Cours de réseaux

M1 Informatique

Faculté Jean Perrin

Plan du cours

Partie 1 : Introduction

Partie 2 : Couche physique

Partie 3 : Couche liaison des données

Partie 4 : Couche Réseau / IPv4

Partie 5 : Couche Réseau / Routage

Partie 6 : Couche Réseau / IPv4, IPv6

Partie 7 : Couche transport : TCP et UDP

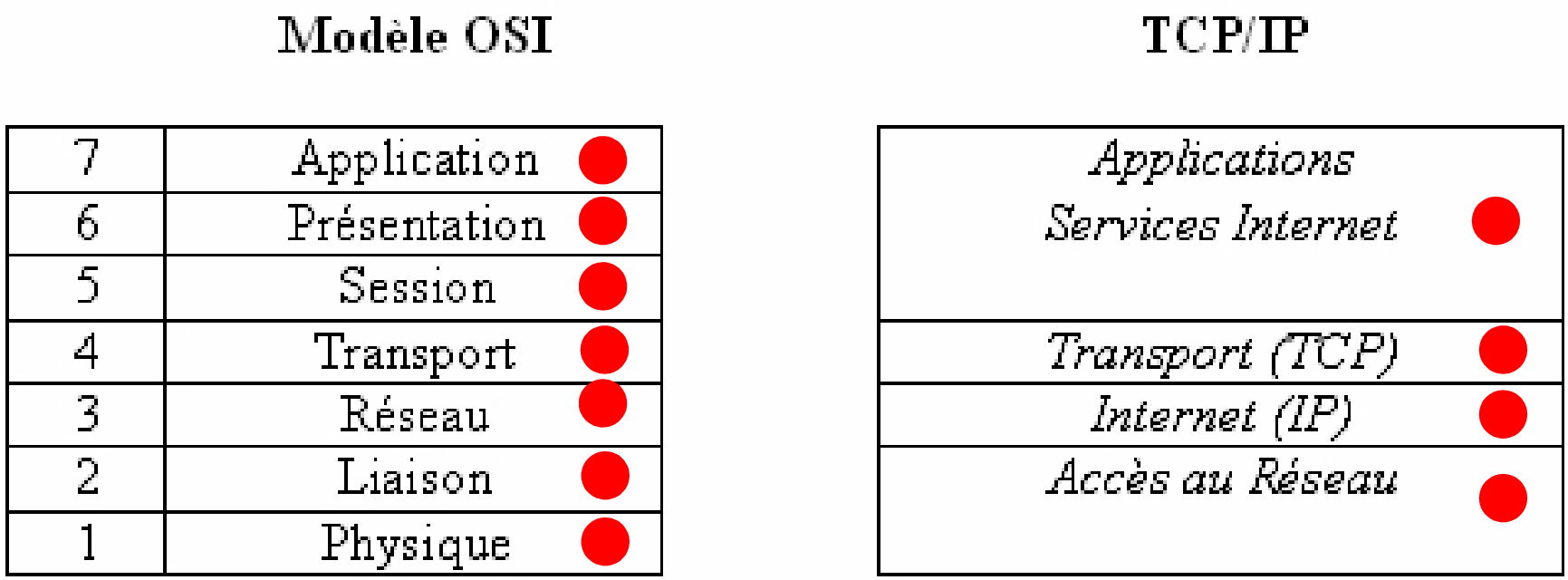
Partie 8 : Couche application

Partie 9 : Couche application / Etude de protocoles

Partie 10 : Notions d'attaques et de sécurité

Notions d’attaques et de sécurité

Vous êtes ici



Pour faire comme dans les films…

Et épater la famille ou les filles…

http://geektyper.com/

Introduction

Toute machine (ordinateur) connecté à un réseau est potentiellement vulnérable et peut faire l'objet d'une **attaque** par un **pirate** (**hacker**).

Une attaque s'appuie sur l'exploitation d'une faille sur le système : soit au niveau du réseau, soit au niveau de la machine (logiciel).

White hat vs Black hat

Il s'agit dans les deux catégories de hackers.

Les « **white hats** » sont des hackers éthiques ou des experts en sécurité. Ils traquent les failles de sécurité pour mieux les prévenir.(ex Kevin Mitnick).

Les « **black hats** » sont des hackers mal intentionnés et qui exploitent les failles de sécurité dans le but de nuire ou d'en tirer profit

Motivation des hackers

Vol de données : informations personnelles, secret industriels, données bancaires

Défi, orgueil, plaisir : prouver sa « puissance » aux autres (ou à soi-même)

Parasitisme : utiliser les ressources performantes d'un système.

Base pour une attaque plus complexe : le hacker utilise un système alpha pour attaquer un autre système.

Vengeance, motivation politique ou idéologique : il s'agit souvent de compromettre le fonctionnement du système (**hacktivistes**) -> attaque par **déni de service** (DoS)

Typologie d'attaques

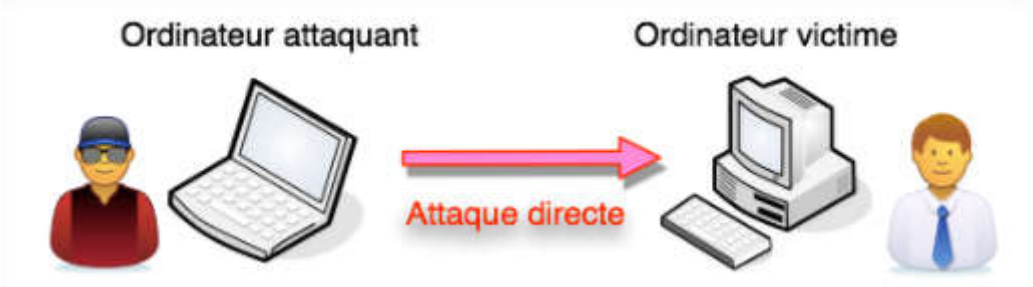
On trouve principalement trois types d'attaques :

- Attaques directes
- Attaques indirectes par rebond
- Attaques indirectes par réponse

Attaques directes

Utilisation d'un script ou d'un logiciel depuis la machine du hacker de manière à attaquer directement l'ordinateur de sa victime.

Hacker peu expérimenté pouvant être très vite repéré.



Attaques indirectes par rebond

Utilisation d'un (ou de plusieurs) ordinateur(s) intermédiaire(s) qui répercute(nt) l'attaque vers la cible.

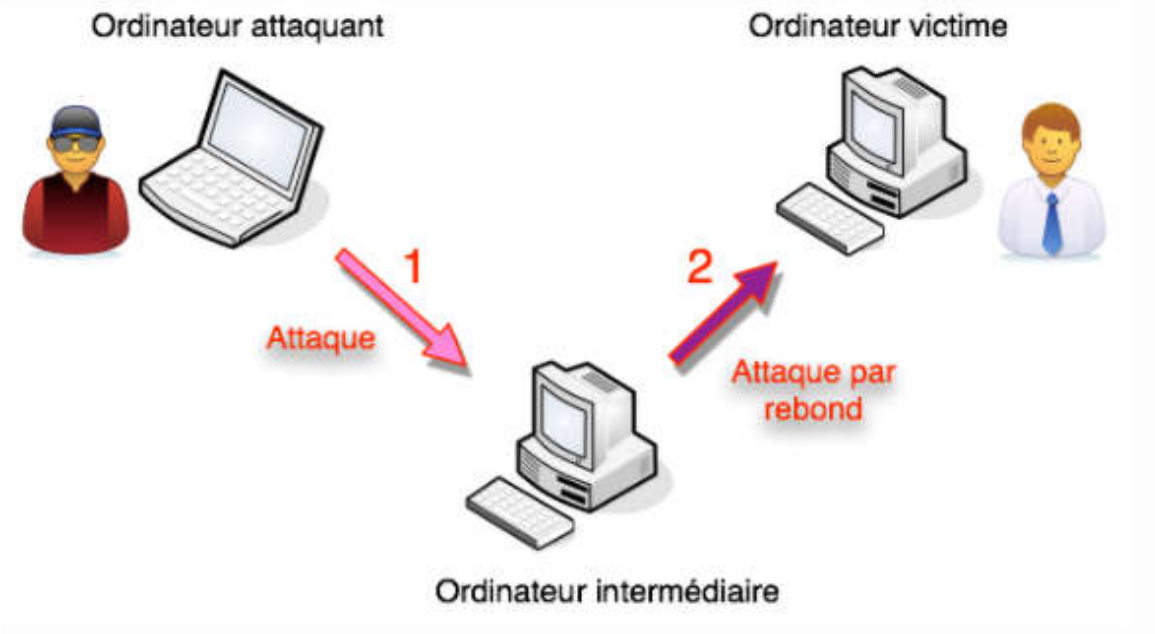
Avantages :

- Masque l'adresse IP du hacker
- Utilise les ressources de la machine intermédiaire
- Permet de s'attaquer à des serveurs plus gros (plus de puissance)

Mais il faut d'abord réussir à attaquer les machines intermédiaires.

Attaques indirectes par rebond

Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire qui répercute l'attaque vers la victime.



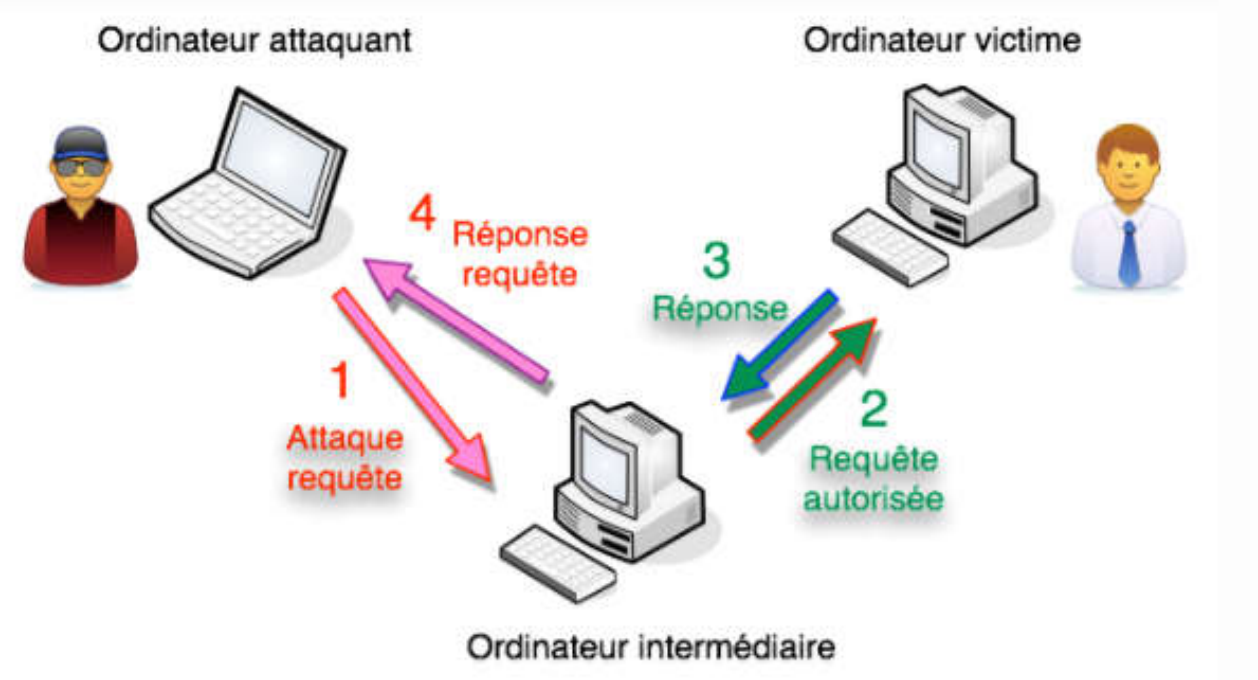
Attaques indirectes par réponses

Attaque dérivée de la précédente et présentant les mêmes avantages.

Le hacker envoie une requête (et non une attaque) vers l'ordinateur intermédiaire. La machine victime exécute cette requête pour l'intermédiaire (autorisé) et la réponse est renvoyée au hacker.

Utilisée surtout pour récupérer des données sensibles ou confidentielles.

Attaques indirectes par réponses



Les phases d'une attaque

L'attaque d'un système est généralement constituée de plusieurs phases:

- La reconnaissance
- Le balayage
- L'accès (attaque véritable)
- Maintien de l'accès
- La suppression des traces

Phase 1 : la reconnaissance

Cette phase se joue en amont de l'attaque. Elle consiste à ressembler le maximum d'information sur la « victime » (site, système, individu).

Ceci peut se faire par des moyens légaux :

- WHOIS (https://whois.arin.net/ui/)
- Site de l' ARIN (American Registry for Internet Number)

Ou illégaux :

- Vol de matériel, de documents
- Fouille de poubelles
- Utilisation de phishing, spywares
- Social engineering (par téléphone, internet ou en direct)

Phase 2 : le balayage

Le balayage consiste à trouver le ou les point(s) d'entrée du système ciblé.

En fonction du type de réseau, il peut prendre divers forme.

Exemple : Balayage de réseau sans fil de manière à pénétrer le réseau.

Le balayage de réseau sans fil

Appelé **WarDriving** : Wireless access research

Il permet de pénétrer facilement sur le réseau en utilisant un PDA, un ordinateur ou un smartphone.

Une clé WEP (*Wired Equivalent Privacy*) se casse en une dizaine de minutes en utilisant des utilitaires dispo sur le net (ex aircrack-ng)

-> *Weak Encryption Protocol*

Une clé WPA (*Wifi Protected Access*), WPA2 ont un meilleur niveau de sécurité (à partir de 20 caractères).

Il s'agit essentiellement de pénétrer le réseau dans le cadre d'une attaque indirecte. On se fait passer pour quelqu'un d'autre.

Le balayage du réseau

Utilisation d'outils tels que

- Scanner de port : indique quels sont les ports ouverts et les services tournant sur un système.
- Outils envoyant des paquets IP permettant de tester le firewall du réseau ou de connaitre le chemin suivi.

Il existe des utilitaires permettant de rechercher les faiblesses d'une machine (services faibles, pb de configuration, etc) afin de corriger les failles (exemple **Nessus, nmap**)

Remarque : Ces outils sont aussi utilisés par les hackers

Phase 3 : l'accès

L'accès au système est la partie visible de l'attaque. Il s'agit véritablement de pénétrer sur le réseau privé ou sur une machine.

Cela peut se faire soit

- En « attaquant » le système d'exploitation ou un logiciel : recherche des mots de passe (exemple dictionnaire, force brute…)
- En utilisant des failles réseaux ou des techniques telles que l'empoisonnement DNS, la saturation ARP, le vol de sessions TCP…

Phase 4 : le maintien de l'accès

Mise en place d'outils spécifiques de manière à pouvoir accéder facilement au système dans le futur.

Exemple :

- Cheval de Troie
- Porte dérobée (**backdoor**)
- **Rootkits** agissant au niveau du système d'exploitation

Phase 5 : la suppression des traces

Le hacker doit faire disparaître toutes les traces de son passage afin d'empêcher de remonter à lui.

Pour cela, il doit par exemple modifier les fichiers de logs pour effacer les indicateurs de son passage.

Les variantes d'attaques réseaux

La plupart des attaques réseau s'appuie sur une ou des vulnérabilités des protocoles (ou de leur mise en œuvre).

La plupart des attaques connues sont des variantes d'une des cinq grandes familles d'attaque :

- Fragments attacks
- IP Spoofing
- TCP Session Hijacking
- ARP Spoofing
- DNS Spoofing

Fragment attacks

Ce type d'attaques (historiques) s'appuie sur la fragmentation des paquets du protocole IP de manière à passer les filtres IP et ainsi autoriser la création d'une session TCP.

Il existe deux types d'attaques de cette famille :

- Tiny Fragment attack
- Fragment overlapping

Remarque : les filtres IP et firewall modernes savent traiter ce type d'attaques.

Fragment attacks

L'objectif est de pouvoir créer une connexion TCP avec la machine cible alors qu'il existe un filtre IP (firewall) interdisant à ma machine de se connecter à la machine cible.

Le travail du firewall est d'empêcher les demandes de connexion TCP provenant d'adresses inconnues.

Fragment attacks

Tiny Fragment

Faille 1 :La RFC 791 impose que tous les nœuds (routeurs) permettent de transmettre des paquets de taille 68 octets sans les fragmenter (taille minimale d'un paquet TCP/IP).

Faille 2 : Un filtre IP applique les mêmes règles de filtrage pour l'ensemble des fragments d'un paquet : la vérification se faisant sur le 1er fragment…

Il s'agit donc de masquer la demande de connexion TCP dans le 2ème paquet, de manière à ne pas être refusé par le filtre IP.

Fragment attacks

Tiny Fragment

L'attaque consiste à fragmenter sur 2 paquets la demande de connexion TCP :

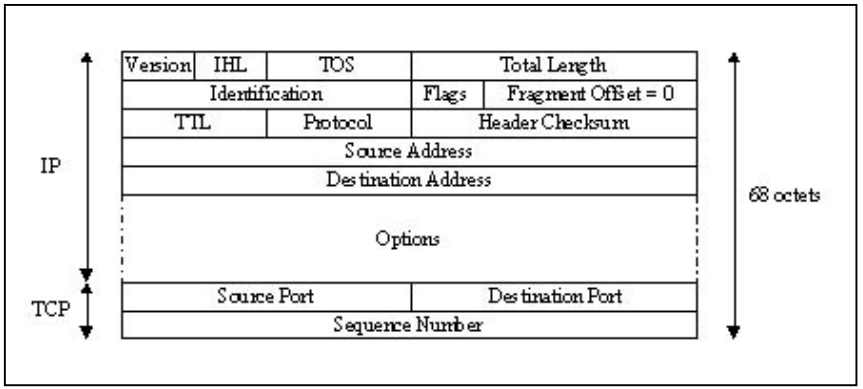
1er fragment contenant les 8 premiers octets de l'en-tête TCP : ports source et destination + numéro de séquence

2ème fragment contenant la partie demande de connexion (SYN = 1 et ACK =0)

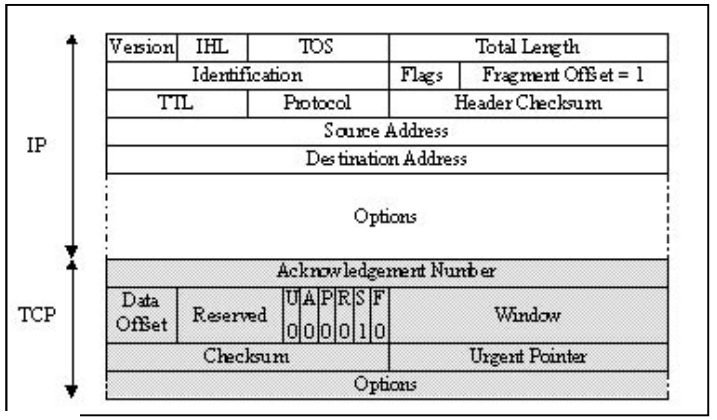
L'ensemble sera reconstitué lors de la défragmentation et envoyé à la couche TCP.

Fragment attacks

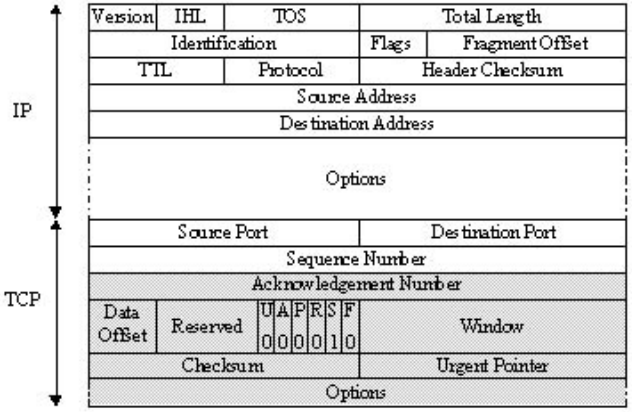
Tiny Fragment



Fragment 1



Fragment 2



Paquet reconstitué

Fragment attacks

Tiny Fragment

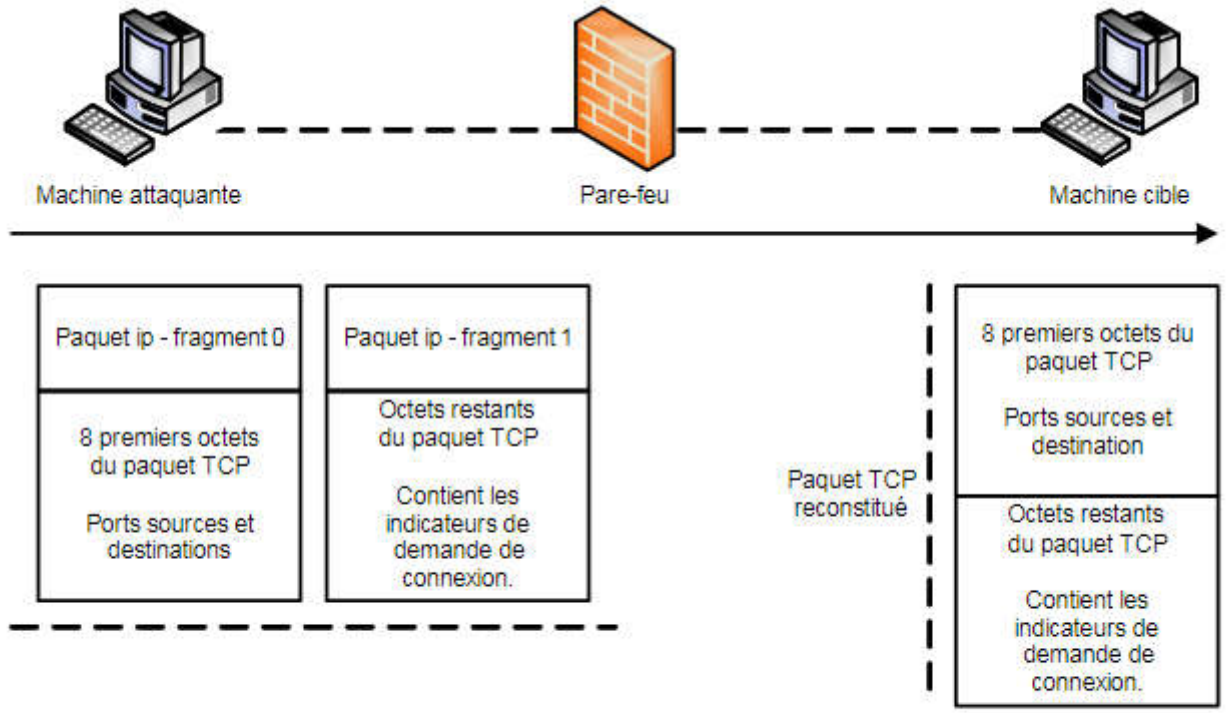


Figure 1.11

L'attaque par Tiny Fragments

Fragment attacks

Fragment overlapping

D'après la RFC 791 si deux fragments se superposent, le second écrase le premier.

L'attaque consiste donc à construire deux fragments de la manière suivante :

- 1er fragment (avec data) ne contenant aucune demande de connexion
- 2ème fragment contenant la demande de connexion et avec un offset tel qu'il écrase la donnée du premier.

Fragment attacks

Fragment overlapping

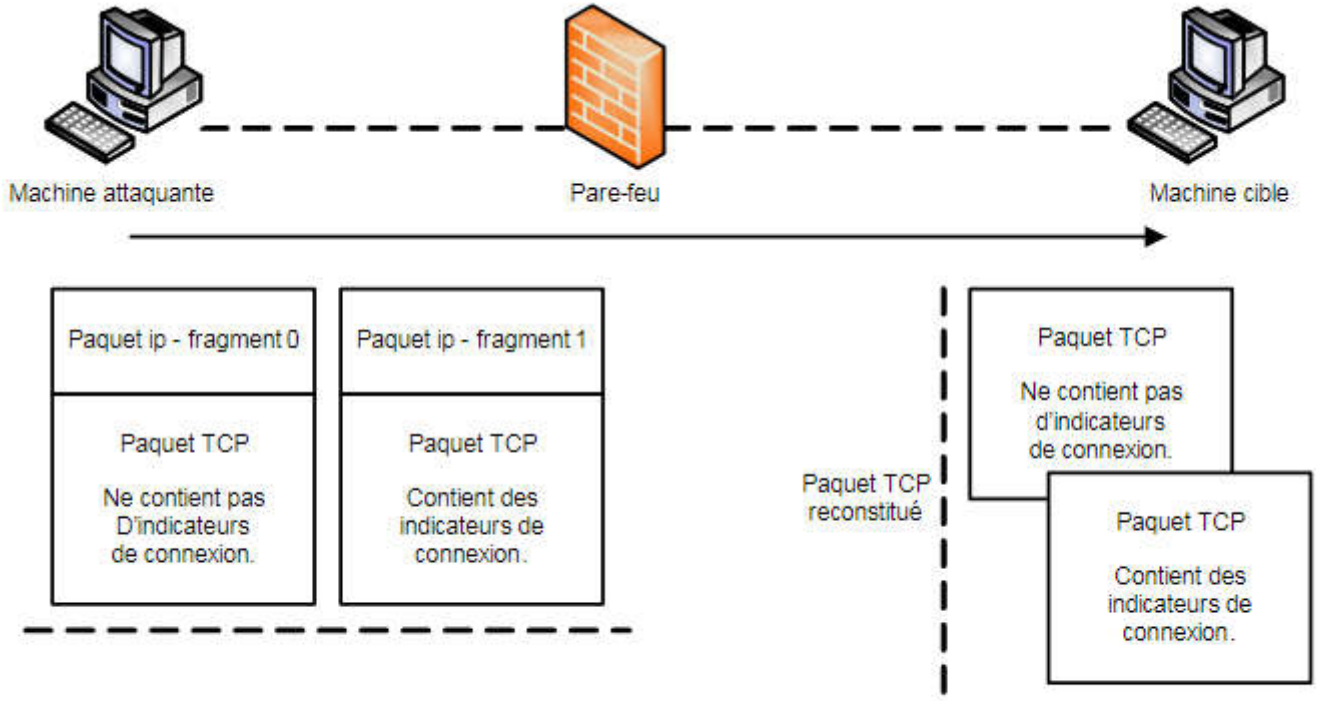


Figure 1.12

L'attaque par Fragment Overlapping

IP Spoofing

Le but est d'**usurper** (to spoof) l'adresse IP d'une machine

- soit pour cacher la source d'une attaque
- soit pour profiter d'une relation de confiance entre deux machines

Il s'agit de modifier l'adresse IP source dans les paquets IP.

La plupart du temps, le hacker ne reçoit donc pas les réponses puisque celles-ci arrivent sur la machine spoofée : on parle de **Blind spoofing**.

Historiquement, il existait cependant des techniques pour récupérer des réponses : utilisation du *Source Routing* ou mise en place du reroutage RIP.

IP Spoofing

Le **Blind Spoofing** s'utilise contre des services de type rlogin ou rsh dans lesquels le mécanisme d'authentification se base uniquement sur l'adresse IP de la machine cliente.

IP Spoofing

L'attaque IP Spoofing s'exécute en plusieurs étapes afin d'ouvrir une connexion TCP sur le port souhaité de la machine attaquée :

0. Détermination de l'adresse IP de la machine de confiance.
1. Prédiction des numéros de séquence de la machine attaquée (envoi de plusieurs paquets et analyse de l'algo d'incrémentation)
2. Mise hors service de la machine de confiance (-> déni de service) afin qu'elle ne réponde plus.
3. Envoi d'une demande de connexion TCP en utilisant l'adresse IP de la machine de confiance.
4. La machine attaquée envoie un ACK|SYN à la machine HS
5. Le pirate acquitte la connexion avec le numéro d'ACK prévu

Rappel : Le pirate ne voit pas ce qui est échangé avec la machine de confiance.

IP Spoofing

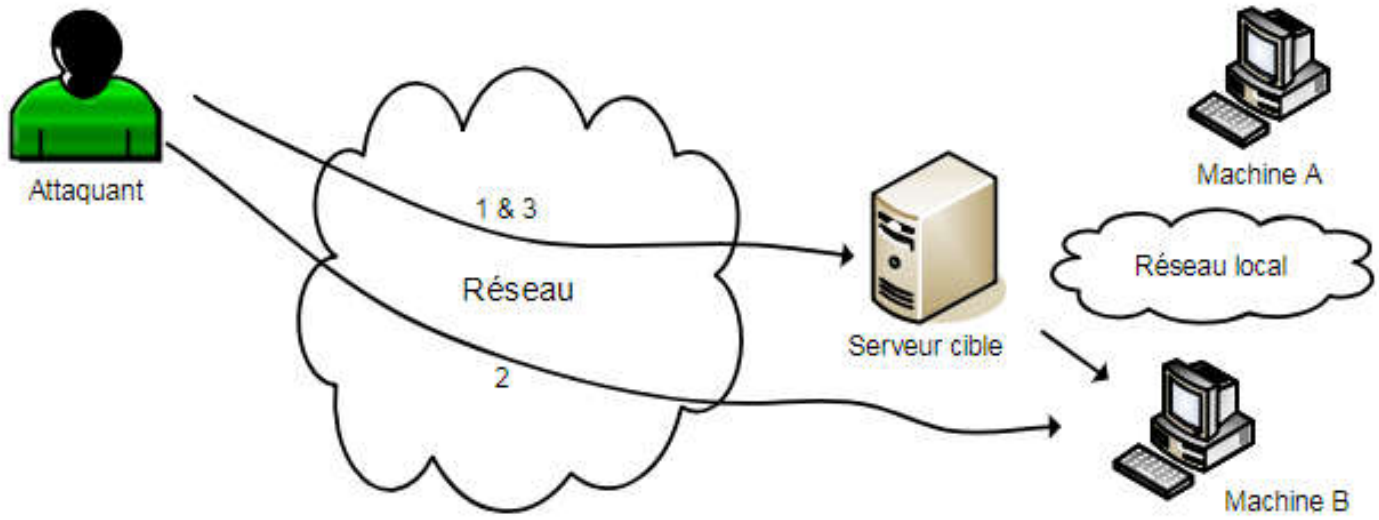


Figure 1.18

L'attaque IP spoofing

IP Spoofing

Comment se protéger

- Supprimer tous les services de type rsh et rlogin.
- Ne pas utiliser l'adresse IP comme unique méthode d'authentification (ajouter au moins un login et un password).
- Utiliser un système avec des numéros de séquence TCP non facilement prédictible.
- Activation de la fonction anti-spoofing sur le firewall.

TCP Session hijacking

Consiste à détourner (**to hijack**) une session TCP déjà établie entre deux machines.

Elle nécessite dans un premier temps une écoute passive sur la ligne (sniffing) de manière à laisser l'initialisation de la connexion TCP. Utilisation de logiciel d'écoute comme **tcpdump** ou **wireshark**.

Les traces sont de la forme :

src > dst : flags numSeq numAck cwindowSize urgentFlag

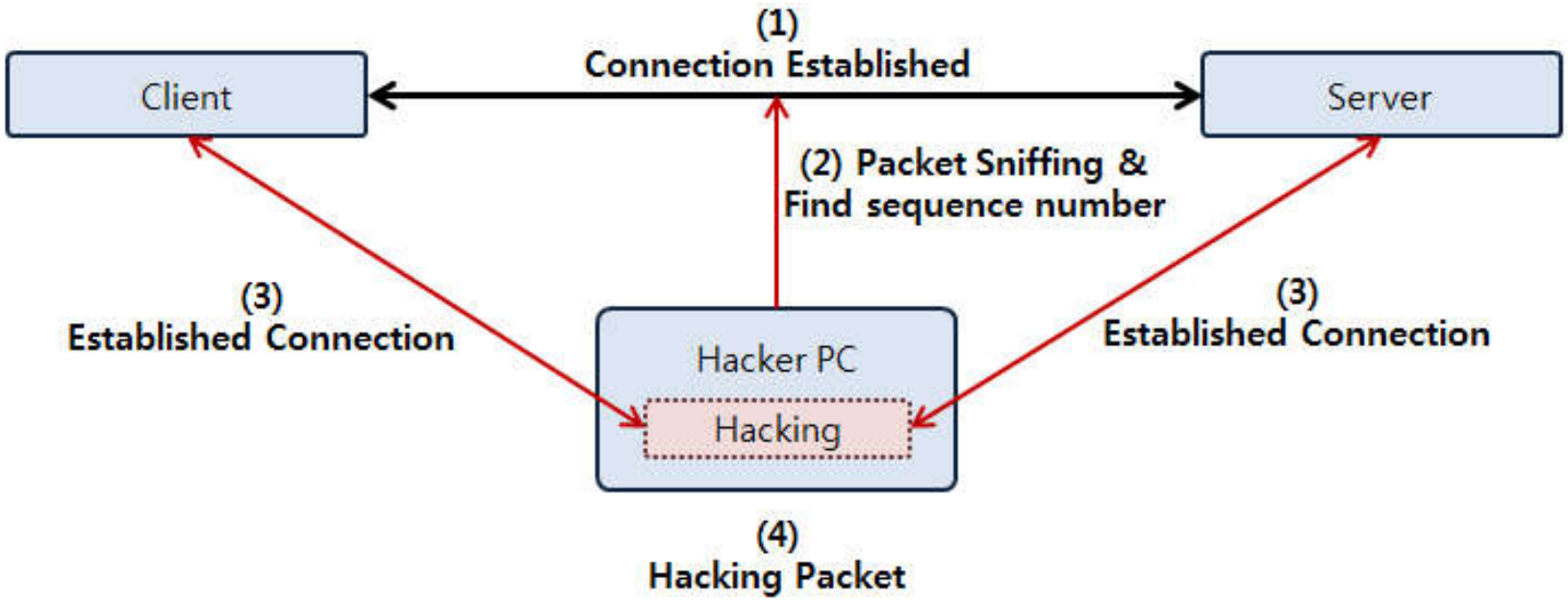
Puis l'attaque consiste en une désynchronisation de chaque côté de la connexion TCP de manière à voler la session.

Par exemple, dans une session entre A et B, la machine C du hacker envoie un ACK à la place de B suite à un envoi de A.

TCP Session hijacking

La **désynchronisation** entre A et B est effectuée lorsque le numéro de séquence du prochain octet envoyé par A est différent du numéro de séquence du prochain octet à recevoir par B et réciproquement.

TCP Session hijacking



TCP Session hijacking

Problème possible

ACK Storm : génération d'une multitude d'ACK due à la désynchronisation des séquences des deux machines légales.

Le pirate peut résoudre ce problème grâce à **l'ARP Spoofing**.

TCP Session hijacking

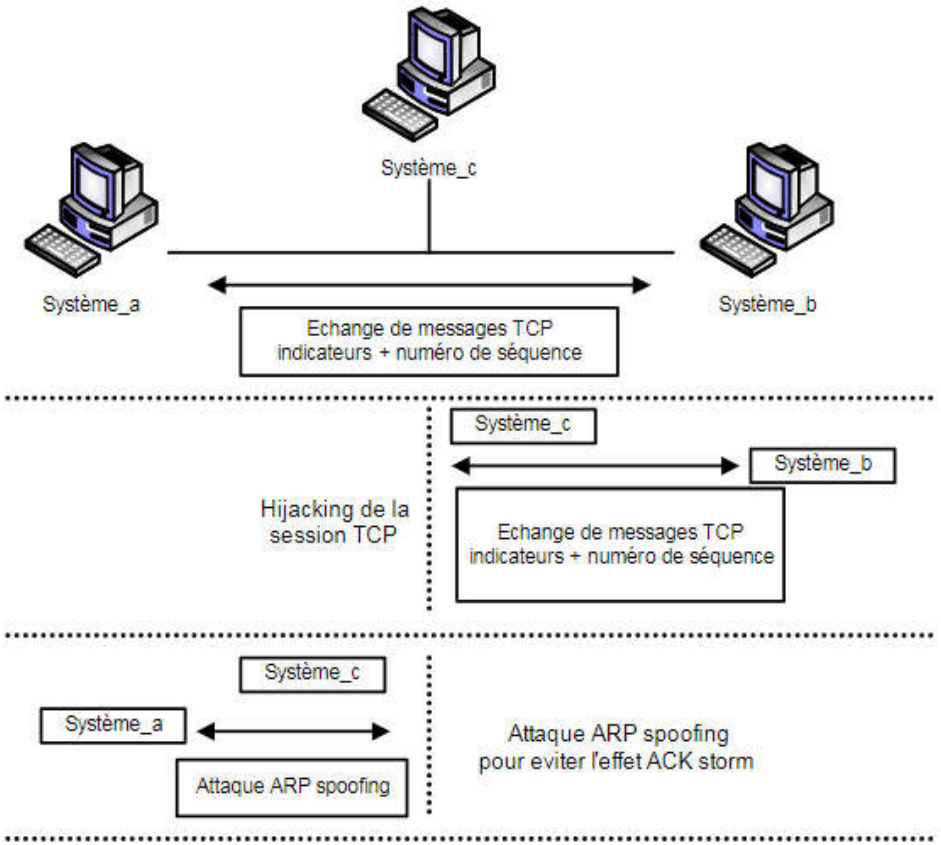


Figure 1.22

Hijacking d'une session TCP

ARP Spoofing

Egalement appelé ARP Redirect.

Cette attaque redirige le trafic réseau d'une ou plusieurs machines vers la machine du pirate. Elle s'effectue sur le réseau physique des victimes.

Rappel : ARP est le protocole de résolution d'adresses permettant de « traduire » une adresse IP en une adresse MAC.

ARP Spoofing

L'attaque corrompt le cache de la machine victime en envoyant des paquets ARP en réponse à une demande d'adresse MAC.

Il s'agit par exemple d'indiquer l'adresse MAC de la machine du pirate comme étant celle correspondant à l'IP d'une passerelle.

Le hacker est désormais destinataire de toutes les requêtes sortantes. Il peut les étudier avant de le router en sortie.

ARP Spoofing

Comment se protéger

- Avoir des logs régulièrement mis à jour et étudiés.
- N'utiliser que des tables ARP statiques.
- Utiliser des logiciels spécialisés pour monitorer les paires IP/MAC.

DNS Spoofing

Cette attaque consiste à faire parvenir de fausses réponses aux requêtes DNS émises par la victime.

2 méthodes possibles :

- DNS ID Spoofing
- DNS Cache Poisoning

DNS ID Spoofing

Principe : envoyer une fausse réponse à une requête DNS **avant** le serveur DNS. Ainsi, les prochaines requêtes vers l'URL cible seront détournées vers le serveur du pirate.

Le problème est de prédire l'ID de la demande (qui est également utilisée pour la réponse) :

- envoyer plusieurs réponses identiques avec des id différents (incrémentés de 1).
- Essayer les 65535 possibilités du champ ID : pas réaliste…
- Trouver l'algo de génération des ID…

Il faut également répondre avant le serveur DNS :

il suffit de le faire tomber avec un déni de service.

DNS Cache Poisoning

Principe : il s'agit ici de corrompre le cache du serveur DNS avec de fausses informations de manière à dérouter les requêtes vers un site pirate.

Utilisation d'un serveur DNS appartenant au hacker et destiné à répondre aux autres serveurs DNS tout en injectant de fausses données.

DNS Spoofing

Comment se protéger

- Mettre à jour les serveurs DNS (pour éviter la prédictibilité des numéros d'identification et les failles permettant de prendre le contrôle du serveur)

- Configurer le serveur DNS pour qu'il ne résolve directement que les noms des machines du domaine sur lequel il a autorité

- Limiter le cache et vérifier qu'il ne garde pas les enregistrements additionnels.

Les dénis de service

DOS : deny of service

Cette classe d'attaques a pour but d'entrainer une indisponibilité partielle ou totale de service.

Cette indisponibilité de service peut être :

- une étape indispensable pour l'élaboration d'une attaque plus complexe
- Une fin en soi simplement pour mettre à mal le service lui-même.

Les dénis de service

Il existe plusieurs types de déni de service utilisant les spécificités des protocoles TCP/IP

- SYN Flooding
- UDP Flooding
- Packet Fragment
- Smurfing
- Déni de service distribué

SYN Flooding

Principe : laisser un grand nombre de connexions TCP en attente sur la machine cible de manière à consommer de la mémoire et de la ressource.

Comment : le hacker envoie un très grand nombre de paquets TCP de type SYN sans jamais renvoyer de ACK à la réponse de la machine victime. (utilisation d'outils tels que synk4)

Astuce : utilisation d'adresses IP aléatoires….

UDP Flooding

Principe : Exploitation du mode non connecté de UDP et de son caractère non adaptatif au flux.

Comment : Génération d'une grande quantité de paquets UDP (**UDP Packet Storm**) vers une machine cible ou entre deux machines. Cela entraine une saturation des ressources et une congestion du réseau.

Remarque : UDP est prioritaire sur TCP.

Il peut donc éventuellement occuper toute la bande passante.

Packet Fragment

Principe : Exploitation de faiblesses dans l'implémentation de certaines piles TCP/IP au niveau de la défragmentation IP.

Exemple : Teardrop : l'offset de fragmentation du second fragment est inférieur à la taille du premier (overlapping). Un réassemblage mal implémenté entraine un crash machine.

Autres attaques de ce type : bonk, boink, newtear, ping of death

Smurfing

Principe : attaque basée sur le protocole ICMP en spoofant les paquets ICMP broadcastés de type ICMP ECHO (ping)

Comment : Spoofer les paquets ICMP ECHO REQUEST envoyés en mettant comme adresse IP celle de la victime. Le hacker envoie ensuite un flux continu de ping vers l'adresse broadcast du réseau cible ce qui a pour effet de démultiplier les réponses vers la victime.

Effet : trafic réseau important et congestion rapide.

Déni de service distribué

Principe : saturation du réseau victime en utilisant plusieurs sources (démons) et des maîtres (master) qui les contrôlent. Les maîtres permettent simplement de jouer le rôle du hacker.

Comment : l'attaque est du type SYN flooding, UDP Flooding ou smurf mais de manière distribuée…

Intérêt du mode distribué : permet de masquer la sources de l'attaque et de mettre sur pied une attaque très massive plus facilement.

L’homme du jour 1

Julian Paul **Assange**,

né le 3 juillet 1971 à Townsville (Australie) est un informaticien et un cybermilitant australien.

Fondateur, rédacteur en chef et porte parole de WikiLeaks site sur lequel il a publié des millions de documents confidentiels relatifs aux modes opératoires de l'armée américaine en Irak (et bien d’autres choses)

Il fait l'objet de poursuites judiciaires de la part des Etats-Unis. Réfugié à l’ambassade d’Equateur à Londres à partir de juin 2012, il est arrêté en avril 2019 par les autorités britanniques.

Il a reçu de nombreux prix en tant que journaliste ou défenseur de la liberté, etc)

2010 : Personnalité de l'année choisie par les lecteurs du magazine TIME
2011 : Médaille d'or du Prix Sydney de la paix pour la « défense du droit des individus à la connaissance
2013 : Prix du courage Yoko Ono Lennon for the Arts

L'homme du jour 2

Guy Fawkes

né le 13 avril 1570 à Stonegate (Angleterre) et mort le 31 janvier 1606 à Westminster.

Il est le membre de la Conspiration des poudres en 1605. (tentative de la part d'un groupe de catholiques de tuer Jacques 1er d'Angleterre, en faisant exploser le bâtiment de la chambre des Lords).

L’homme du jour 2

Son masque (V pour vendetta) est le symbole du mouvement des **anonymous** dans la lutte pour la liberté d’expression.

Conclusion

Aujourd'hui la sécurité contre les attaques à distance se renforce de plus en plus contrairement à la sécurité interne.

De nombreuses attaques (IP Spoofing, fragment attacks) apparaissent et subsistent à cause de bugs et de failles au niveau des OS.

La sécurité passe par une vigilance au quotidien sur tous les plans : matériel, logiciel et surtout humain.