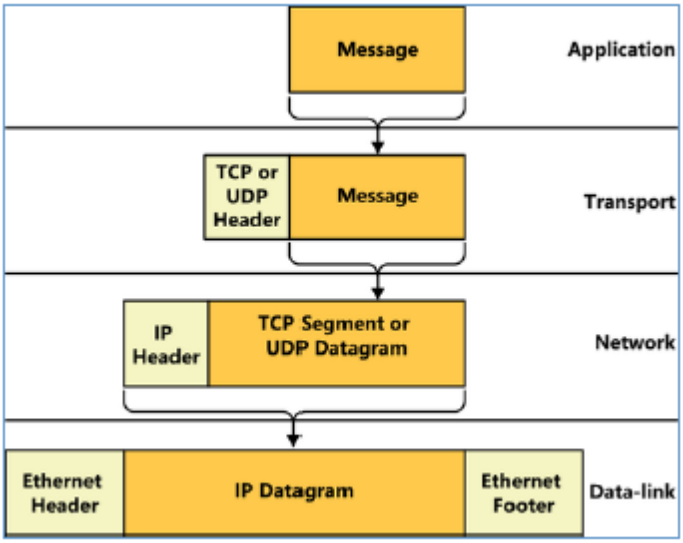
Sécurité Informatique

Chapitre 2 A : Les attaques réseau

1. Introduction générale :

Les vulnérabilités et les attaques possibles sur les réseaux informatiques sont si variées qu'il est illusoire de vouloir les décrire de manière exhaustive, nous allons néanmoins tenter de définir les bases et de donner un bon aperçu de ces attaques afin de rendre plus facile la



compréhension des nouvelles variantes qui apparaissent chaque jour.

1.1. Rappel sur les réseaux

Fig.1 le principe d'encapsulation

1.1.1. les protocoles de transport : TCP et UDP

- les deux protocoles utilisent des **ports source** et **destination** ➔ pour différencier des paquets échanges différentes applications.
- TCP : mode avec connexion :
  - Une connexion doit être établie
    - **SYN :** « Bit SYN=1 , Bit ACK = 0»
    - **SYN + ACK:** « Bit SYN=1 , Bit ACK =1 »
    - **ACK** « Bit SYN=0 , Bit ACK = 1 »
  - Les données sont comptées : **Numéro de séquence.**
  - Les données sont vérifiées et acquittées : **Numéro d'acquittement**.
  - UDP : mode sans connexion

Port source : 80					**Port destination** : 5419				
Numéro de séquence : on commence par un numéro aléatoire = **ISN**									
Numéro d'acquittement = ex : 40013, signifier j'ai bien reçu le paquet 40012 ➔ j'attend le paquet N 40013									
Taille	Réservé	...	Bit ACK	Bit SYN	Bit RST	Bit FIN	.....	.....	.....
.....					.....				
.....						.....			
Message									

Fig2. Segment TCP

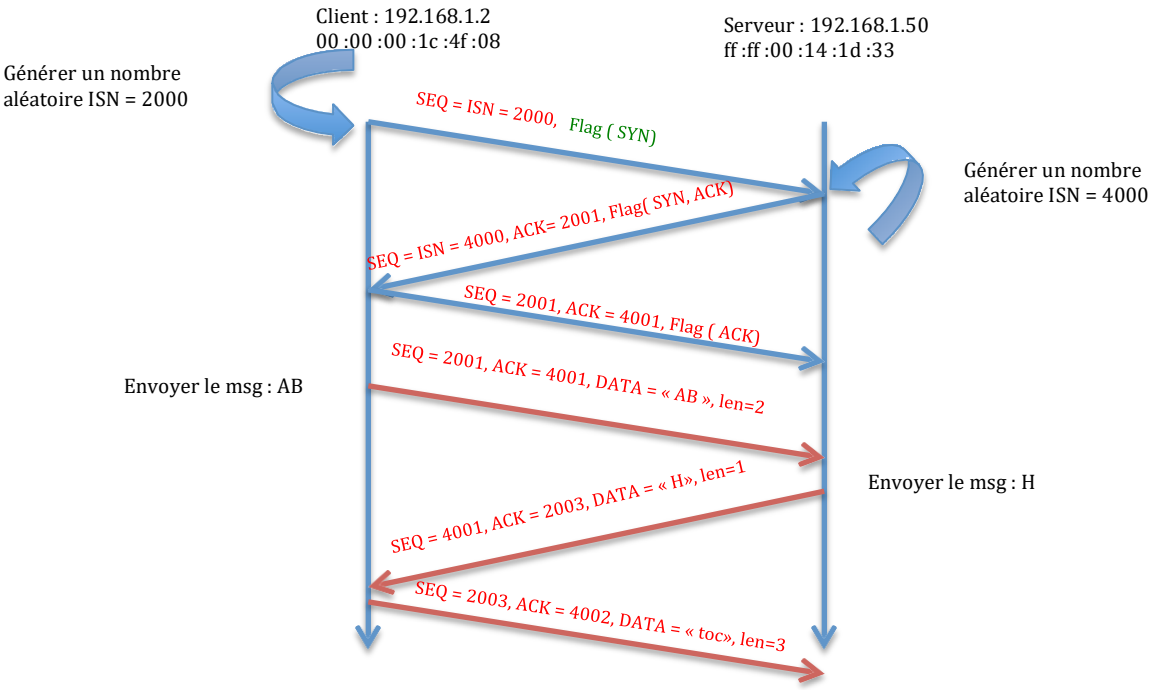


Fig3. Etablissement d'une connexion TCP (en bleu)

1.1.2. Le protocole IP :

...	...	...	...
@IP source		@IP destination	
Segment TCP (voir la figure 2)			

Fig4. Paquet IP

1.1.3. Le protocole Ethernet :

@MAC source	@MAC destination
Paquet IP (voir la figure 4)	

Fig.5 trame Ethernet

1.1.4. **Résumé** : Ethernet + IP + TCP:

@MAC source :00 :00 :00 :1c :4f :08					**@MAC destination** ff :ff :00 :14 :1d :33				
@IP source : 192.168.1.2					**@IP destination : 192.168.1.50**				
Port source : 80					**Port destination** : 5419				
Numéro de séquence : 2003									
Numéro d'acquittement : 4002									
Taille	Réservé	...	ACK=1	SYN=0	RST=0	FIN =0	.....	.....	.....
.....					.....				
.....						.....			
Message = TOC									

Fig6. Le message TOC après l'encapsulation de touts les protocoles

1.1.5. Le protocole ARP : (couche internet) à la place de IP

Lorsqu'une source souhaite envoyer un paquet à une adresse IPv4, elle doit connaître l'adresse MAC correspondante.

Pour cela :

- la machine source (Client : 192.168.1.2 _ 00 :00 :00 :1c :4f :08) va émettre une trame dite ***requête ARP*** **« who has 192.168.1.50 ? »** à tout les machine (ou le passerelle).

- Une seule machine (Serveur 192.168.1.50) répondra avec une ***réponse ARP*** **« 192.168.1.50 is at ff :ff :00 :14 :1d :33 »**

@MAC source :00 :00 :00 :1c :4f :08	**@MAC destination** ff :ff :ff :ff :ff :ff :ff / .. : .. : .. : .. : .. : .. **(diffusion sur tout les réseau / ou l'adresse Mac du passerelle)**
Sender IP: 192.168.1.2	**Target IP: 192.168.1.50**
Sender MAC : 00 :00 :00 :1c :4f :08	**Target MAC**: 00 :00 :00 :00 :00 :00 (POUR DIRE QUE JE CONNAIS PAS L'ADRESSE MAC)

Fig.7. Requête ARP du client (who has 192.168.1.50)

@MAC source : ff :ff :00 :14 :1d :33	**@MAC destination** 00 :00 :00 :1c :4f :08
Sender IP: 192.168.1.50	**Target IP: 192.168.1.2**
Sender MAC : ff :ff :00 :14 :1d :33	**Target MAC**: 00 :00 :00 :1c :4f :08

Fig.8. Réponse ARP du serveur (192.168.1.50 is at ff :ff :00 :14 :1d :33)

2. Techniques utilisées pour attaquer un réseau :

2.1. Usurpation d'identité :

Dans les réseaux, il est possible de falsifier son identité réseau en modifiant l'adresse MAC ou l'adresse IP des paquets émis, par exemple pour contourner un contrôle de sécurité.

2.1.1. usurpation d'adresse MAC :

Les adresses MAC sont écrites en dur dans les cartes réseaux lors de leur fabrication. Elles ne peuvent donc a priori pas être changées. En revanche, aujourd'hui il existe des outils qui permettent d'envoyer des trames Ethernet en utilisant une autre adresse MAC que celle inscrite dans la carte.

- **Objectif** : permettre de passer un contrôle de sécurité (un point d'accès permet de restreindre son utilisation à certaines adresses MAC enregistrées).

2.1.2. usurpation d'adresse IP :

Il est également possible d'usurper une adresse IP source. Les paquets de données sont traités différemment en fonction de leur adresse source.

- **Ex1 :** Dans les réseaux, un routeur ou un pare-feu peut laisser passer des paquets dont l'adresse source indique qu'ils proviennent d'un site privilégié.
- **Ex2** : **rsh**, sous Unix, peut permettre l'exécution de commandes sans demander de mot de passe, à condition que la requête émane d'une adresse IP digne de confiance

3. Attaques sur les réseaux informatiques

3.1. écoute réseau (sniffer) :

L'écoute réseau consiste simplement à capturer une image du trafic qui circule sur un brin de réseau.

- **Ex** : mettre la carte réseau en mode écoute « Promiscuous mode »
- **Objectif** : Un des buts de l'écoute est d'exploiter le fait que de nombreuses méthodes d'authentification transmettent des mots de passe en clair sur le réseau.

3.2. Vol d'une session (hijacking)

Le vol d'une session est un moyen de s'introduire dans un system sans avoir besoin de connaître un nom d'utilisateur et un mot de passe.

- L'attaquant attend qu'un utilisateur légitime se connecte à distance au système.
- Une fois que l'utilisateur s'est authentifié et que la connexion est établie, l'attaquant prend le contrôle de la connexion et l'utilise à ses fins.

- La notion de session peut s'appliquer à différents niveaux (vol de session TCP « voir exo1 TD3 », vol d'une session Web, etc...)

3.3. IP Spoofing « usurpation d 'adresse IP dans des paquets TCP »

Dans cette attaque il y a 3 acteurs : l'attaquant (PC1), la victime (PC2), l'ordinateur dont l'adresse IP est forgé (PC3).

Pour réussir une attaque " IP Spoofing" dans le cas d'une connexion Tcp :

- Le PC3 (le propriétaire de l'adresse IP qu'on va utiliser) doit être arrêté ➔ hors service / Denis de service / l'isoler.
- l'attaquant (PC1) doit remplacer son adresse IP par l'adresse IP de la machine hors service (PC3).
- L'attaquant aura besoin de voir l'ISN utilisé par la victime ➔ pour envoyer des acquittements corrects.

Il existe 3 scenarios possibles :

3.3.1. Scenario 1 : l'attaquant et l'ordinateur dont l'adresse IP est forgé dans le même sous réseau « 192.168.1.0 » :

$IP_{attaquant}$ = 192.168.1.1

$IP_{victime}$ = 10.0.0.2

$IP_{forgé}$ = 192.168.1.3

i. L'attaquant (PC1) envoi une demande de connexion TCP à la victime (PC2) en utilisant l'adresse IP de la machine 3 :

CMD1 = | IP_{source} = 192.168.1.3 | $IP_{destination}$= 10.0.0.2 | SEQ(6000) | SYN.

ii. La victime (PC2) croit que la demande de connexion « CMD1 » vient de la machine 3

➔ Elle doit envoyer une CMD2 de type SYN, ACK au PC3 (et pas l'attaquant), avec le numéro ISN (ex : 9000).

CMD2 =| IP_{source} = 10.0.0.2 | $IP_{destination}$= 192.168.1.3 | SEQ(9000) | SYN | ACK

iii. Comme l'attaquant (PC1) se trouve dans le même sous réseau que l'ordinateur dont l'adresse IP est forgé (PC3) ➔ il peut utiliser un sniffer pour analyser la CMD2 et voir ce qui est à l'intérieure (c.à.d. il peut voir l'ISN =9000) ➔ il peut envoyer un ACK correcte : ACK=9001

iv. L'attaquant envoi un ACK correct à la victime pour confirmer la synchronisation

CMD3 = | IP_{source} = 192.168.1.3 | $IP_{destination}$= 10.0.0.2 | SEQ(6001) | ACK= 9001 | ACK.

v. Si La victime fait confiance à l'adresse IP= 192.168.1.3, dans ce cas l'attaquant peut bénéficier des nouvelles services. Ainsi, l'attaquant peut masquer sa propre identité pour réaliser une attaque contre un serveur.

3.3.2. Scénario 2 : l'attaquant et la victime se trouvent dans le même sous réseau

Le même principe que le 1er scénario, à la seule différence que l'écoute se passera dans le sous réseau où se trouve la victime et l'attaquant.

3.3.3. Scénario 3 : spoofing aveugle

Dans ce cas, l'attaquant n'est ni dans le sous-réseau de la cible ni dans celui de la machine dont l'adresse IP est forgée ➔ il ne sera pas capable d'écouter le paquet SYN-ACK ➔ il ne peut pas voir l'ISN.

Solution :

Deviner l'ISN ➔ analyser l'algorithme de génération de l'ISN de la victime. Comment trouver l'échantillon à analyser? En ouvrant quelques connexions légitimes avec la victime.

3.4. Détournement de connexion :

Les réseaux locaux câblés sont généralement commutés. L'efficacité du « Sniffer » est alors fortement réduite puisqu'il ne voit que le trafic concernant la machine sur laquelle il est installé.

Cette attaque consiste à détourner les paquets afin qu'ils transitent par lui, en utilisant l'une des attaques suivante :

- **Empoisonnement du cache ARP** : en altérant le cache ARP, il est possible de faire correspondre une adresse IP (victime) avec une adresse MAC différente (l'adresse MAC d'un attaquant). « la technique est décrite dans le TD et le TP »
    - **Conséquence** : les paquets à destination de l'adresse IP seront envoyés au travers Ethernet à l'adresse MAC de l'attaquant.
- **Empoisonnement DNS** : il est possible de corrompre la correspondance entre les noms de domaines et les adresses IP. Cela peut être réalisé en forgeant des réponses DNS, en modifiant le cache du serveur, ou en attaquant le serveur DNS primaire.

3.5. Découverte réseau :

Un attaquant cherchant à pénétrer un réseau ou une machine va devoir s'informer sur l'environnement cible.

La découverte réseau consiste à connaître quelles sont ***les machines allumées***, ***les ports ouverts***, ***les services actifs*** ainsi que ***les systèmes d'exploitation*** utilisés dans un réseau cible.

L'outil *nmap* est très utilisé pour ce genre de travaux et offre une très grande variété d'options pour atteindre les différents objectifs.

3.6. Dénis de service :

Une attaque par Denis de service (DoS) consiste à empêcher un système informatique de fonctionner correctement.

3.6.1. Inondation de requêtes SYN : « SYN flooding »

Cette attaque consiste à envoyer tellement de demande de connexion TCP « SYN » vers la cible qu'elle se trouve noyée et n'est plus capable de répondre aux requêtes légitimes.

Description :

- ✓ L'attaquant envoi un très grand nombre de demande connexion TCP.
- ✓ La machine qui reçoit un **SYN** répond par un **SYN-ACK.** A ce moment, la connexion est partiellement établie.
- ✓ la machine cible met cette connexion dans une queue de connexions qui attendent un ACK pour compléter la procédure d'établissement de connexion.
- ✓ L'attaquant n'envoi jamais les acquittement attendus.
    - **Conséquences** : la queue devient saturée, ce qui empêche le système d'accepter de nouvelle connexion☺.
    - **Contre-mesure :**
        - les connexions partiellement établies sont effacées si elles ne sont pas acquittées dans un délai raisonnable.

- Utiliser une fille d'attente circulaire.

3.6.2. Attaque par réflexion :

Une attaque par réflexion consiste à envoyer une requête à un grand nombre de machines, chacune allant répondre à la victime.

Ex : l'attaque « smurf » : consiste à noyer la victime par des réponse ICMP

- ✓ L'attaquant inscrit l'adresse de la victime comme adresse IP source dans le paquet ICMP.
- ✓ L'attaquant envoi la requête ICMP à plusieurs machines.
- ✓ Les machines qui reçoivent une requête ICMP doivent envoyer une réponse ICMP à la victime
    - Avantage : la victime n'aura aucun moyen de savoir qui lui veut du mal.

3.6.3. Dénis de service distribué : « DDoS »

Consiste a utiliser un grand nombre de machines simultanément afin d'attaquer une seule cible.