17

LA SÉCURITÉ

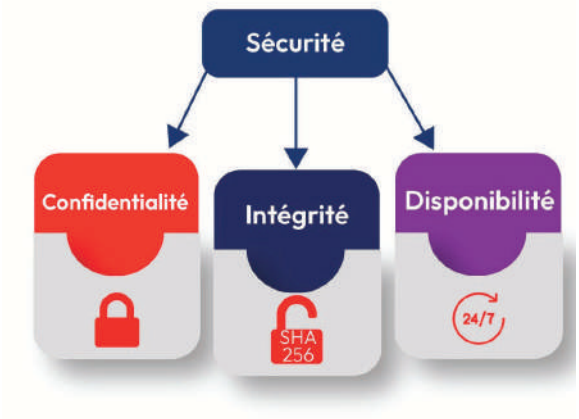
17.1. Concepts de base de la sécurité

17.1.1. Objectifs de la sécurité :

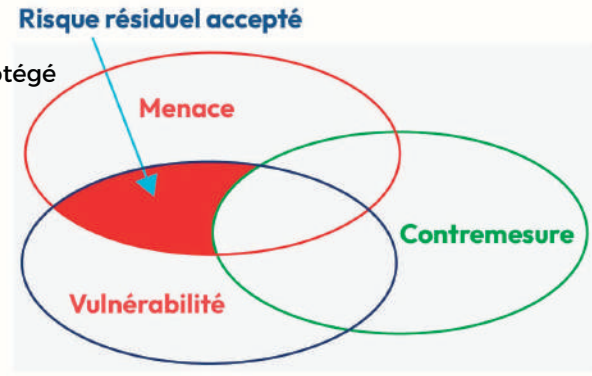
La confidentialité a été définie par l'ISO comme "le fait de s'assurer que les informations ne sont lisibles que par les personnes dont l'accès est autorisé".

L'intégrité des données signifie que les modifications apportées aux données ne sont effectuées que par des personnes/systèmes autorisées.

La disponibilité fait référence à la garantie d'un accès permanent aux données pour toute personne autorisée.



17.1.2. Terminologie de la sécurité :



The asset (L'atout) est quelque chose qui doit être protégé et peut inclure des biens, des personnes et des informations qui ont de la valeur pour l'entreprise.

La menace est un danger qui existe dans l'environnement d'un système informatique indépendamment de celui-ci : Criminel, pirate, employé mécontent, concurrent, etc.

La vulnérabilité est une faiblesse du système informatique qui le rend susceptible à une menace :

- Vulnérabilités système.
- Vulnérabilités des programmes.
- Vulnérabilités des protocoles.
- Vulnérabilités humaines, etc.

L'exploit est un mécanisme conçu pour trouver et exploiter une vulnérabilité dans une application ou un système informatique.

L'attaque informatique est l'exploitation d'une vulnérabilité du système informatique généralement pour faire des dommages.

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée dans le système informatique.

Les contre-mesures sont les méthodes de contrôle mises en œuvre dans un système informatique pour réduire ou éliminer le risque :

- Contre-mesures administratives.
- Contre-mesures physiques.
- Contre-mesures techniques.

Le risque résiduel accepté est le risque subsistant après la mise en œuvre des contre-mesures de sécurité.

17.2. Les menaces et les vulnérabilités :

17.2.1. Acteurs de menaces :

Les acteurs de menaces en cyber sécurité informatique sont des individus ou des groupes qui cherchent à exploiter les vulnérabilités des systèmes informatiques.

Il existe plusieurs types d'acteur de menaces, tels que les pirates informatiques, les groupes de cyber-activistes et les acteurs nationaux, avec des motivations ainsi que des méthodes différentes.

Pour se protéger contre ces menaces, il est important de comprendre les différents acteurs et de mettre en place des stratégies de sécurité efficaces afin de les identifier et les prévenir.

Il est essentiel de maintenir une vigilance constante
et de mettre en place des mécanismes de surveillance pour détecter les intrusions potentielles.

Les pirates :

- **Les pirates à chapeau blanc (White Hat) :** Ce sont des pirates éthiques qui utilisent leurs compétences pour améliorer le système d'information.
- **Les pirates à chapeau gris (Grey White) :** Ce sont des criminels non éthiques qui utilisent leurs compétences pour des raisons malveillantes.
- **Les pirates à chapeau noir (Black Hat) :** Ce sont des pirates non éthiques, qui ont pour but de nuire à d'autres personnes ou organisations.

Les script kiddies (Les pirates néophytes) : Ce sont des pirates qui n'ont pas beaucoup d'expérience et qui exécutent des scripts généralement sans buts lucratifs.

Les testeurs de vulnérabilité : Ce sont généralement des pirates à chapeau gris qui tentent de trouver des vulnérabilités et les signaler aux responsables.

Les hacktivistes : Ce sont des pirates à chapeau gris avec des motivations idéologiques.

Cybercriminels : Ce sont des pirates à chapeau noir qui travaillent pour des organisations de cybercriminalité.

Parrainé par l'État : Ce sont des pirates à chapeau blanc ou à chapeau noir qui ont comme cibles des gouvernements étrangers, des groupes terroristes ou des entreprises.

17.2.2. Outils de sécurité :

OUTILS	RÔLES	EXEMPLES
Craqueurs de mots de passe	La récupération des mots de passe	• John the Ripper • Ophcrack • L0phtCrack • THC Hydra • RainbowCrack • Medusa
Outils de piratage sans fil	Piratage des réseaux sans fil	• Aircrack-ng • Kismet • InSSIDer • KisMAC • Firesheep • NetStumbler
Outils d'analyse et de piratage réseau	Analyse du réseau pour trouver la liste des machines disponibles, les ports ouverts, etc.	• Nmap • SuperScan • Angry IP Scanner • NetScanTools
Outils de création de paquets	Test de la robustesse d'un pare-feu en utilisant des paquets forgés (Spoofés)	• Hping • Scapy • Socat • Yersinia • Netcat • Nping • Nemesis

OUTILS	RÔLES	EXEMPLES
Renifleurs de paquets	Capture et analyse des paquets au sein d'un réseau.	• Wireshark • Tcpdump • Ett ercap • Dsniff • EtherApe • Paros • Fiddler • Ratproxy • SSLstrip
Détecteurs de rootkit	Vérification de l'intégrité des répertoires et des fichiers.	• AIDE • Netfi lter • PF: OpenBSD Packet Filter
Générateurs de bruits (Fuzzers)	Découverte des vulnérabilités.	• Skipfi sh • Wapiti • W3af
Outils d'investigation	Découverte des traces de preuves existant dans une machine.	• Sleuth Kit • Helix • Maltego • Encase
Débogueurs	L'ingénierie inverse sur des fichiers binaires lors de l'écriture d'exploits.	• GDB • WinDbg • IDA Pro • Immunity Debugger

OUTILS	RÔLES	EXEMPLES
Piratage de systèmes d'exploitation	Systèmes d'exploitation conçus pour le piratage.	• Kali Linux • Knoppix • BackBox Linux
Outils de chiffrement	Le chiffrement des données	• VeraCrypt • CipherShed • OpenSSH • OpenSSL • Tor • OpenVPN • Stunnel
Outils d'exploitation des vulnérabilités	Vérification si une machine est vulnérable à une attaque ou non.	• Metasploit • Core Impact • Sqlmap • Social Engineer Toolkit • Netsparker
Analyseurs de vulnérabilité	Identification des ports ouverts, recherche des vulnérabilités, etc.	• Nipper • Secunia PSI • Core Impact • Nessus v6 • SAINT • Open VAS

17.2.3. Types d'attaque :

TYPE D'ATTAQUE	RÔLE
Attaque d'écoute	La capture et la surveillance du trafic
Attaque par modification de données	Modification de données à l'insu de l'expéditeur ou du destinataire
Attaque par usurpation d'adresse IP	Construction d'un paquet IP qui semble provenir d'une adresse valide
Attaque basée sur un mot de passe	Si le pirate a le mot de passe d'un compte d'utilisateur, il peut utiliser tous ses droits pour manipuler le réseau
Attaque par déni de service	Rendre un service ou une machine inaccessible
Attaque de l'Homme-au-Milieu	Positionnement entre la source et la destination pour surveiller la capture et contrôler la communication
Attaque à clé compromise	Accès à une communication sécurisée à l'insu de l'expéditeur et du destinataire
Attaque de reniflement (Sniffer)	Surveillance et capture des échanges de données réseau

17.2.4. Les attaques réseau courantes :

LES ATTAQUES DE RECONNAISSANCE :

Les attaques de reconnaissance sont des attaques utilisées pour la collecte d'informations à propos de la cible :

- Trouver des informations personnelles
- Trouver des adresses IP
- Trouver des ports ouverts
- Trouver le système installé
- Rechercher les applications installées
- Trouver des vulnérabilités

Quelques techniques de reconnaissance :

- Lancement des requêtes d'informations sur une cible (Google, Whois, etc.)
- Balayage du réseau cible pour trouver les adresses IP actives
- Analyse des ports des adresses IP actives (Nmap, SuperScan, Angry IP Scanner et NetScanTools).
- Analyse de vulnérabilités (Nipper, Secuna PSI, Core Impact, Nessus, SAINT, et Open VAS)

LES ATTAQUES PAR ACCÈS :

Les attaques par accès sont des attaques qui permettent d'accéder à la machine vulnérable de la cible.

Attaque par mot de passe :

Dans le cas d'une attaque par mot de passe, la personne malveillante tente de trouver le mot de passe en utilisant quelques techniques :

- Attaque par force brute
- Attaque par dictionnaire
- Attaque hybride

Attaque par usurpation :

Dans le cas d'une attaque par usurpation, la machine du hacker tente de se faire passer pour une autre machine de confiance dans le réseau :

- Usurpation d'adresse IP
- Usurpation d'adresse MAC
- Usurpation d'un service comme DHCP, etc.

Exploitation de confiance :

Dans le cas d'une attaque de confiance, le pirate menace les privilèges non autorisés pour accéder à un système.

Redirection de ports :

Dans le cas d'une attaque par redirection de ports, le hacker utilise un système compromis comme base d'attaques contre d'autres cibles.

Homme-Au-Milieu (Man In The Middle) :

Dans une attaque d'homme au milieu, le pirate se positionne entre deux entités légitimes afin de lire ou de modifier les données qui transitent entre les deux parties.

Attaque de dépassement de tampon :

Dans une attaque de dépassement de tampon, la personne malveillante exploite la mémoire tampon de la cible et la submerge de valeurs inattendues.

L'ingénierie sociale :

L'ingénierie sociale est une attaque qui exploite des failles humaines pour effectuer des actions de piratage.

Quelques techniques d'ingénierie sociale :

- Prétexte
- Hameçonnage (Phishing)
- Courrier indésirable (SPAM)
- Contrepartie (Something for Something)
- Usurpation d'identité (Spoofing)
- Accès non autorisé (Tailgating)
- Espionnage par-dessus l'épaule (Shoulder Surfing)
- Fouille poubelle (Dumpster Diving)

LES ATTAQUES PAR DÉNI DE SERVICE :

Une attaque par déni de service **DOS** (**D**enial **O**f **S**ervice) est une attaque qui consiste à rendre un service ou une machine inaccessible.

Deux types d'attaques DOS :

- **Attaque DOS par saturation :** l'acteur de menaces envoie une très grande quantité de trafic que la cible ne peut pas gérer.
- **Attaque DOS par exploitation de vulnérabilités :** l'acteur de menaces formate les paquets d'une manière malveillante que la cible ne peut pas traiter.

Une attaque DOS distribué est une attaque qui utilise plusieurs connexions (Zombies) pour rendre une machine ou un service distant inaccessible.

17.2.5. Programmes malveillants :

LES VIRUS :

Définition :

Un virus est tout programme informatique capable d'**infecter** un autre programme informatique en le modifiant afin qu'il puisse **se reproduire**.

Il nécessite une action humaine pour se propager et infecter d'autres ordinateurs.

Types de virus :

Les virus du secteur de démarrage : Il attaque le secteur de démarrage, la table de partition de fichiers ou le système de fichiers.

Les virus du micrologiciel : Il attaque le micrologiciel du périphérique.

Les virus contenus dans les macros : Il utilise la fonction de macro de MS Office ou d'autres applications.

Les virus de programmes : Il s'insère dans un autre programme exécutable.

Les virus de script : Il attaque l'interpréteur du système d'exploitation utilisé pour exécuter des scripts (PowerShell, Bash, etc.).

LES CHEVAUX DE TROIE :

Définition :

Un cheval de Troie est un programme qui crée une **porte dérobée** dans une machine afin d'entrer et de recevoir des informations sensibles.

Programme « Cheval de Troie » :

Il est composé de deux versions :

Version serveur : C'est la version qui s'installe dans la machine de la cible pour répondre aux requêtes du pirate.

Version client : C'est le programme qui s'installe dans la machine du pirate pour envoyer des requêtes à la cible.

Types de cheval de Troie :

Un cheval de Troie peut mener plusieurs actions malveillantes visant la cible :

TYPE DE CHEVAL DE TROIE	DESCRIPTION
Accès distant	Il permet un accès distant non autorisé.
Envoi de données	Il envoie des données sensibles à l'acteur de menace.
Destructeur	Il endommage ou supprime des documents de la cible.
Proxy	Il utilise la cible comme rebond pour att aquer d'autres victimes.
FTP	Il transfère des fichiers non autorisés à l'acteur de menace.
Désactivateur de logiciel de sécurité	Il désactive l'antivirus ou le pare-feu
Déni de service	Il ralentit ou arrête un service ou une machine cible
Enregistreur de frappes	Il enregistre les frappes de touches et envoie le résultat à l'acteur de menace

AUTRES LOGICIELS MALVEILLANTS :

LOGICIEL MALVEILLANT	DESCRIPTION
Logiciel publicitaire	Il affiche la publicité non sollicitée lors de son utilisation : • Partie incitant l'utilisateur à l'installer • Partie gérant l'affichage de la publicité
Logiciel de rançon (Ransomware)	L'acteur de menace restreint l'accès au système informatique et exige le paiement d'une rançon pour enlever la restriction
Rootkit	L'acteur de menace restreint l'accès au système informatique et exige le paiement d'une rançon pour enlever la restriction
Logiciel espion	Un logiciel espion recueille des informations sur les habitudes, l'historique de navigation, le numéro de carte de crédit, les mots de passe, etc.
Ver	Il peut s'autoreproduire et se propager en utilisant des mécanismes réseau sans l'action de l'utilisateur.

17.3. Menaces et vulnérabilités :

17.3.1. Menaces et vulnérabilités liées au protocole IP :

ATTAQUES DE RECONNAISSANCE ICMP :

Les attaques de reconnaissance ICMP sont une forme d'attaque utilisée pour recueillir des informations sur un système ou un réseau cible en utilisant le protocole ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol).

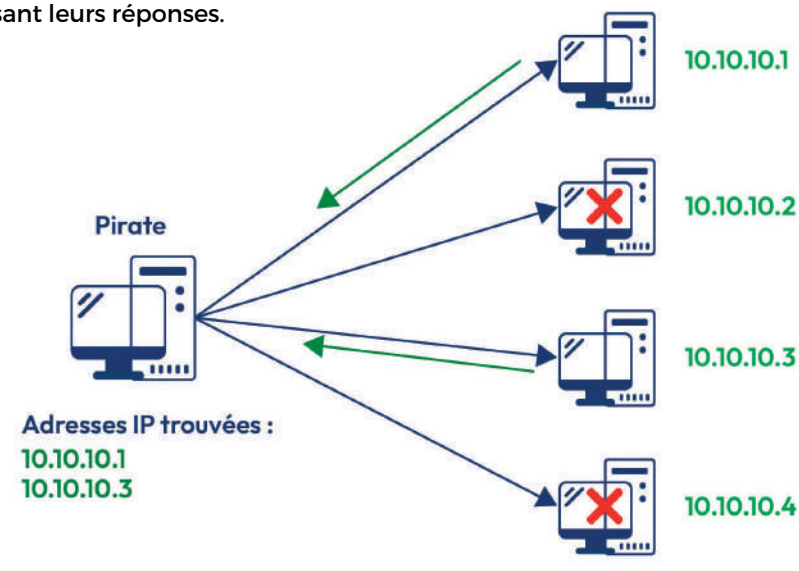
Ces attaques consistent à envoyer des paquets ICMP spécifiques à la cible, dans le but de récolter des informations sur les systèmes et les réseaux cibles, comme les adresses IP, les noms d'hôtes et les configurations de sécurité.

Les informations recueillies peuvent ensuite être utilisées pour planifier et lancer des attaques plus avancées.

Les attaques de reconnaissance ICMP peuvent être détectées et bloquées en utilisant des outils de sécurité réseau tels que les pare-feux et les systèmes de détection d'intrusion.

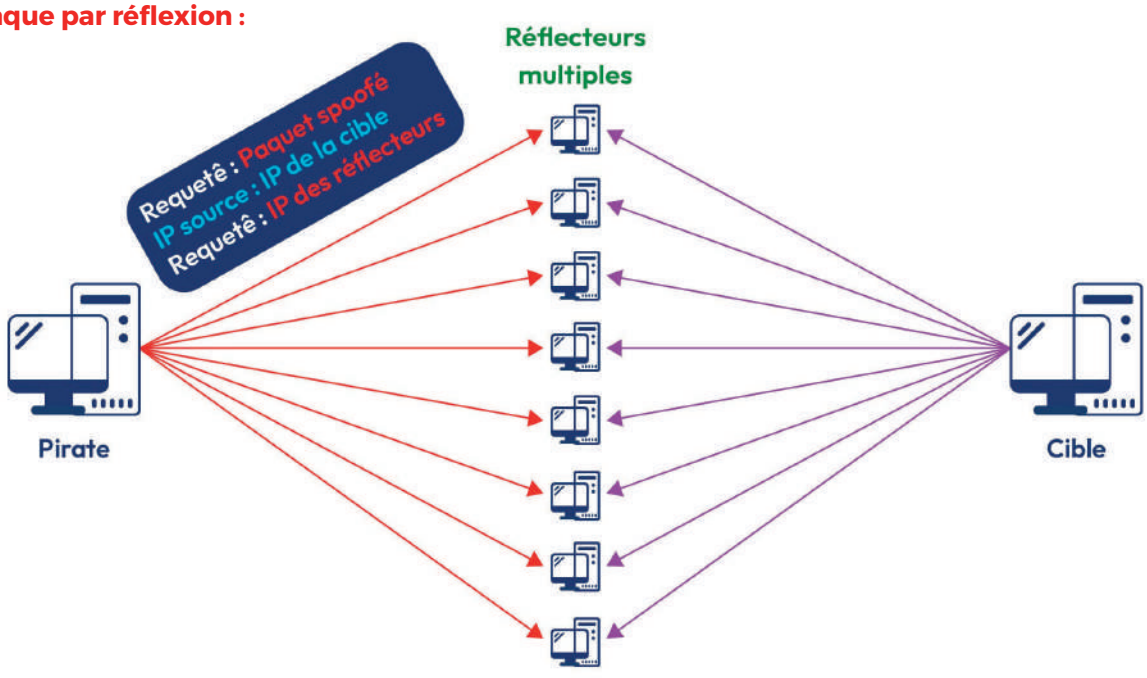
Il est important de prendre des mesures pour limiter l'utilisation de ICMP dans votre réseau, afin de minimiser les risques de reconnaissance.

Les acteurs de menaces utilisent des paquets de demandes d'écho ICMP pour découvrir les hôtes sur un réseau, en analysant leurs réponses.



ATTAQUES DE RÉFLEXION ET D'AMPLIFICATION:

Attaque par réflexion :



- L'acteur de menace usurpe l'adresse IP d'une cible.
- L'acteur de menace envoie le paquet de demandes d'écho ICMP usurpé à des machines appelées réflecteurs.
- Les réflecteurs répondent à la requête par un paquet de réponses d'écho ICMP en utilisant l'adresse de la cible.

Attaque par amplification :

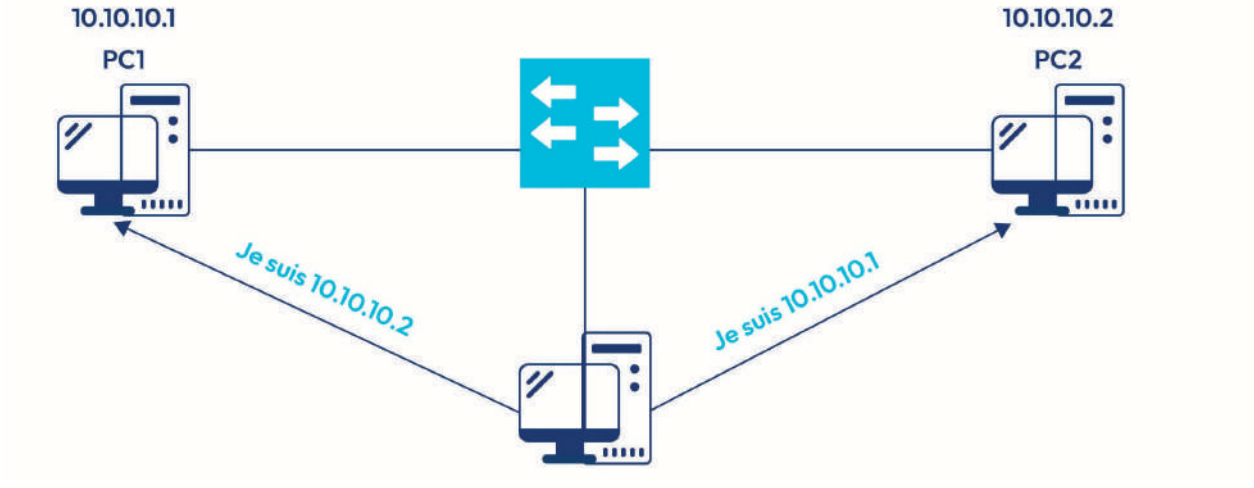
Une attaque par amplification est un exemple d'attaque par réflexion.

La seule spécification est que les réponses des réflecteurs sont considérablement plus grandes que la demande d'origine et amplifient considérablement la taille des données et la bande passante utilisée → Ce qui provoque un déni de service.

> Il existe d'autres formes d'attaques d'amplification et de réflexion basées sur DNS et NTP.

ATTAQUES PAR USURPATION D'ADRESSES :

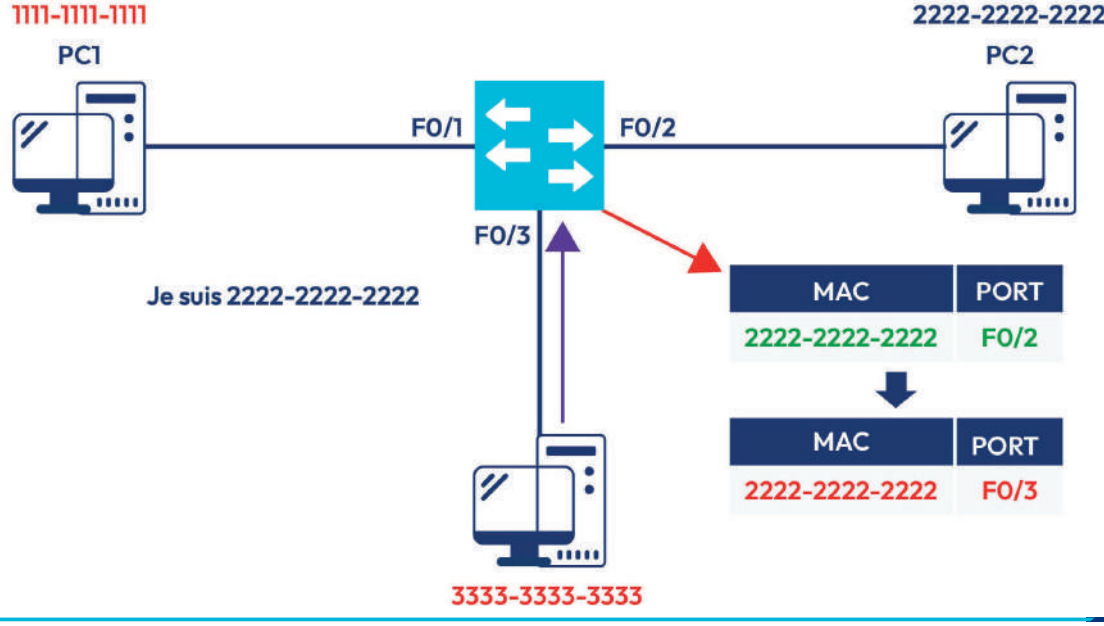
Usurpation d'adresse IP :



L'acteur de menace crée des paquets contenant de fausses informations d'adresse IP source pour :

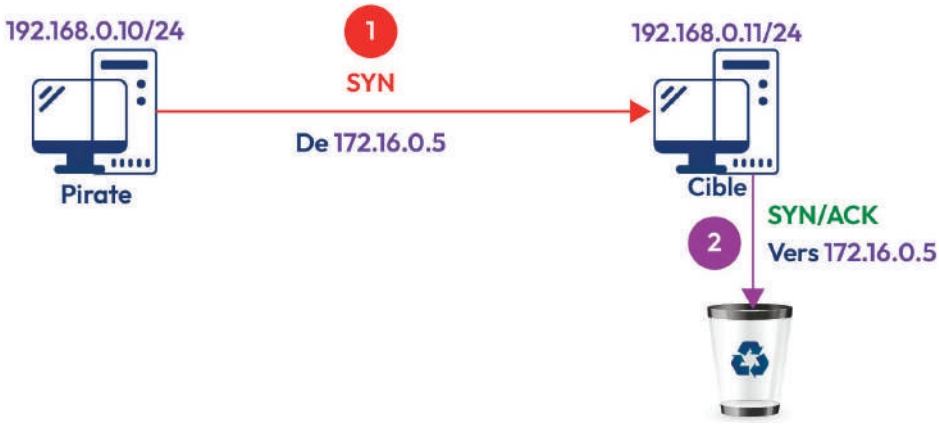
- Masquer l'identité de l'expéditeur.
- Ou se faire passer pour un autre utilisateur légitime.

Usurpation d'adresse MAC :

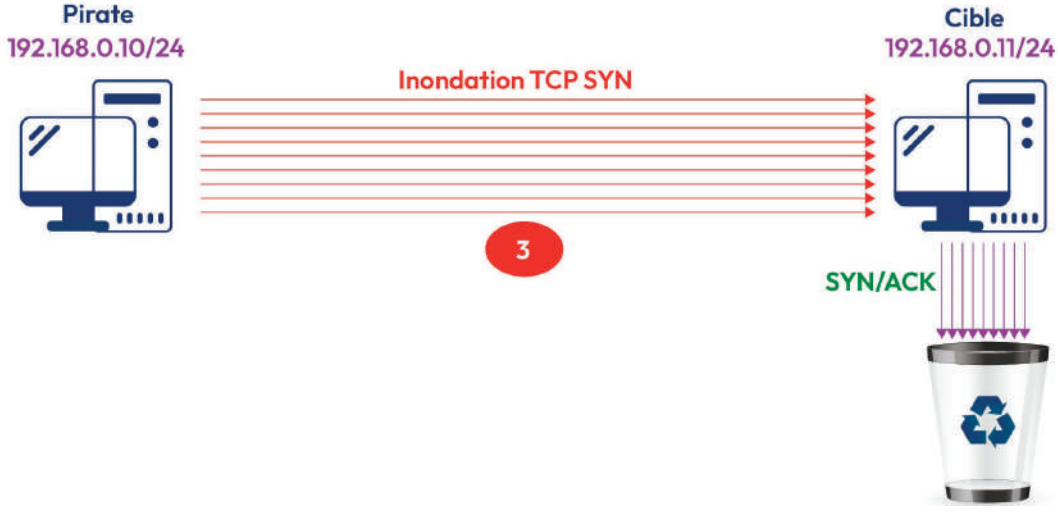


17.3.2. Menaces et vulnérabilités liées aux protocoles TCP et UDP :

INONDATION TCP SYN :

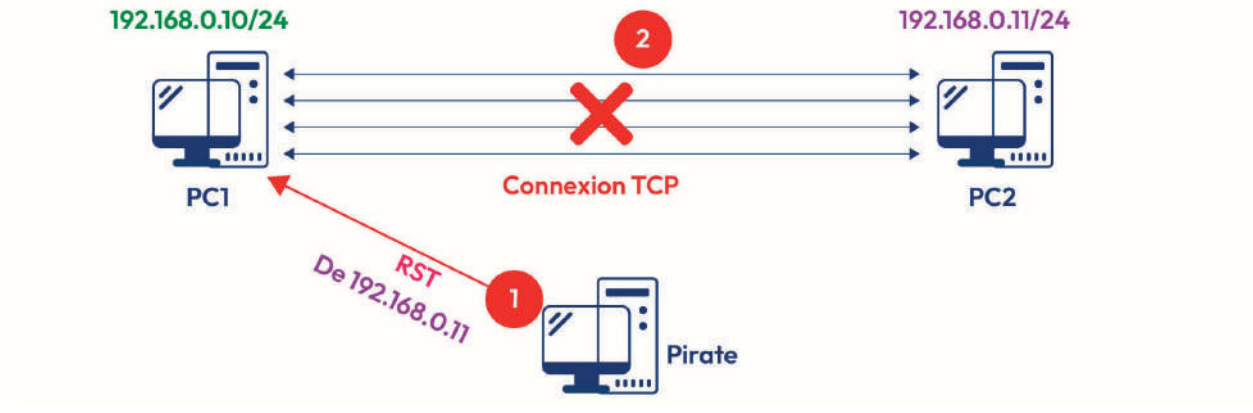


- L'acteur de menace envoie une demande de connexion à la cible en utilisant comme adresse IP source une adresse IP inexistante.
- La cible répond par un paquet SYN/ACK à l'adresse IP inexistante.
- L'acteur de menace n'envoie pas de paquet ACK → La connexion TCP est en file d'attente (Session TCP semi-ouverte).



- Le pirate répète l'opération plusieurs fois afin de saturer la machine cible.
- La machine cible ne répond plus aux requêtes TCP normales.

ATTAQUES DE RÉINITIALISATION TCP :



- L'acteur de menace envoie un paquet RST usurpé en utilisant l'adresse de PC2 comme adresse source.
- PC1 arrête la connexion TCP avec PC2.

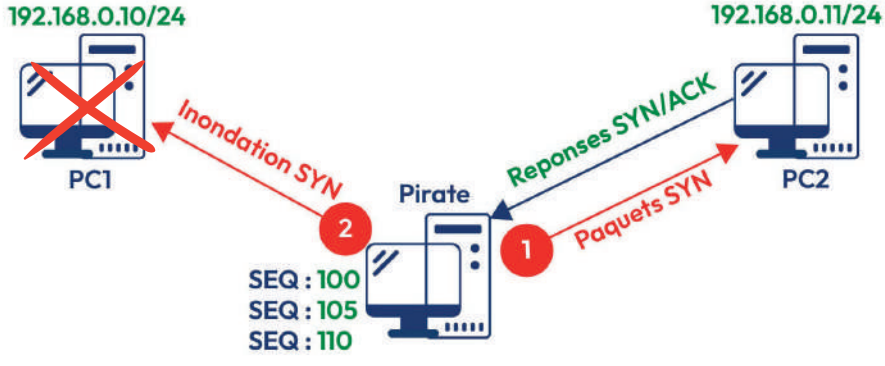
DÉTOURNEMENT D'UNE SESSION TCP :

Étape 1 : Prédiction des numéros de séquence

- L'acteur de menace envoie des paquets SYN en utilisant son adresse IP.
- L'acteur de menace reçoit des réponses SYN/ACK contenant des numéros de séquences (100, 105,110).
- L'acteur de menace prévoit que le numéro de séquence suivant est SEQ = 115.

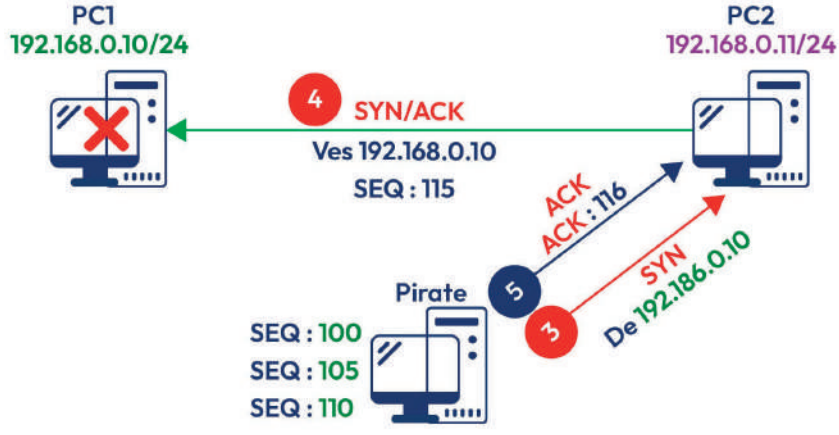
Étape 2 : Inondation de PC1 par des paquets SYN (Attaque DoS)

- L'acteur de menace mène une attaque d'inondation TCP SYN sur PC1 afin de la rendre hors service (pour empêcher qu'elle réponde par un paquet RST).

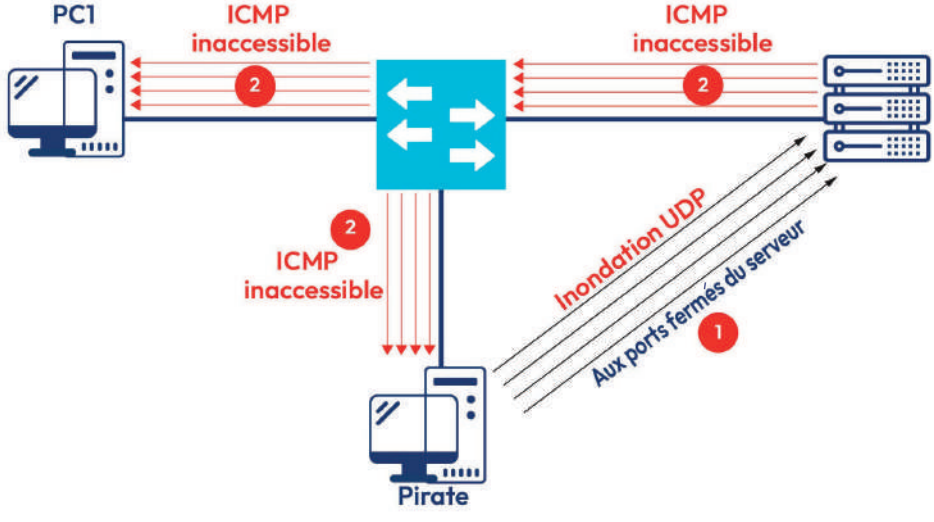


Étape 3 : Usurpation d'identité de la machine PC1

- L'acteur de menace envoie à PC2 un paquet SYN usurpé en utilisant l'adresse de PC1.
- PC2 répond par un SYN/ACK à PC1 avec le numéro de séquence prévu (SEQ = **115**).
- Le pirate construit un paquet ACK avec un numéro ACK = SEQ + 1 = 116 et l'envoie à PC2.
- La session TCP est détournée.



ATTAQUE PAR INONDATION UDP :

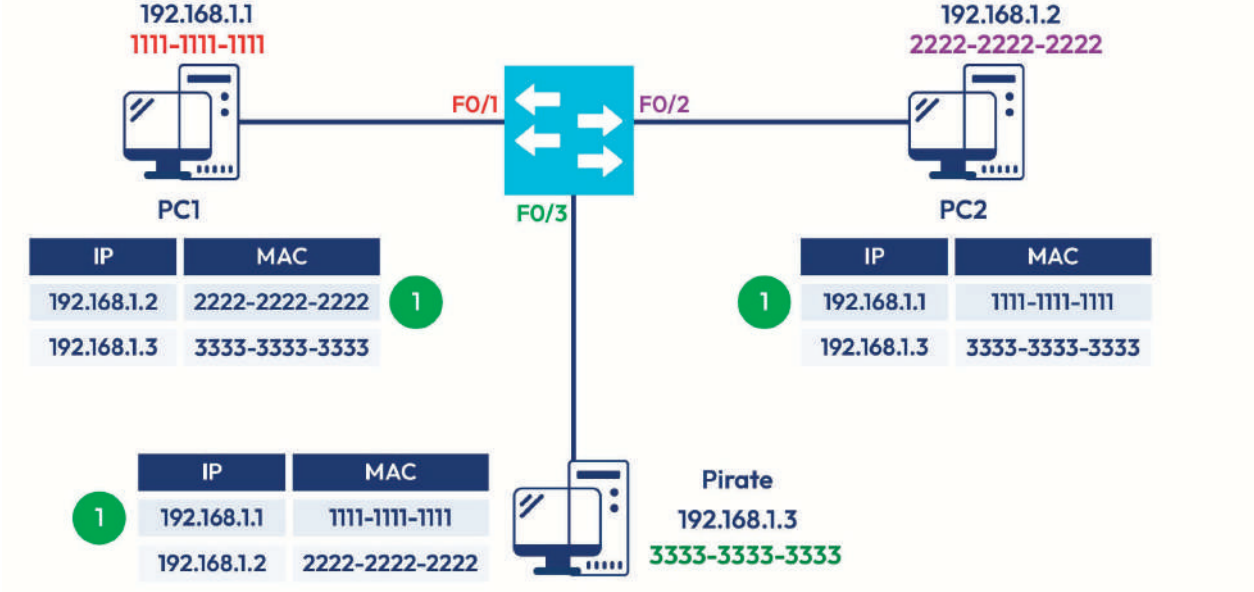


- L'acteur de menace envoie un très grand nombre de paquets UDP aux ports fermés du serveur.
- Le serveur répond par un très grand nombre de paquets « **ICMP inaccessible**»
- Le réseau est saturé → un déni de service.

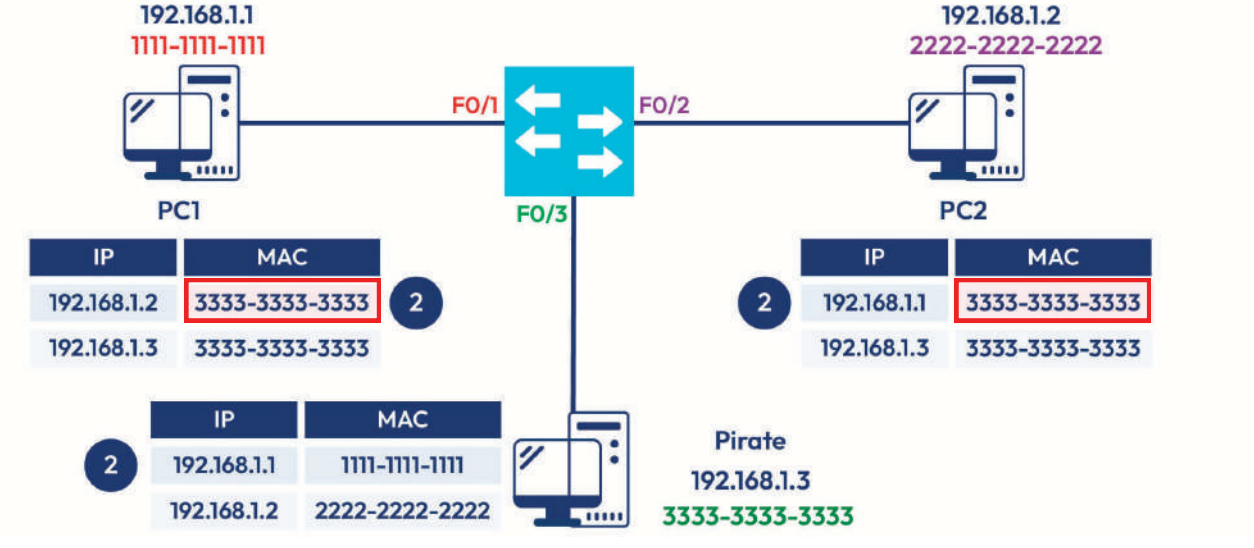
17.3.3. Menaces et vulnérabilités liées aux services réseau :

EMPOISONNEMENT DU CACHE ARP :

Dans le cas normal, le cache ARP contient les informations sur les autres machines du réseau (Adresse IP/ Adresse MAC correspondante).



L'acteur de menace envoie des paquets ARP gratuits (**Gratuitous ARP**) aux ordinateurs pour modifier le cache ARP en associant son adresse MAC aux autres adresses IP.



ATTAQUES DNS :

Attaques résolveur ouvert DNS :

Un résolveur ouvert DNS est un serveur DNS public qui répond aux requêtes des clients en dehors de son domaine administratif.

Attaque d'empoisonnement du cache DNS :

L'acteur de menace envoie des informations falsifiées vers un résolveur DNS pour rediriger les utilisateurs de sites légitimes vers des sites malveillants.

Attaque par amplification et réflexion du DNS :

L' acteur de menace envoie plusieurs requêtes DNS en utilisant une adresse IP d'un hôte cible.

Attaque sur l'utilisation des ressources du DNS :

Elle consiste à consommer toutes les ressources du résolveur DNS ouvert.

Attaques furtives DNS :

Ce sont des attaques utilisées par les acteurs de menace pour cacher leurs identités.

Flux rapide DNS :

C'est une technique qui consiste à associer plusieurs adresses IP et plusieurs noms de domaine, mais également à changer rapidement ces adresses IP (les enregistrements A sont changés en permanence).

L'acteur de menace utilise cette technique pour masquer son site de phishing et de diffusion de logiciels malveillants.

Double flux rapide DNS :

L'acteur de menace modifie rapidement, en plus des enregistrements A, l'adresse IP du serveur de noms faisant autorité (les enregistrements A et NS sont changés en permanence).

Algorithmes de génération de domaine :

Les acteurs de menace utilisent ces algorithmes pour générer aléatoirement des noms de domaine.

Attaques d'observation de domaine DNS :

Les acteurs de menace utilisent ces attaques pour la collecte des informations d'identification du compte de domaine afin de créer silencieusement plusieurs sous-domaines à utiliser pendant les attaques.

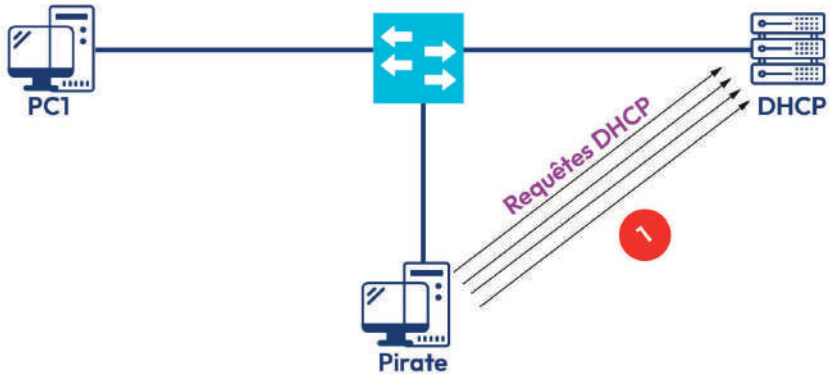
Attaques par tunnellisation DNS :

C'est une technique qui consiste à placer le trafic non DNS dans le trafic DNS.

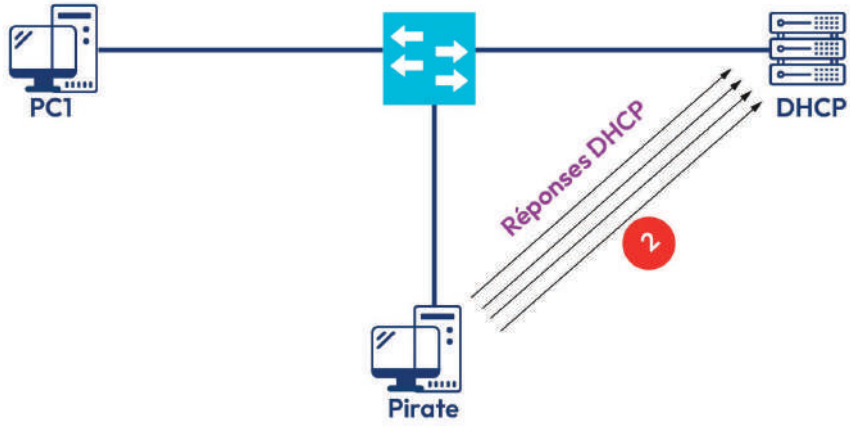
ATTAQUES DHCP :

Attaques par épuisement de ressources DHCP :

L'acteur de menace envoie plusieurs requêtes DHCP au serveur DHCP.



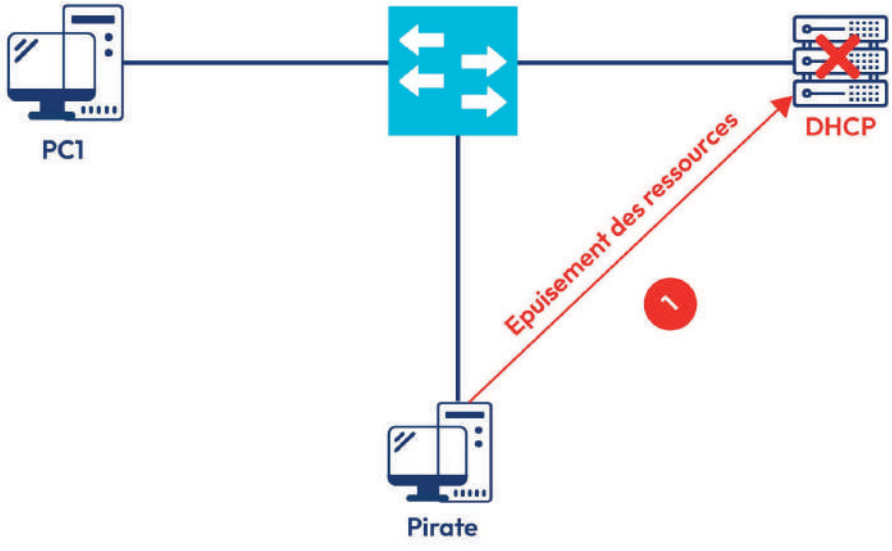
Le serveur DHCP répond aux requêtes ➔ toutes les ressources sont épuisées.



Le serveur DHCP se trouve dans l'incapacité de répondre aux requêtes DHCP normales.

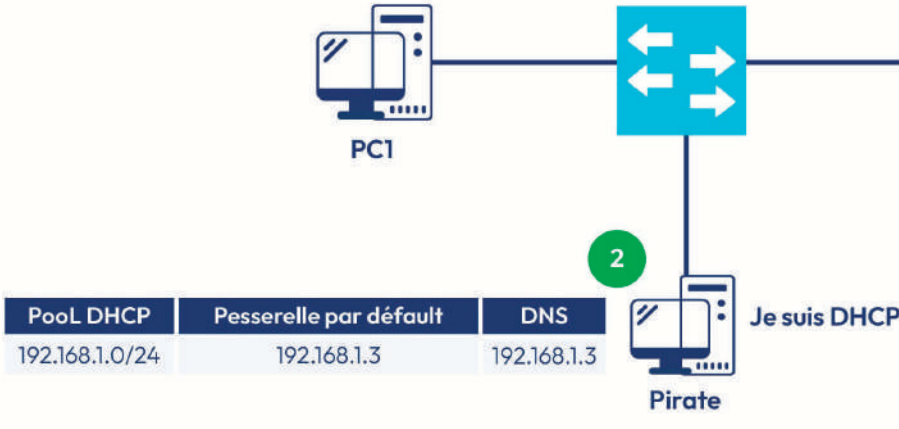
Attaques par usurpation DHCP :

L'acteur de menace peut utiliser une attaque par épuisement de ressources.

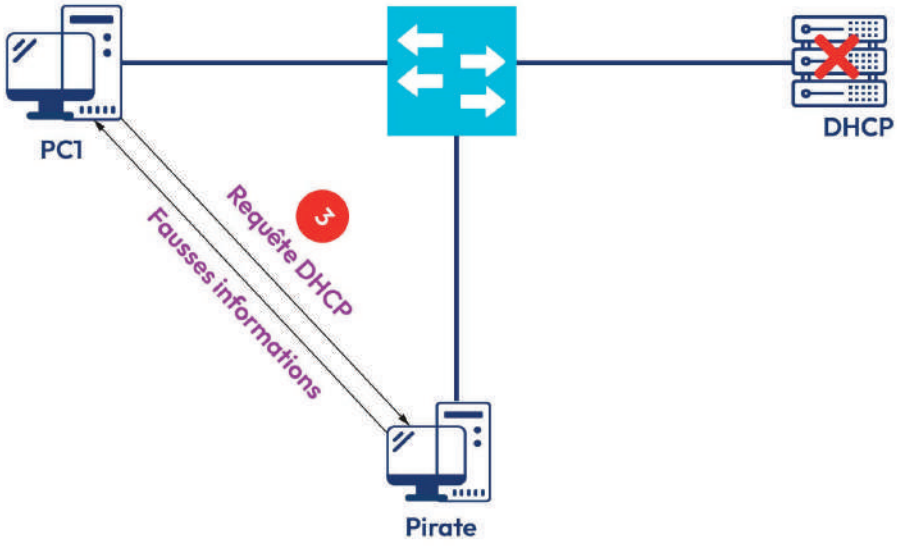


L'acteur de menace configure sa machine comme serveur DHCP en utilisant de fausses informations :

- Adresses IP attribuées erronées.
- Passerelle par défaut erronée.
- Adresses des serveurs DNS erronées.

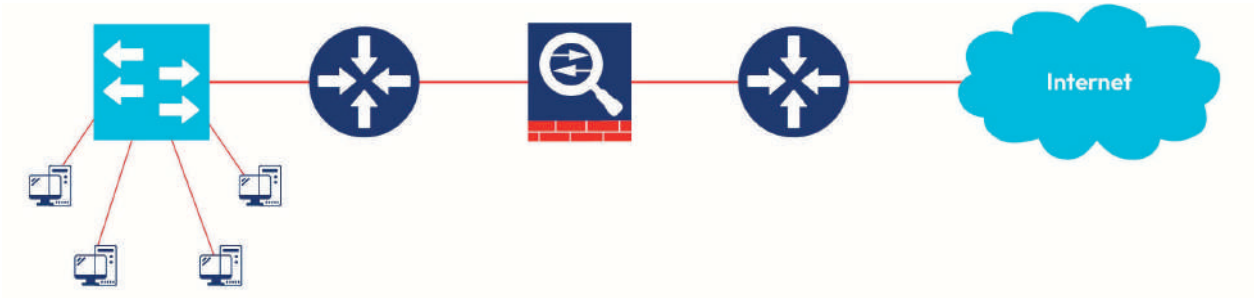


L'acteur de menace envoie les fausses informations configurées aux clients demandant les services DHCP.



17.4. Bonnes pratiques pour la sécurité du réseau :

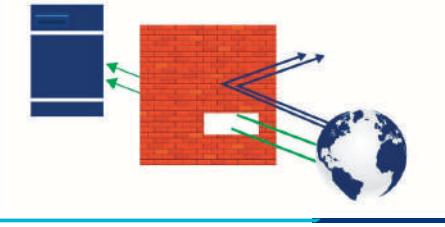
17.4.1. Défense en profondeur :



On utilise un pare-feu ou d'autres dispositifs de sécurité pour sécuriser le réseau interne de l'entreprise.

Pare-feu :

C'est un système qui impose une politique de contrôle d'accès entre les différents réseaux de l'entreprise : il s'agit d'un filtre de trafic réseau.

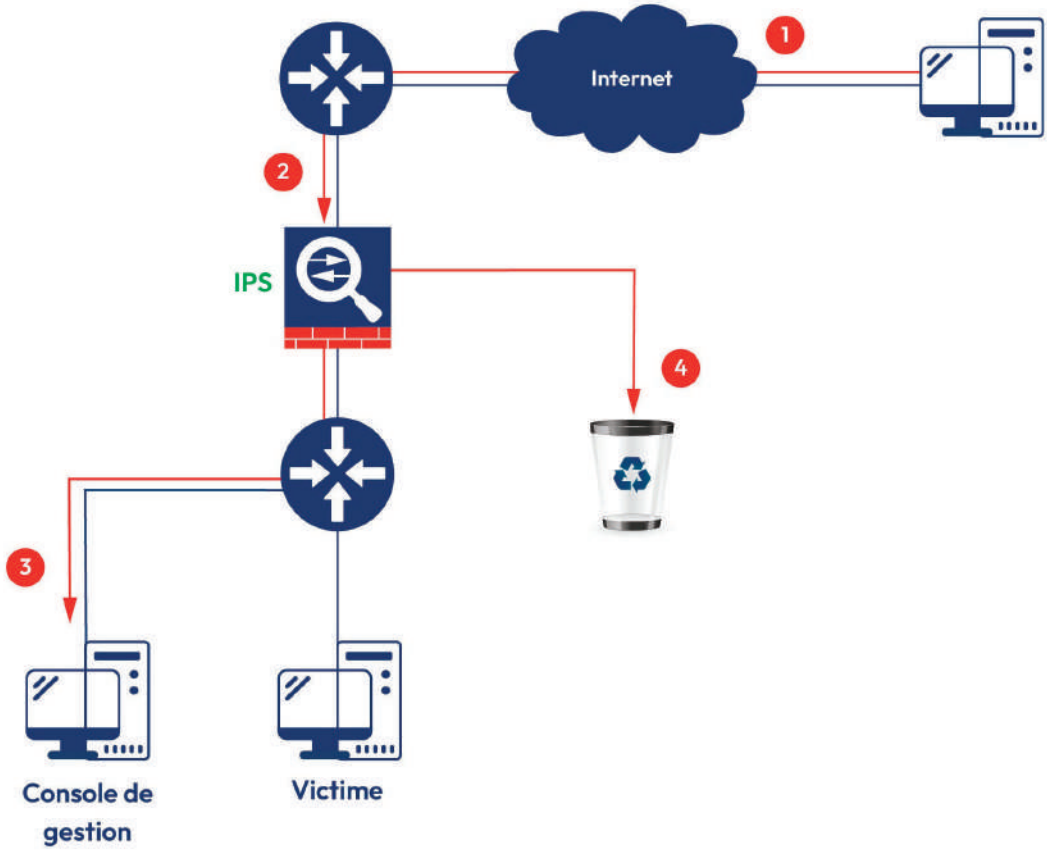


17.4.2. IPS (Intrusion Prevention System) :

Un IPS est un système qui permet la prévention des intrusions aux réseaux.

D'ailleurs, il existe sous différentes formes :

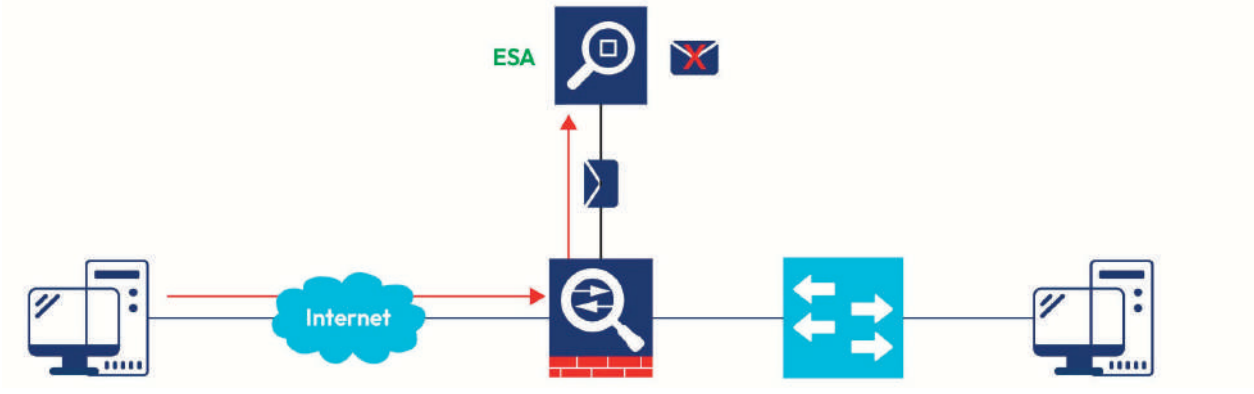
- Un routeur configuré avec le logiciel Cisco IOS IPS.
- Un dispositif spécialement dédié pour les fonctionnalités IPS.
- Un module installé dans le pare-feu ASA, dans un commutateur ou un routeur.



17.4.3. Équipements de sécurité de contenu :

APPLIANCE DE SÉCURITÉ DE MESSAGERIE CISCO (ESA)

ESA (Cisco **E**mail **S**ecurity **A**ppliance) est un appareil spécialement conçu pour surveiller le protocole de transfert de courrier simple SMTP.

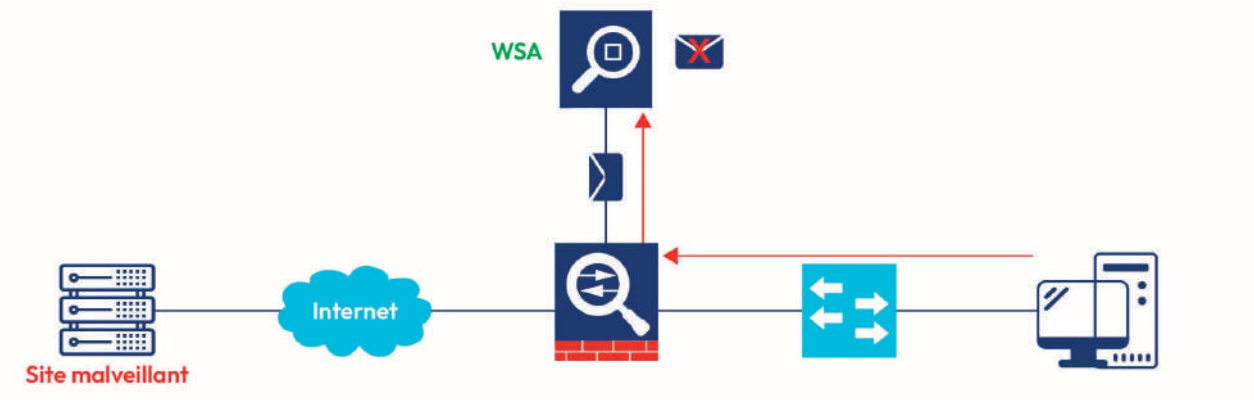


APPLIANCE DE SÉCURITÉ WEB CISCO (WSA)

WSA est une technologie contre les menaces du Web.

Elle combine :

- Une protection contre les logiciels malveillants.
- La visibilité et le contrôle des applications.
- Les contrôles de politique d'utilisation.
- Les rapports.



17.5. La cryptographie :

Les 4 éléments de communication sécurisée :

- Intégrité des données.
- Authentification d'origine.
- Confidentialité des données.

17.5.1. L'intégrité des données

L'intégrité est un processus qui consiste à assurer que si les données sont modifiées, cette modification sera détectée.

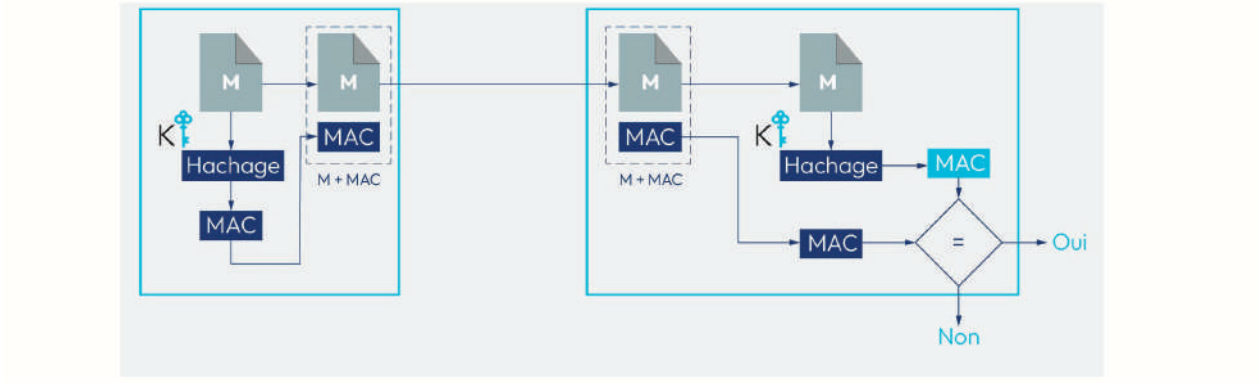
Les fonctions de hachage sont des fonctions qui permettent d'assurer l'intégrité d'un message ou d'un document.

Exemples :

ALGORITHME DE HACHAGE	TAILLE DE L'EMPREINTE
MD5	128
SHA-1	160
SHA-224	224
SHA-256	256
SHA-384	384
SHA-512	512

17.5.2. Authentification d'origine :

L'authentification d'origine est utilisée pour vérifier la source d'un message en utilisant une clé secrète en plus des fonctions de hachage (**HMAC** : **H**ash **M**essage **A**uthentication **C**ode).



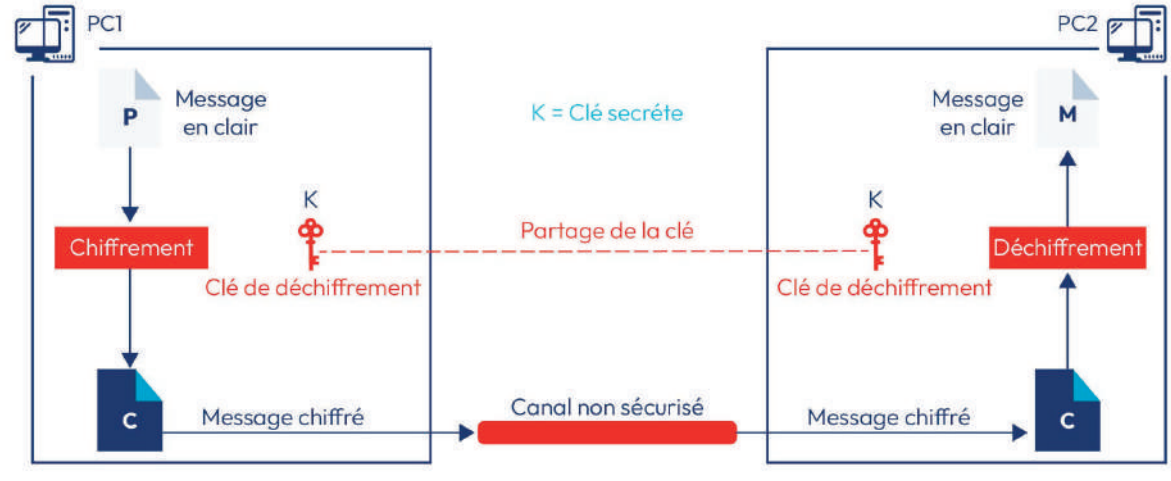
17.5.3. Confidentialité des données :

La confidentialité des données est assurée par le chiffrement.

D'ailleurs, il existe deux types de chiffrements :

- **Chiffrement symétrique :** Clé de chiffrement = clé de déchiffrement
- **Chiffrement asymétrique :** Clé de chiffrement ≠ clé de déchiffrement

LE CHIFFREMENT SYMÉTRIQUE :



Avantages :

- Le chiffrement symétrique assure **la confidentialité des données.**
- Le chiffrement symétrique est **très rapide,** car il se base sur des opérations logiques très faciles à exécuter par un processeur (XOR,AND,OR,NOR, ...).

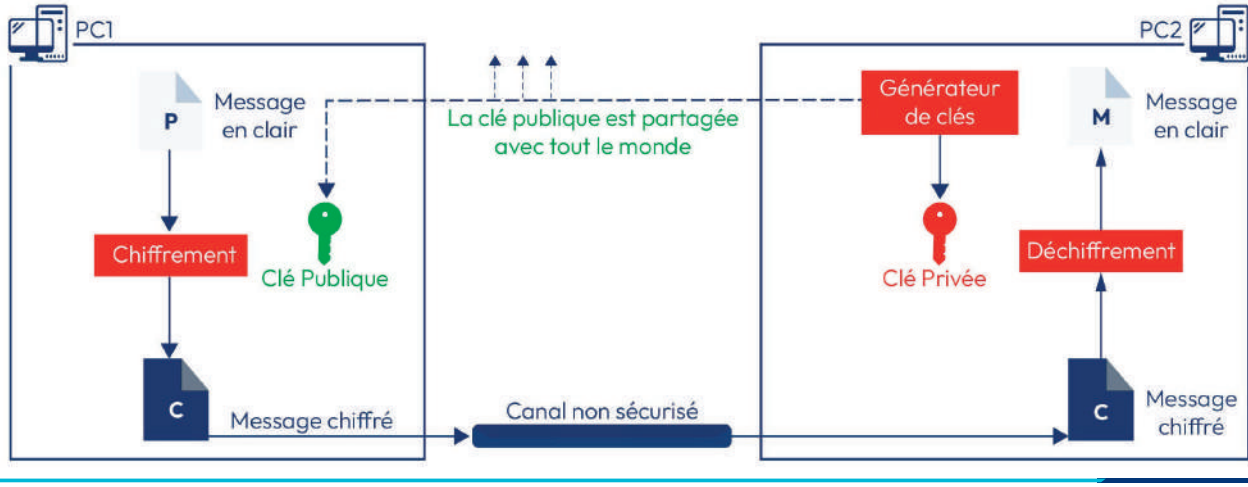
Inconvénients :

- Le chiffrement symétrique a un problème dans **le partage de la clé secrète** (la source et la destination doivent toutes les deux posséder la même clé).
- La **multiplicité de clés secrètes** : pour n périphériques, on doit avoir n*(n-1)/2.

Exemples d'algorithmes de chiffrement symétrique :

ALGORITHMES	DESCRIPTION
DES	La taille de clé secrète (56 bits), la taille du bloc (64 bits)
3DES	La taille de clé secrète (112 bits), la taille du bloc (64 bits)
AES	La taille de clé secrète (128-192-256 bits), la taille du bloc (128 bits)
SEAL	La taille de la clé secrète (160 bits)
RC	RC4 est un algorithme de chiffrement par flux développé par Ron Rivest.

LE CHIFFREMENT ASYMÉTRIQUE :



Avantages :

- Le chiffrement asymétrique assure **la confidentialité des données.**
- Le chiffrement asymétrique n'a **pas de problème de partage des clés** : il utilise la méthode de **D**iffie-**H**ellman **DH** pour le partage du secret.
- Le chiffrement asymétrique n'a **pas de problème de multiplicité des clés**.

Inconvénient :

- Le chiffrement asymétrique est trop lent : il utilise des opérations compliquées pour le chiffrement et le déchiffrement telles que la puissance, etc.

Exemples d'algorithmes de chiffrement asymétrique :

ALGORITHMES DE CHIFFREMENT ASYMÉTRIQUE	LONGUEUR DE CLÉ
DH : Diffie-**H**ellman	512, 1024, 2048, 3072, 4096
DSS : **D**igital **S**ignature **S**tandard DSA : **D**igital **S**ignature **A**lgorithm	De 512 à 1024
RSA : **R**ivest, **S**hamir et **A**dleman	De 512 à 2048
ElGamal	De 512 à 1024
Techniques de courbe elliptique	160

> L'algorithme de **D**iffie-**H**ellman DH permet d'échanger un secret entre deux entités d'une manière sécurisé (Le secret n'est pas véritablement partagé)

La sécurité informatique est un **enjeu crucial** pour protéger les systèmes et les informations des organisations contre les menaces cybernétiques.

Il est important de mettre en place des stratégies de sécurité efficaces pour identifier et prévenir les menaces, telles que les pare-feux, les systèmes de détection d'intrusion, les politiques de sécurité strictes et la formation des employés sur les meilleures pratiques de sécurité.

Il est également important de maintenir une vigilance constante afin de détecter les intrusions potentielles et de mettre en place des mécanismes de surveillance pour y faire face.

La sécurité informatique est un processus continu qui nécessite une attention constante pour protéger les systèmes et les informations contre les menaces en constante évolution.