Année 2009-2010

esil

Sécurité des systèmes informatiques
— Deni de service —

Nicolas Baudru
mél : nicolas.baudru@esil.univmed.fr
page web : nicolas.baudru.esil.perso.univmed.fr

Mise en garde

Ce cours a uniquement pour but de vous montrer les faiblesses des protocoles de la suite TCP/IP, et de vous aider à vous prémunir des attaques utilisant ces faiblesses.

Nous déclinons toute responsabilité quant à la mauvaise utilisation de ce cours.

L'utilisation des différentes attaques décrites dans ce cours peut être sanctionnée jusqu'à trois ans de prison et soixante quinze mille euros d'amende.

Sniffing

esil

☞ Renifleur : Software ou hardware permettant de surveiller et analyser le trafic transitant sur une portion d'un réseau (près d'un point d'accès wifi, sur un câble coaxial, sur un routeur, ...).
➥ nécessite des droits adaptés (ex : administrateurs pour le mode promiscuous).

☞ Données analysées : paquets IP, segments TCP/UDP, parfois plus.
➥ permet d'administrer efficacement le réseau en détectant les problèmes de congestions par exemple

☞ Attaque : utilisé de manière moins "conventionnelle", un sniffer permet aussi de récupérer et analyser les données transmisses sur le réseau.
➥ problèmes juridiques
➥ consultation aisée des données non chiffrées
➥ récupération des mots de passe

Sniffing – quelques outils

esil

☞ tcpdump C'est un outil en ligne de commande pour écouter ce qui se passe sur une interface réseau, disponible sur Linux, Mac, Windows, ...

Exemple : $ tcpdump

...
11 :21 :54.768942 IP 192.168.29.157.49580 > 192.168.29.1.domain
...

De nombreuses options sont disponibles : possibilité d'afficher le contenu des paquets, d'utiliser des filtres sur l'émetteur, le destinataire, le protocole, ...

Exemple : $ tcpdump host www.esil.univmed.fr and port 22

☞ Wireshark (Ethereal), Cain & Abel versions graphiques aux capacités étendues

Spoofing

esil

- Usurpation d'identité : peut avoir lieu à différents niveaux :
  - adresse IP
  - port TCP/UDP
  - nom de domaine DNS
  - etc.

- Permet de tromper un firewall, un service TCP, un serveur d'authentification

Dénis de Service (DoS)

esil

- ☞ Il s'agit de saturer un réseau ou un système pour le rendre inopérant.
- ☞ Très énervant pour la victime, facile à réaliser pour le pirate.
- ☞ Souvent basée sur une mauvaise implémentation de la pile TCP/IP ou une mauvaise configuration des firewalls ou des serveurs.
- ☞ Peut être provoquée par une seule machine ou simultanément par plusieurs machines (Distributed DoS).
- ☞ Un système de détection d'intrusion peut permettre de réagir au plus tôt à un déni de service afin d'y remédier.

Dénis de Service (DoS)

De très nombreuses méthodes permettent d'arriver à un DoS :

- le SYN flood consiste à saturer un serveur en envoyant un grand nombre de paquets TCP avec le flag SYN armé.
- l'UDP flood consiste à saturer le trafic réseau en envoyant un grand nombre de paquets UDP à une machine.
- la Teardrop Attack utilise une faiblesse de certaines piles TCP/IP (ex : sur Windows 95/98) au niveau de la fragmentation et du reassemblage.
- le ping of death utilise aussi une faiblesse de certaines piles TCP/IP lors de la gestion de paquets ICMP trop volumineux.
- le smurfing est aussi une attaque basée sur le protocole ICMP.
- les bombes e-mail consistent à envoyer sur le réseau des mails trop volumineux.

Détournement de flux

esil

☞ Cette attaque consiste à rediriger un flux de données (ex : connexion TCP) pour écouter, altérer ou détruire les informations transmises, ou prendre le contrôle d'un serveur.

☞ souvent basée sur une mauvaise implémentation de la pile TCP/IP et de l'IP spoofing

☞ Ce type d'attaque peut être les prémisses d'une attaque du type Man in the Middle.

Man in the Middle

esil

☞ Dans cette attaque une personne s'interpose de manière invisible au milieu d'une connexion pour écouter, altérer ou détruire les informations transmises, ou prendre le contrôle d'un serveur.

☞ souvent basée sur une mauvaise implémentation de la pile TCP/IP : ex : l'ARP cache poisoning

☞ Ce type d'attaque est très puissante puisqu'elle permet même de récupérer des mots de passe, de comprendre des connexions chiffrées, ...

Plan

esil

1 SYN Flooding

2 UDP Flooding

3 Attaque par fragmentation

4 Attaque par ICMP

5 ARP Poisoning

6 DNS Spoofing

7 Blind spoofing

8 TCP Hijacking

Fiche technique

esil

☞ Principe : multiplier les demandes de connexion TCP sans jamais les confirmer.

☞ Conséquences :

- DoS ;
- prépare à une autre attaque : le blind spoofing.

☞ Se protéger :

- une bonne configuration des firewalls permet de détecter/limiter ce type d'attaque. Par exemple, on peut limiter le nombre de connexions TCP par seconde.

Rappels sur TCP (Transmission Control Protocol)

esil

☞ Couche au dessus de IP

☞ Fournit un service orienté connexion entre la source et le destinataire : TCP assure que tous les paquets émis arrivent dans l'ordre grâce à plusieurs mécanismes

- les numéros de séquence (des paquets envoyés et reçus)
- les timers (pour l'établissement de la connexion, la retransmission, ...)
- le three-way-handshake

☞ Une connexion TCP est identifiée par $< destAddr, destPort, srcAddr, srcPort >$

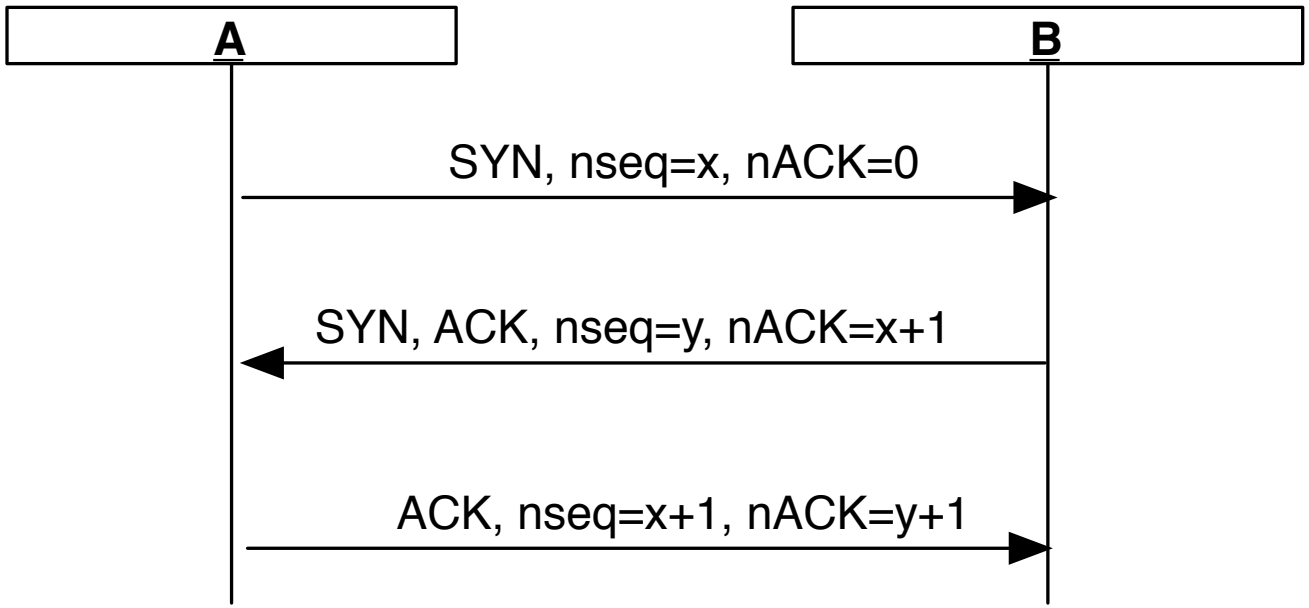
☞ Entête d'un paquet TCP

16-bit source port number	16-bit destination port number
32-bit sequence number	
32-bit acknowledgment number	
header length and flags	16-bit windows size
16-bit TCP checksum	16-bit urgent pointer
options	

☞ Remarque : Les flags peuvent être : URG, ACK, PSH, RST, SYN and FIN.

Rappels sur TCP – le three-way-handshake

esil

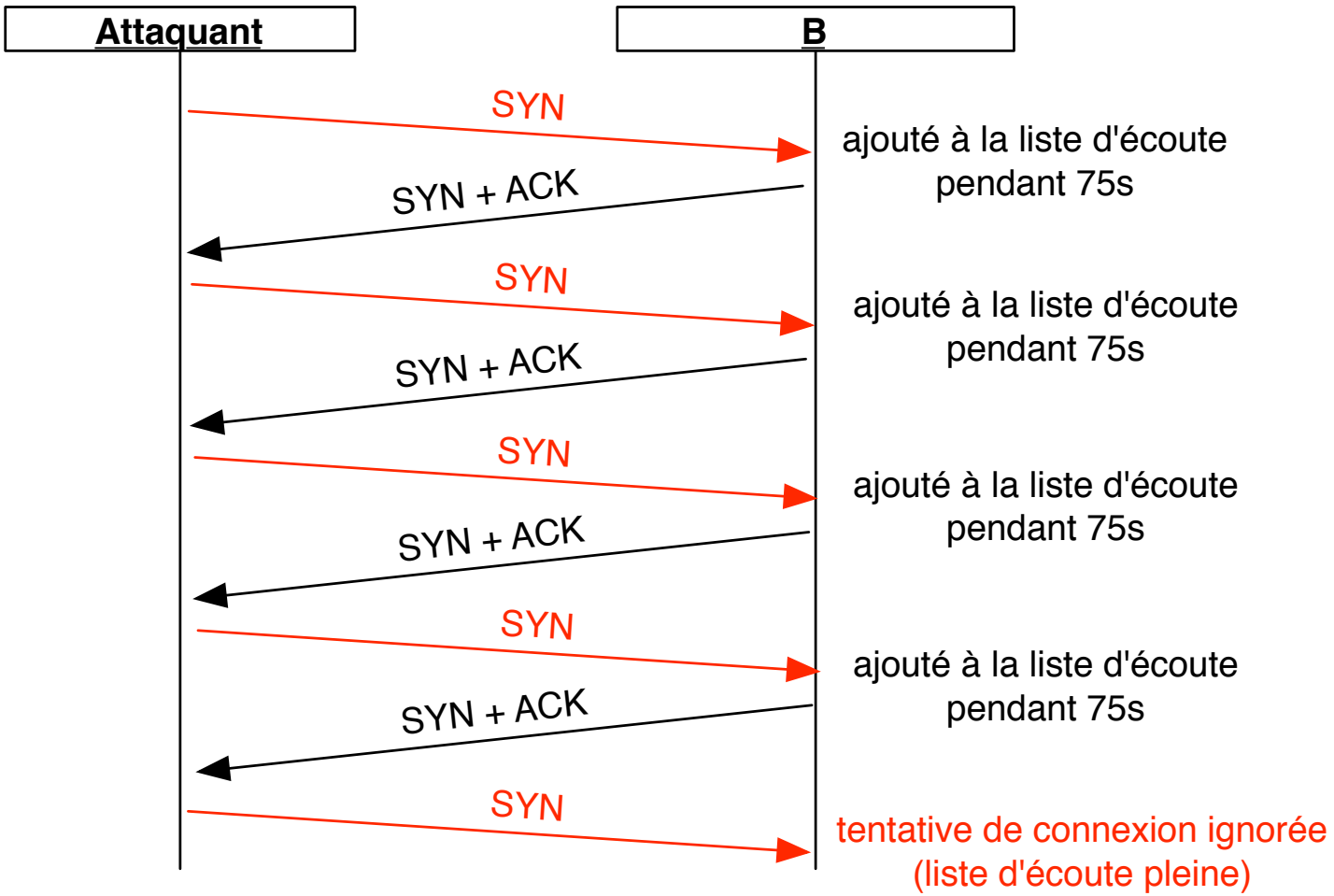


☞ Remarques importantes :

- les numéros de séquence initiaux x et y sont choisis “aléatoirement”.
- un timer est déclanché après l'envoi d'un SYN.
- si une réponse tarde trop à arriver (>75s), la connexion est abandonnée.

Fonctionnement du SYN Flooding

esil



Plan

esil

1 SYN Flooding

2 UDP Flooding

3 Attaque par fragmentation

4 Attaque par ICMP

5 ARP Poisoning

6 DNS Spoofing

7 Blind spoofing

8 TCP Hijacking

Fiche technique

esil

☞ Principe : cette attaque exploite le mode non connecté du protocole UDP. Elle consiste à générer une grande quantité de paquets UDP soit à destination d'une machine soit entre deux machines (Ex : Chargen Denial of Service Attack).

☞ Conséquences :

- DoS : congestion du réseau et saturation des ressources des deux hôtes victimes ;
- congestion généralement plus importante qu'avec le TCP Flooding car
  - UDP ne possède pas de mécanisme de contrôle de congestion ;
  - les paquets UDP sont prioritaires sur les paquets TCP.
- la totalité de la bande passante peut être saturée : effondrement de la totalité du réseau

☞ Se protéger :

- Configurer les firewalls pour limiter le trafic UDP.
- Désactiver si possible certains services comme echo et chargen.

Rappels sur IP (Internet Protocol)

esil

☞ C'est la couche réseau d'internet : son rôle est d'acheminer un paquet de la source vers le destinataire

☞ C'est un service sans connexion : les datagrammes (paquets IP) peuvent passer par des routeurs différents, se doubler et même se perdre

<table>
<tr><td>version</td><td>IHL</td><td>service</td><td colspan="2">total length</td></tr>
<tr><td colspan="3">identification</td><td>flags</td><td>fragmentation offset</td></tr>
<tr><td colspan="2">time to live</td><td>protocol</td><td colspan="2">header checksum</td></tr>
<tr><td colspan="5">32-bit source address</td></tr>
<tr><td colspan="5">32-bit destination address</td></tr>
<tr><td>options</td><td colspan="4">padding</td></tr>
</table>

☞ Faiblesse d'IP :

- Aucun champs n'est chiffré dans une entête IP
- Il n'y a pas de service d'authentification

➥ le spoofing est aisé

Rappels sur UDP (User Datagram Protocol)

esil

☞ C'est un protocole de la couche transport

☞ C'est un service sans connexion et non fiable : les paquets UDP peuvent se doubler ou se perdre

☞ Aucun service supplémentaire n'est ajouté par rapport à IP

☞ Entête d'un paquet UDP :

port source (16 bits)	port destination (16 bits)
longueur	total de contrôle

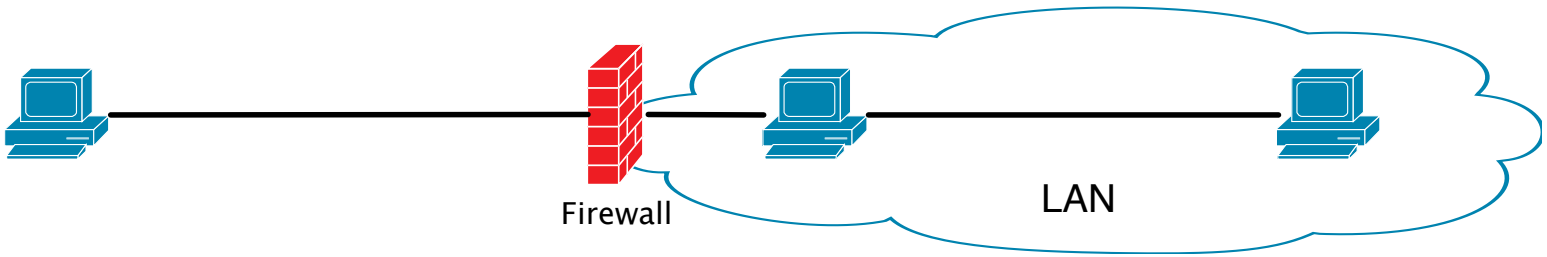
☞ Faiblesse d'UDP :

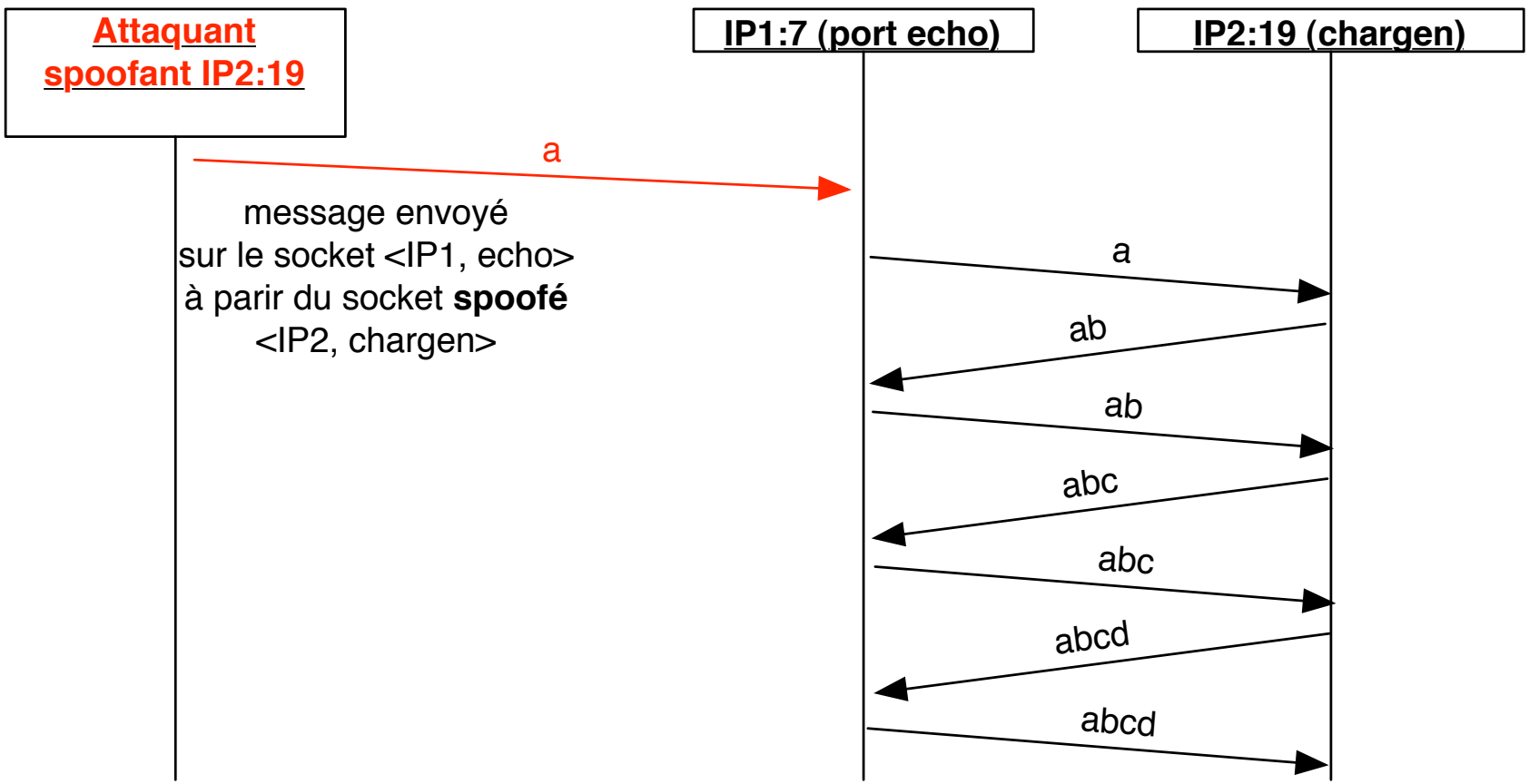
- Aucun champs n'est chiffré dans une entête UDP
- Il n'y a pas de service d'authentification

➥ le spoofing est aisé

Chargen Denial of Service Attack

esil





Plan

esil

1 SYN Flooding

2 UDP Flooding

3 Attaque par fragmentation

4 Attaque par ICMP

5 ARP Poisoning

6 DNS Spoofing

7 Blind spoofing

8 TCP Hijacking

Fiche technique

esil

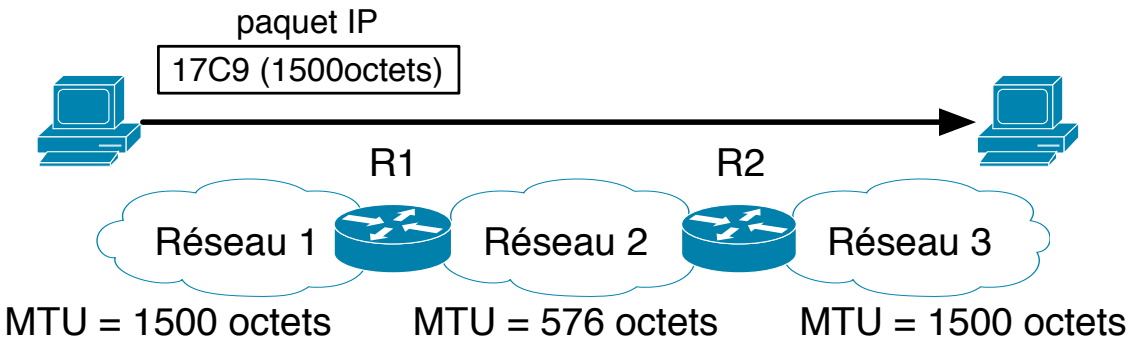
☞ Principe : Les dénis de service de type Packet Fragment utilisent des faiblesses dans l'implémentation de certaines piles TCP/IP au niveau de la défragmentation IP (réassemblage des fragments IP). Une des attaques les plus connues utilisant ce principe est Teardrop.

☞ Conséquences : Certains cas de réassemblage non prévus entraînent un crash de la machine et donc un déni de service.

☞ Se protéger : Installer si possible une implémentation de la pile TCP/IP résistant à cette faille.

Rappels sur la fragmentation

esil



entête IP :

version	IHL	service	total length	
identification			DF | MF	fragmentation offset
time to live		protocol	header checksum	
32-bit source address				
32-bit destination address				

entêtes des différents fragments :

	Identification	MF	offset
Fragment 1	17C9	1	0
Fragment 2	17C9	1	69
Fragment 3	17C9	0	138

Teardrop Attaque

esil

☞ L'idée On découpe le paquet original en deux fragments de telle sorte que le deuxième fragment est contenu dans le premier (overlapping).

Exemple : si pour un paquet original de 800 octets, on effectue intentionnellement la fragmentation suivante :

entêtes des différents fragments :

	Identification	MF	offset	taille du fragment
Fragment 1	17C9	1	0	552
Fragment 2	17C9	0	5	248

Alors le second fragment recouvre le premier.

Plan

1 SYN Flooding

2 UDP Flooding

3 Attaque par fragmentation

4 Attaque par ICMP

5 ARP Poisoning

6 DNS Spoofing

7 Blind spoofing

8 TCP Hijacking

Fiche technique

esil

☞ Principe : Cette attaque utilise
- le protocole ICMP,
- de l'IP spoofing,
- parfois le broadcast.

☞ Conséquences :
- denis de service (dans le cas de smurfing par exemple).
- interception de paquets.

☞ Se protéger :
- configurer les firewalls pour limiter le trafic ICMP par seconde ;
- configurer les firewalls pour bloquer les ping ;
- interdire le broadcast.

Rappels de ICMP

esil

☞ C'est un protocole de diagnostic complémentaire à IP : ICMP est un mécanisme de contrôle des erreurs au niveau IP.
☞ Chaque message ICMP est encapsulé dans un paquet IP pour traverser le réseau bien que ICMP n'est pas un protocole de niveau supérieur à IP.

☞ Entête d'un paquet ICMP (32 bits) :

type d'erreur (8bits)	info complémentaire (8bits)	header checksum

☞ Quelques types d'erreur :

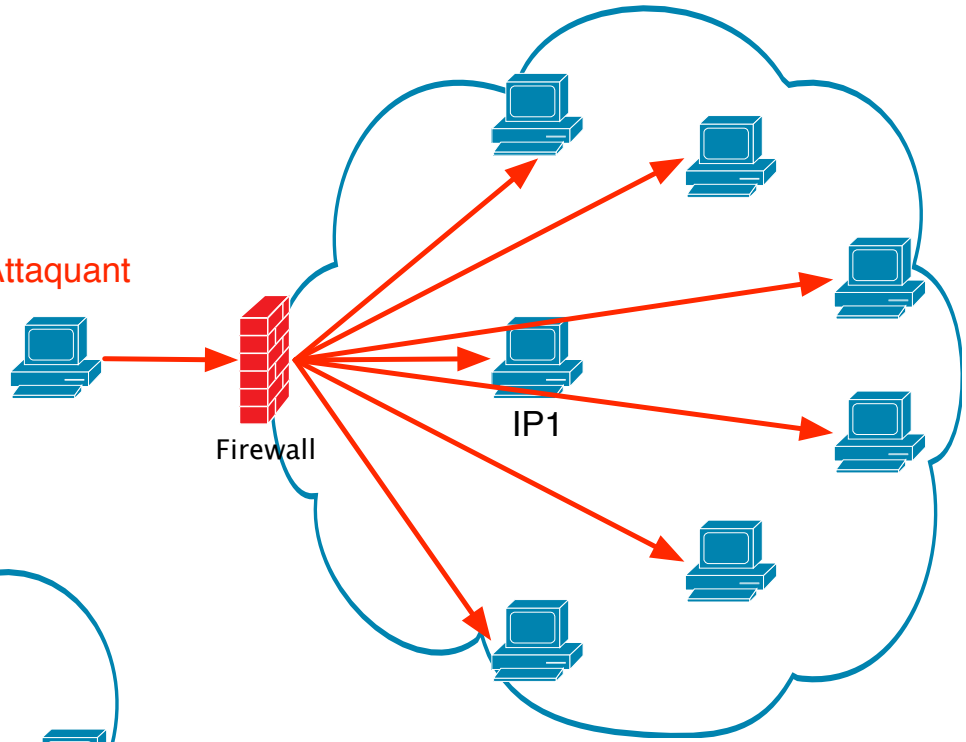
- type 8 (Echo Request) : test si la machine cible est opérationnelle
- type 0 (Echo Reply) : en réponse au paquet ICMP de type 8
- type 11 (Time Exceeded) : exploité par traceroute

smurfing

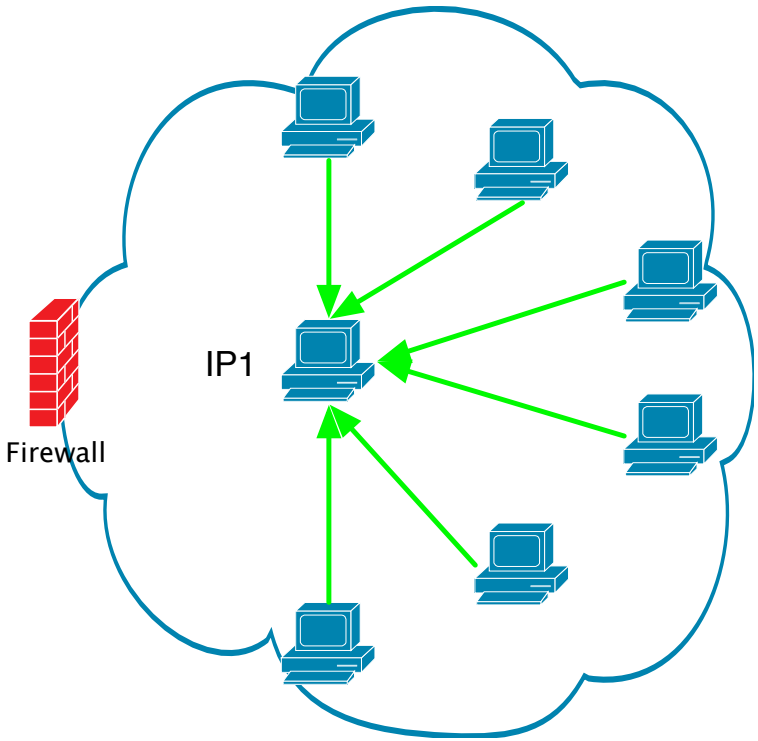
esil

1

envoi d'un
message ICMP de type
echo request
à tous les PC avec une
comme adresse source
celle de la machine cible
(ici IP1)



2



En conséquence, tous les
PC vont renvoyer un message
ICMP echo reply à IP1

Autres attaques par ICMP

esil

☞ Les messages ICMP “Time exceeded” ou “Destination unreachable” peuvent forcer un ordinateur à casser ses connexions en cours (celles concernées par le message). Si un attaquant envoie de manière répétée de faux messages de ce type, il peut causer un DoS.

☞ Les messages ICMP "Redirect" (normalement utilisés par les routeurs) permettent de détourner un flux de données en spécifiant la route que doit emprunter les paquets. Deux restrictions : l'attaquant doit être sur le même réseau local, et d'autre part, une connexion entre l'attaquant et la victime doit déjà exister.

Plan

1 SYN Flooding

2 UDP Flooding

3 Attaque par fragmentation

4 Attaque par ICMP

5 ARP Poisoning

6 DNS Spoofing

7 Blind spoofing

8 TCP Hijacking

Fiche technique

esil

☞ Principe : cette technique consiste à empoisonner les tables de correspondance $< adresseIP, adresseMAC >$ de tous les équipements informatiques d'un réseau.
Elle opère au niveau Ethernet et utilise :

- l'IP spoofing
- le broadcast
- des requêtes ARP

☞ Conséquences :

- DoS ;
- sniffing (même si un switch se trouve entre l'attaquant et la victime) ;
- peut être utilisée pour des attaques plus évoluées du type man in the middle.

☞ Se protéger :

- saisir manuellement les tables ARP (peu réaliste) ;
- centraliser les tables de correspondance sur un serveur DHCP ;
- surveiller le trafic ARP (avec par ex arpwatch ou un NIDS).

Rappels sur le protocole Address Resolution Protocol (ARP)

esil

☞ protocole de niveau 2 qui permet à une machine d'obtenir la correspondance entre adresses MAC et adresses IP des autres machines. Cette correspondance est localement stockée dans un cache ARP.

☞ Entête d'un paquet ARP :

<table>
<tr><td colspan="2">type de matériel (16bits)</td><td>type de protocole (16bits)</td></tr>
<tr><td>lg adr. phys</td><td>lg adr. log.</td><td>requête/réponse ARP/RARP</td></tr>
<tr><td colspan="3">adr. phy. émetteur</td></tr>
<tr><td colspan="2">adr. phy. émetteur</td><td>adr. log. émetteur</td></tr>
<tr><td colspan="2">adr. log. émetteur</td><td>adr. phy. destinataire</td></tr>
<tr><td colspan="3">adr. phy. destinataire</td></tr>
<tr><td colspan="3">adr. log. destinataire</td></tr>
</table>

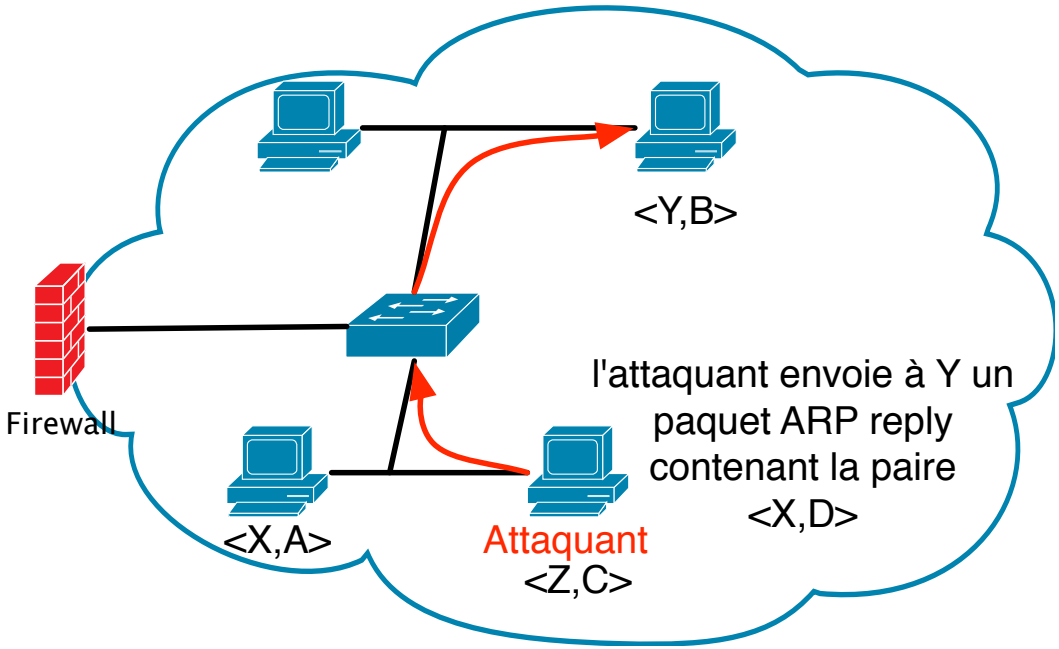
☞ Quelques précisions :

- type de matériel : 1 si Ethernet ;
- type de protocole : 0x0806 pour ARP.

➥ pas de protection : très facile à spoofer

Obtenir un DoS

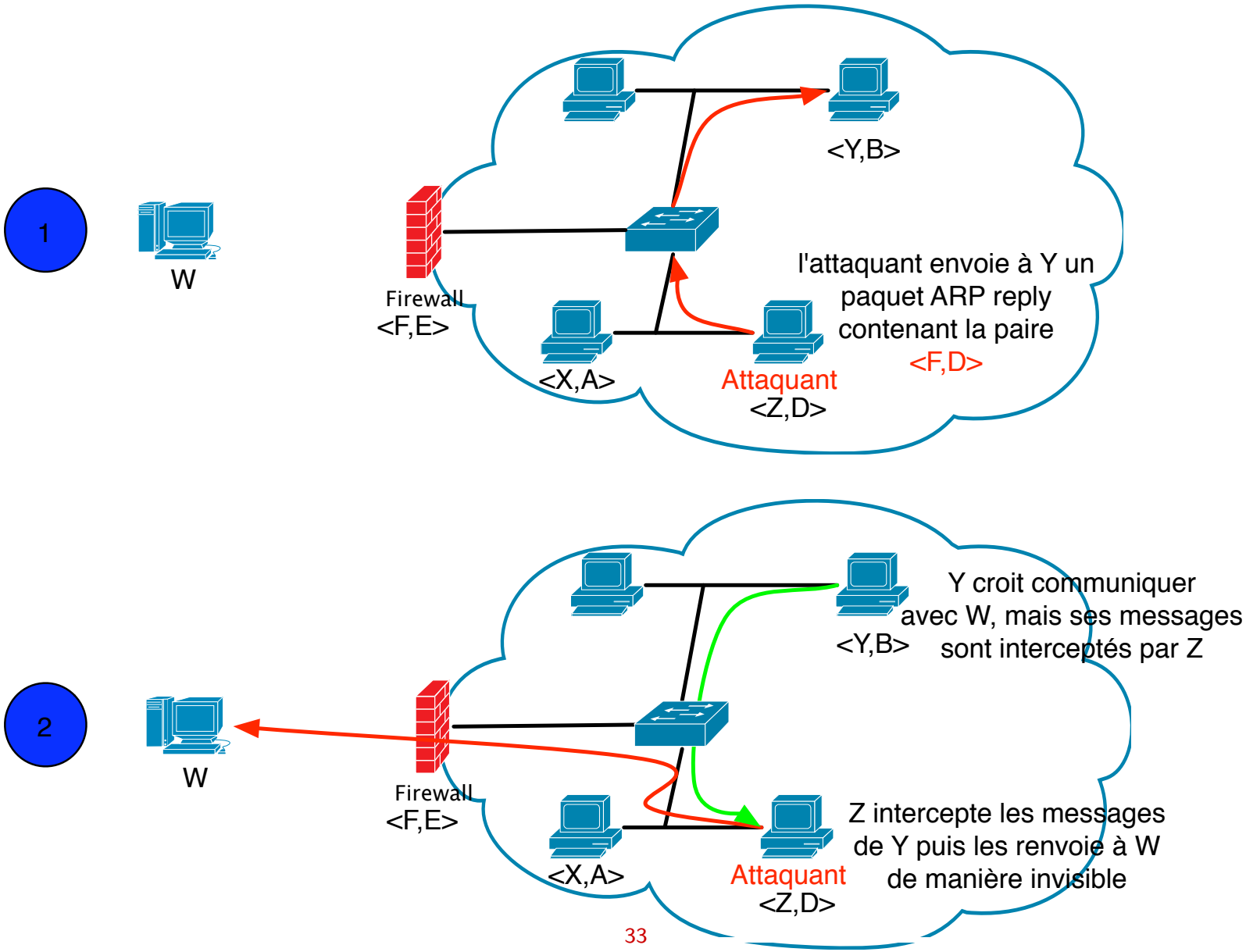
esil



- L'attaquant empoisonne le cache de la victime en lui envoyant de fausses correspondances $< adr.log., adr.phy. >$:
  ➥ la victime ne peut plus communiquer normalement (DoS).
- Cette attaque peut être déployée sur l'ensemble du réseau par broadcast.
- Cette attaque peut être employée pour isoler une machine des autres.
- Cette attaque est invisible pour le switch.

Rediriger un flux de données

esil



Plan

1 SYN Flooding

2 UDP Flooding

3 Attaque par fragmentation

4 Attaque par ICMP

5 ARP Poisoning

6 DNS Spoofing

7 Blind spoofing

8 TCP Hijacking

Fiche technique

esil

☞ Principe : cette technique consiste à faire parvenir à une victime de fausses réponses aux requêtes DNS. Cette attaque utilise

- IP spoofing
- la persistance des correspondances <nom, IP> dans les caches DNS

☞ Conséquences :

- DoS ;
- sniffing dans le cas d'une redirection vers un site pirate : risques de vols de session, de cookies, d'informations personnelles

☞ Se protéger :

- rendre les numéros d'identification des requêtes difficilement prédictibles ;
- configurer le serveur DNS pour qu'il ne résolve directement que les noms des machines du domaine sur lequel il a autorité (i.e. limiter le cache) ;
- ne pas baser de systèmes d'authentification sur le nom de domaine ;
- utiliser DNSsec.

Rappels sur le protocole DNS

esil

☞ Rôle du DNS : permet de mettre en relation les noms d'hôtes ou de serveurs de messagerie avec leurs adresses IP.

☞ Fonctionnement : le coeur du DNS est une base de données répartie représentant un "schéma de nommage hiérarchique" fondé sur la notion de domaine. Lorsqu'un programme a besoin d'une adresse IP correspondant à un nom :

1. le programme fait appel à un résolveur ;
2. ce dernier envoie une requête UDP de résolution de nom au serveur DNS local ;
3. si le serveur local connaît ce nom (il est dans son cache), il envoie une réponse au résolveur sinon il interroge récursivement les serveurs de plus haut niveau ;
4. une fois la réponse obtenue, le résolveur indique l'adresse IP cherchée au programme.

☞ Quelques précisions :

- les requêtes et les réponses sont appairées grâce à un numéro d'identification.
- tous les serveurs DNS ayant participé à la recherche mettent à jour leur cache

DNS cache poisoning

esil

☞ Le DNS Cache Poisoning consiste à corrompre le cache d'un serveur DNS avec de fausses informations. Pour cela le pirate C doit avoir sous son contrôle :

- un nom de domaine, par exemple pirate.com
- et le serveur DNS ayant autorité sur celui-ci ns.pirate.com.

☞ On suppose ici que le serveur DNS de A ne connaît pas l'adresse IP de B et C. L'attaque se déroule alors en plusieurs étapes :

1. Le pirate envoie une requête vers le serveur DNS de A demandant la résolution du nom de sa machine (appartenant au domaine pirate.com) ;
2. Le serveur DNS de A relaie cette requête à ns.pirate.com et obtient une réponse qu'il stocke dans son cache ;
3. C envoie une requête au serveur DNS de A pour connaître sa propre adresse IP. Il obtient alors une réponse contenant le numéro d'identification courant ID utilisé par le serveur DNS de A.

DNS cache poisoning – suite

4. C envoie aussitôt une requête au serveur DNS de A pour connaître l'adresse IP de B ;
5. Ce serveur DNS relaie la requête au serveur de niveau supérieur ;
6. Avant que la réponse du serveur de niveau supérieur arrive, C envoie une réponse DNS falsifiée : elle contient la paire <nom de B, adresse IP de C> et possède l'identifiant ID+1 (il est aussi nécessaire de spoofer l'adresse IP du serveur DNS de niveau supérieur) ;
7. La réponse du serveur DNS de niveau supérieur arrivant après, elle sera ignorée par le serveur de A.
8. A va alors communiquer avec C, tout en croyant communiquer avec B.

Plan

1 SYN Flooding

2 UDP Flooding

3 Attaque par fragmentation

4 Attaque par ICMP

5 ARP Poisoning

6 DNS Spoofing

7 Blind spoofing

8 TCP Hijacking

Fiche technique

esil

☞ Principe : technique utilisée pour profiter d'une relation de confiance (basée sur les adresses IP) entre deux machines (ex : rlogin, rsh). Cette attaque utilise

- de l'IP spoofing,
- une faiblesse de certaines implémentations du protocle TCP conduisant à des numéros de séquence facilement prédictibles,
- les options de routage du protocole IP ou le reroutage,
- le SYN flooding.

☞ Conséquence :

- Établissement d'une liaison clandestine entre l'attaquant et l'hôte cible.

☞ Se protéger :

- prévenir ce type d'attaque en testant s'il est facile de deviner le numéro de séquence TCP (par exemple en utilisant nmap) ;
- supprimer les services se basant uniquement sur une identification IP (ex : rlogin) et utiliser à la place des tunnels (ex : ssh) ;
- configurer les routeurs pour supprimer les messages contenant des options de routage : désactiver l'option source IP routing sur les firewall.

Rappels sur IP (Encore)

esil

☞ Entête IP

version	IHL	service	total length	
identification			flags	fragmentation offset
time to live		protocol	header checksum	
32-bit source address				
32-bit destination address				
options	padding			

☞ Précisons un peu :

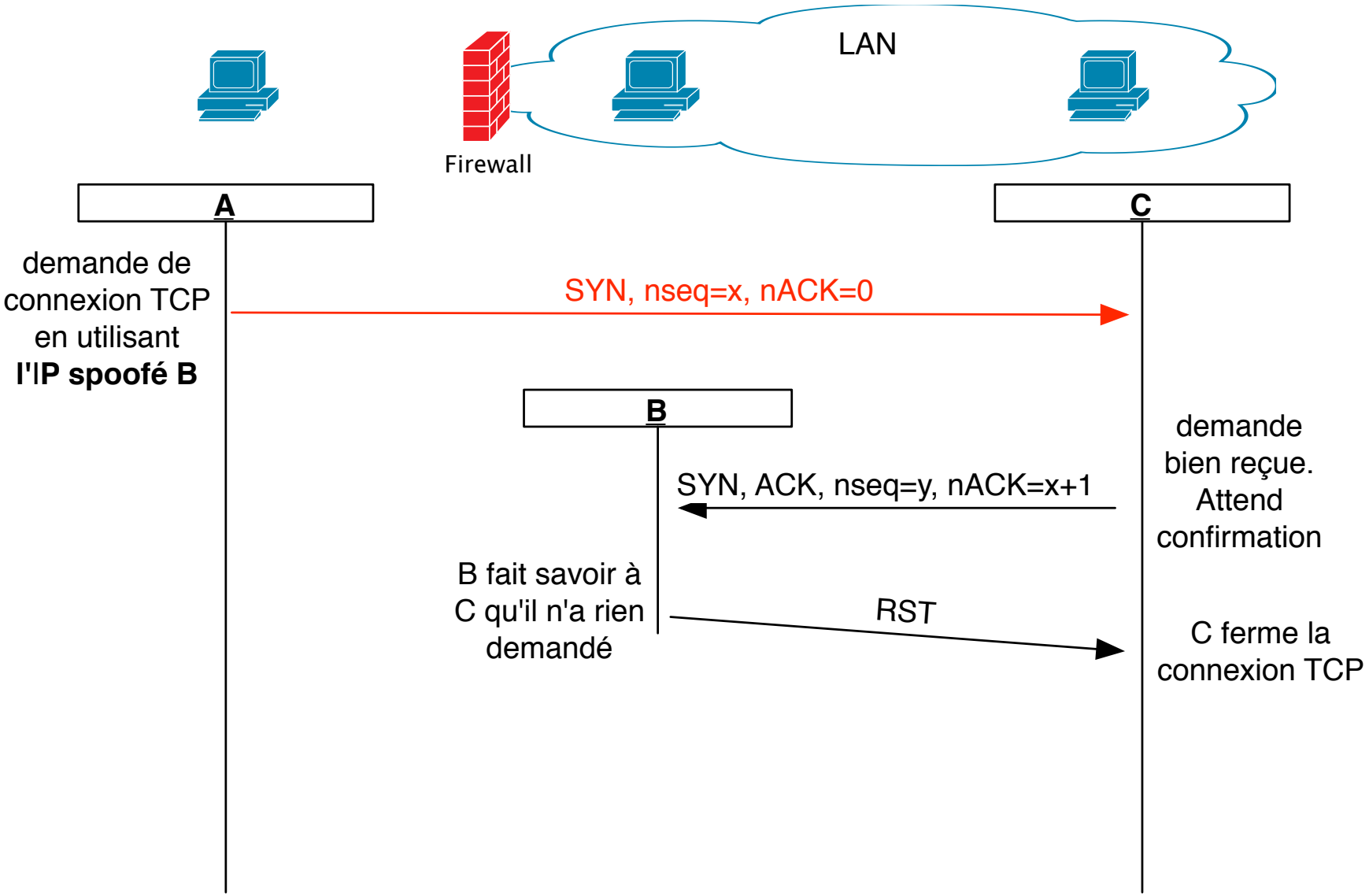
- l'option "based routing" permet de spécifier la route que doit suivre le paquet
- l'option "record route" permet d'enregistrer la route qu'a suivi le paquet

☞ Usurpation de l'adresse IP :

- cette technique consiste à contrefaire l'adresse source d'un paquet IP.
- les communications ne peuvent avoir lieu que de l'attaquant vers l'attaqué. (sauf si le sniffing est possible, l'option source routing est active, ou les tables de routage ont été modifiées).

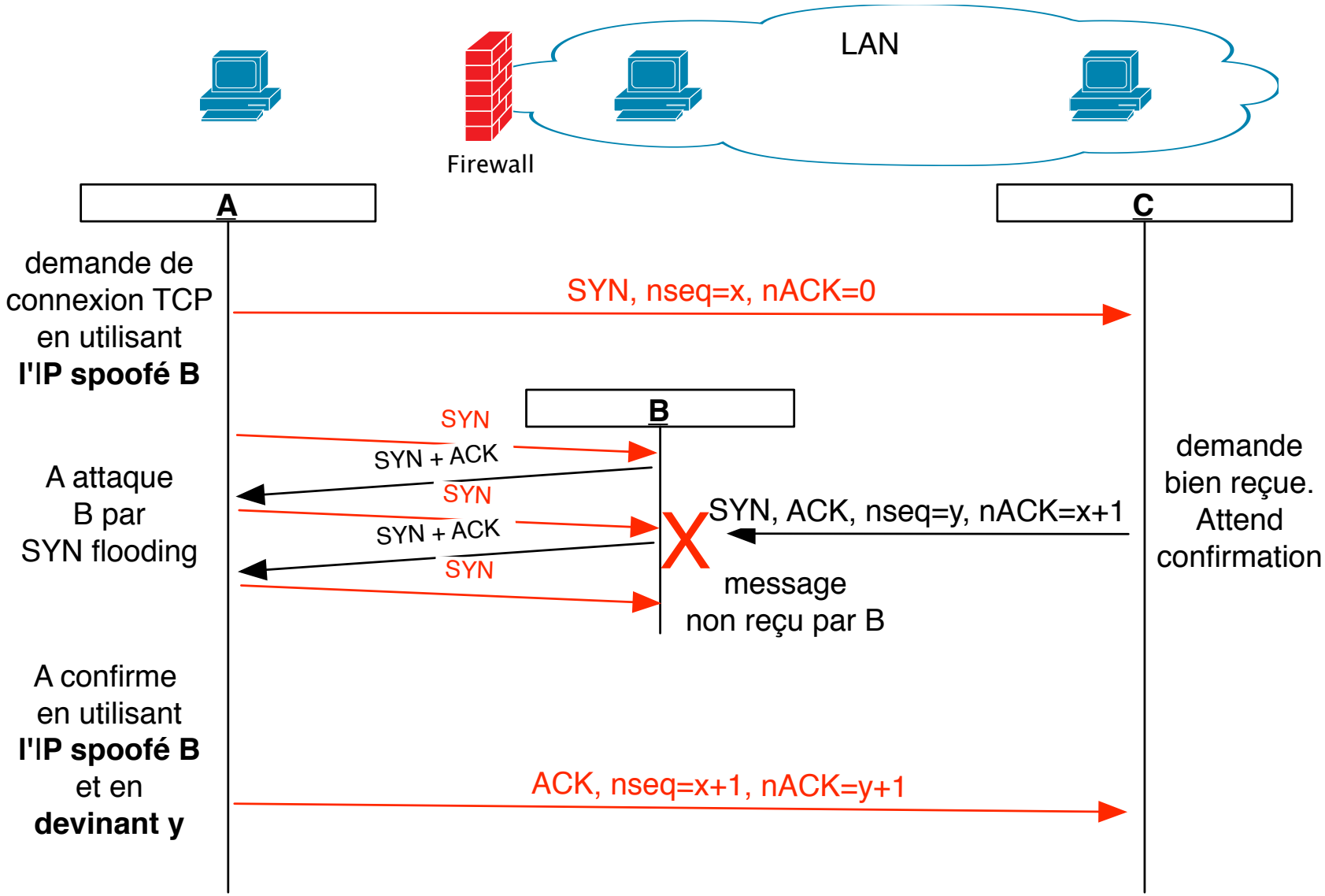
Rappels sur TCP (encore) – le message RST

esil



Blind spoofing

esil



Blind spoofing (suite et fin)

esil

☞ Prédiction des numéros de séquence TCP :

- à chaque paquet TCP est associé un numéro de séquence initiale.
- Suivant l'implémentation de la pile TCP/IP, ce nombre est généré en fonction du temps, de manière linéaire ou de manière pseudo-aléatoire.

➥ cette attaque est possible uniquement si les numéros de séquence sont prévisibles (génération linéaire ou dépendante du temps).

Plan

1 SYN Flooding

2 UDP Flooding

3 Attaque par fragmentation

4 Attaque par ICMP

5 ARP Poisoning

6 DNS Spoofing

7 Blind spoofing

8 TCP Hijacking

Fiche technique

esil

☞ Principe : technique utilisée pour s'insérer au milieu d'une connexion entre deux hôtes. Cette attaque utilise

- du sniffing : l'attaquant doit pouvoir reniffler les paquets émis par les deux hôtes
- de l'IP spoofing,
- la désynchronisation d'une connexion TCP,
- le SYN flooding.

☞ Conséquences :

- attaque du type man in the middle ;
- Cette attaque fonctionne même dans le cas d'une authentification sécurisée.

☞ Se protéger :

- empêcher ou limiter le sniffing ;
- vérifier la présence de la signature de l'attaque.

Rappels sur TCP – désynchronisation

esil

☞ Qu'est-ce ? Quand le numéro de séquence d'un paquet reçu n'est pas le même que celui attendu, la connexion est dite désynchronisée. Dans ce cas la couche TCP du destinataire peut :

- stocker ce paquet dans son buffer ;
- l'ignorer et signaler une erreur à l'émetteur (envoi d'un ACK avec le numéro de séquence attendu) ;
- l'ignorer complètement.

☞ Quand peut-on provoquer la désynchronisation dans TCP :

- pendant la phase de connexion en trois temps ;
- une fois la connexion établie.

☞ Remarque : Si les deux hôtes sont désynchronisés et s'ils signalent l'erreur par des ACKs, alors un très grand nombre de ACKs va avoir lieu dans le réseau. Cela constitue souvent la signature d'une attaque par TCP Hijacking

TCP Hijacking – Principe

esil