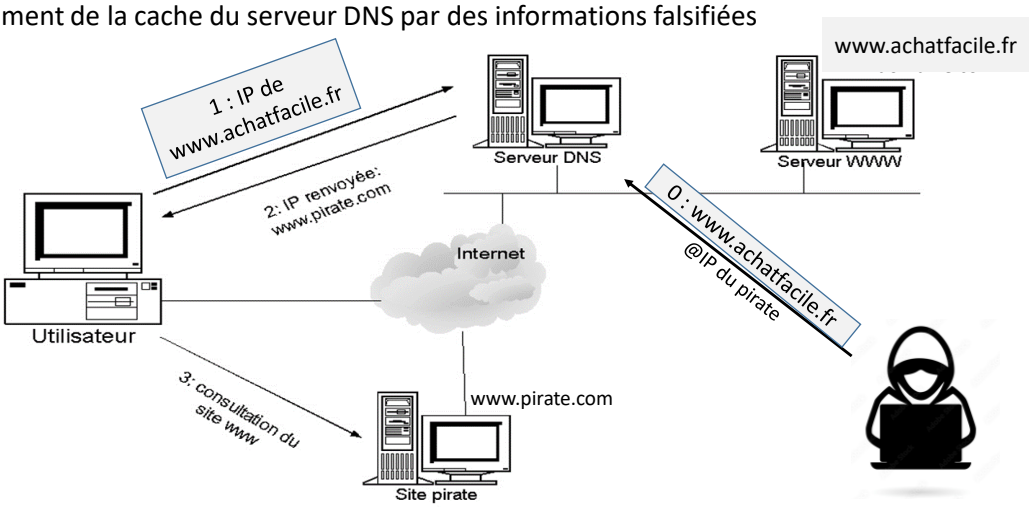
10. DNS Spoofing

- Appelé aussi DNS Cache poisoning. L'objectif de cette attaque est d'empoisonner la cache DNS par des fausses informations du serveur DNS, l'attaque se déroule en plusieurs étapes :
  1. Le pirate envoi au serveur DNS cible des informations falsifiées, à savoir un nom de domaine publique correspond à une adresse IP du pirate.
  2. Les informations erronées sont alors mises dans le cache du serveur DNS cible.
  3. Une machine faisant une requête sur le serveur DNS cible demandant la résolution d'un des noms corrompus aura pour réponse une adresse IP de la machine pirate.

IV. Les attaques sur le réseau

10. DNS Spoofing

Empoisonnement de la cache du serveur DNS par des informations falsifiées



IV. Les attaques sur le réseau

11. Session Hijacking

- Appelé aussi « Détournement de session ».
- Permet à un pirate de voler la session d'un utilisateur légitime connecté à une application Web.
- Ainsi, un pirate peut être connecté à une application Web sans avoir l'identifiant et le mot de passe de l'utilisateur légitime.

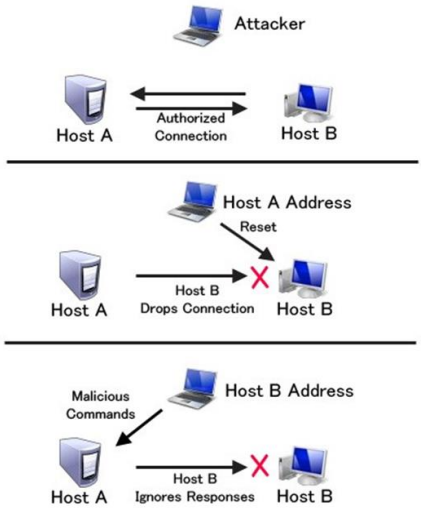
IV. Les attaques sur le réseau

11. Session Hijacking

1. L'attaquant écoute le réseau et attend que l'utilisateur se connecte avec son login/mdp

2. Une fois la session est capturée, l'attaquant essaye de mettre l'utilisateur en état hors service.

3. L'attaquant va utilisé la session capturée pour s'authentifier auprès du serveur (Host A).



IV. Les attaques sur le réseau

12. Attaque sur les mots de passe

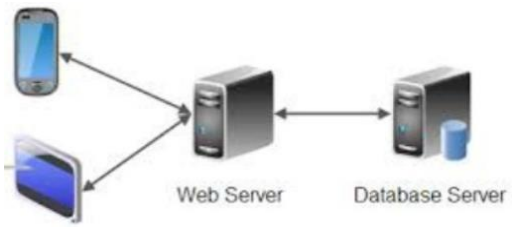
- Tentatives pour obtenir des mots de passe afin d'accéder de manière non autorisée à des comptes utilisateurs et des systèmes.
- On trouve plusieurs technique pour cracker un mot de passe :
  - **Attaque par Brute Force** : Méthode consiste à essayer toutes les combinaisons possibles de chiffres, symboles et caractères jusqu'à trouver le bon mot de passe.
  - **Attaque par Dictionnaire** : Méthode consiste à utiliser une liste prédéfinie de mots « dictionnaire » pour tester chacun comme mot de passe.
  - **Attaque par Rainbow Table** : Utilise des tables pré calculées de hachages de mots de passe. Permet de retrouver rapidement un mot de passe à partir de son hachage.

Les attaques sur les applications Web

V. Les attaques sur les applications Web

1. Introduction

- **Application Web** est hébergée sur un **serveur Web**, qui est installé sur un **système d'exploitation**.
- Un serveur Web vulnérable est exploitable pour attaquer une application Web.
- Un système d'exploitation vulnérable est exploitable pour attaquer le serveur et l'application Web.
- Diverses attaques ciblent les applications Web, l'exploitation de leurs vulnérabilités permet à un pirate de voler les données, perturber les services, ou accéder au système et le réseau.



V. Les attaques sur les applications Web

2. Injection SQL

- Le langage SQL (Structured Query Language) permet d'interagir avec les bases de données.
- Les applications Web modernes utilisent des bases de données pour gérer les données et afficher un contenu dynamique aux clients.
- L'injections SQL ou SQLi, est une attaque sur une application Web qui permet au pirate d'injecter des **commandes SQL malveillantes** dans l'application Web pour compromettre la base de données et accéder à des données confidentielles.

V. Les attaques sur les applications Web

2. Injection SQL

Objectifs d'une attaque SQLi :

- Contournement de l'authentification.
- Déterminer la structure de la base de données.
- Vol d'informations sensibles.
- Supprimer des données de la base de données
- Exécution des commandes sur le SGBD pour interagir avec l'OS (obtenir un shell distant).

V. Les attaques sur les applications Web

3. Cross-Site Scripting (XSS)

- L'attaque XSS consiste à injecter du code malveillant (généralement du JavaScript) dans une application Web via les zones de texte.
- Ce code malveillant s'exécute dans le navigateur des utilisateurs
- L'exploitation de cette attaque permet Vol de cookies (session), redirection vers des sites malveillants, défiguration de sites web exécution de scripts malveillants dans le navigateur de la victime.

V. Les attaques sur les applications Web

3. Cross-Site Scripting (XSS)

L'objectif d'une attaque XSS est :

- Vol de cookie d'authentification.
- Porte d'entrée pour les injections CSRF.
- Redirections des utilisateurs vers un site de phishing.
- Exécution d'un malware.
- Attaque sur le système.

V. Les attaques sur les applications Web

4. Cross-Site Request Forgery (CSRF)

- CSRF (Cross-Site Request Forgery) est une attaque qui **usurpe l'identité** de la victime et envoie des commandes non désirées sur un site web.
- L'attaque CSRF est réalisée par la création d'un **lien** contenant du **code malveillant** destiné à être **exécuté par le navigateur de la victime** afin d'interagir avec une **session ouverte** sur un **autre site** à l'insu de l'utilisateur.
- Le serveur ne peut pas contrôler si le client légitime à lui-même générer la requête.

V. Les attaques sur les applications Web

4. Cross-Site Request Forgery (CSRF)

Exemple : soit L'URL suivante de la banque de la victime :

https://banquedelavictime.fr/virement?numcpte=2776abc&montant=**5000**&etat=**1**

- Etant donné que la victime est connecté (login & mot de passe) à sa banque.
- Toute requête provenant de la session du client passe par le serveur de la banque.
- Le pirate envoi cette URL à la victime, et l'oblige d'exécuter cette transaction (transfert le montant **5000** du compte de la victime vers le compte **27766abc**.

V. Les attaques sur les applications Web

5. Autres attaques selon OWASP

1. Injection
2. Cross-Site Scripting (XSS)
3. Violation de gestion d'authentification et de session
4. Référence directe non sécurisée à un objet
5. Falsification de requêtes intersite (CSRF)
6. Mauvaise configuration de sécurité
7. Stockage de données cryptographiques non sécurisé
8. Défaillance dans la restriction des accès à une url
9. Protection insuffisante de la couche transport
10. Redirection et renvois non validés

Evaluation des connaissances

VI. Applications

Question 1 :

- Quel type de logiciel malveillant oblige l'utilisateur à payer pour le supprimer ?
  - A. Trojan horse
  - B. Keylogger
  - C. Adware
  - D. Ransomware

Question 2 :

- Quel type d'attaque est une attaque Smurf ?
  - A. Déni de service distribué (DDoS)
  - B. Déni de service (DoS)
  - C. Escalade de privilèges
  - D. Menace interne malveillante

VI. Applications

Question 3 :

- Vous inspectez le système d'un utilisateur qui s'est plaint de la lenteur de son utilisation d'Internet. Après avoir analysé le système, vous remarquez que l'adresse MAC de la passerelle par défaut dans le cache ARP fait référence à la mauvaise adresse MAC. Quel type d'attaque a eu lieu ?
  - A. Brute force
  - B. DNS poisoning
  - C. Buffer overflow
  - D. ARP poisoning

VI. Applications

Question 4 :

- Vous analysez le trafic Web en transit vers votre serveur Web et vous remarquez que quelqu'un se connecte avec un nom d'utilisateur Bob et un mot de passe « pass » ou 1=1--. Laquelle des affirmations suivantes décrit ce qui se passe ?
  - A. XML injection
  - B. SQL injection attack
  - C. LDAP injection
  - D. Denial of service

VI. Applications

Question 5 :

- Laquelle des propositions suivantes décrit le **mieux** une attaque zero-day ?
  - A. Une attaque qui modifie la date du système de l'ordinateur à 00/00/00
  - B. Une attaque qui modifie l'adresse source du paquet
  - C. Une attaque qui n'a jamais lieu
  - D. Une attaque qui utilise un exploit dont le fournisseur du produit n'a pas encore connaissance

VI. Applications

Question 6 :

- Quel type d'attaque implique que le pirate déconnecte l'une des parties d'une communication et continue la communication tout en se faisant passer pour ce système ?
  - A. Man in the middle
  - B. Denial of service
  - C. SQL injection
  - D. Session hijacking

VI. Applications

Question 7 :

- Quel type d'attaque de mot de passe implique l'utilisation d'un fichier dictionnaire et des modifications des mots dans le fichier dictionnaire ?
  - A. Dictionary attack
  - B. Brute-force attack
  - C. Hybrid attack
  - D. Modification attack

VI. Applications

Question 8 :

- Tom a été invité à télécharger un logiciel d'impôt gratuit pour remplir sa déclaration de revenus cette année. Après avoir téléchargé et installé le logiciel, Tom remarque que son système fonctionne lentement et il reçoit une notification de son logiciel antivirus. Quel type de logiciel malveillant a-t-il installé ?
  - A. Rootkits
  - B. Keylogger
  - C. Vers
  - D. Cheval de troie