



Dénis de Service et usurpation d'identité

par BALLAN Emilie et SURANGKANJANA JAI Gaëtan

disponible en ligne : <http://www.e-eck.org/>



UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE



PLAN

- Introduction
- Déniis de service:
 - Tcp Syn
 - Land
 - Teardrop
 - Smurf
 - Ping de la mort
- Vol de session:
 - Tcp hijacking



INTRODUCTION



LOI

- Article 323-1 - Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende.



LOI

- Article 323-2 - Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

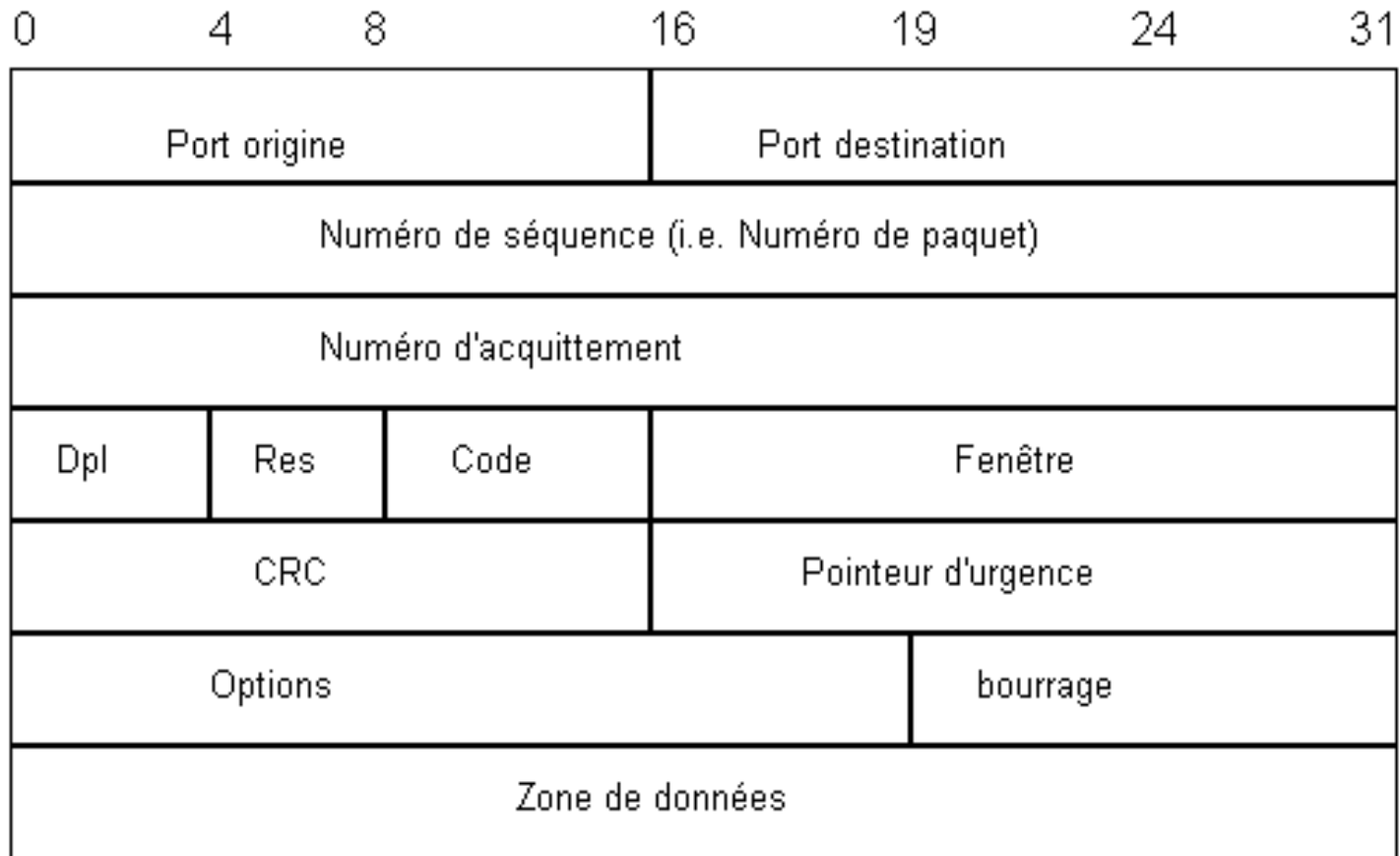


INTRODUCTION

[Rappel sur TCP/IP]

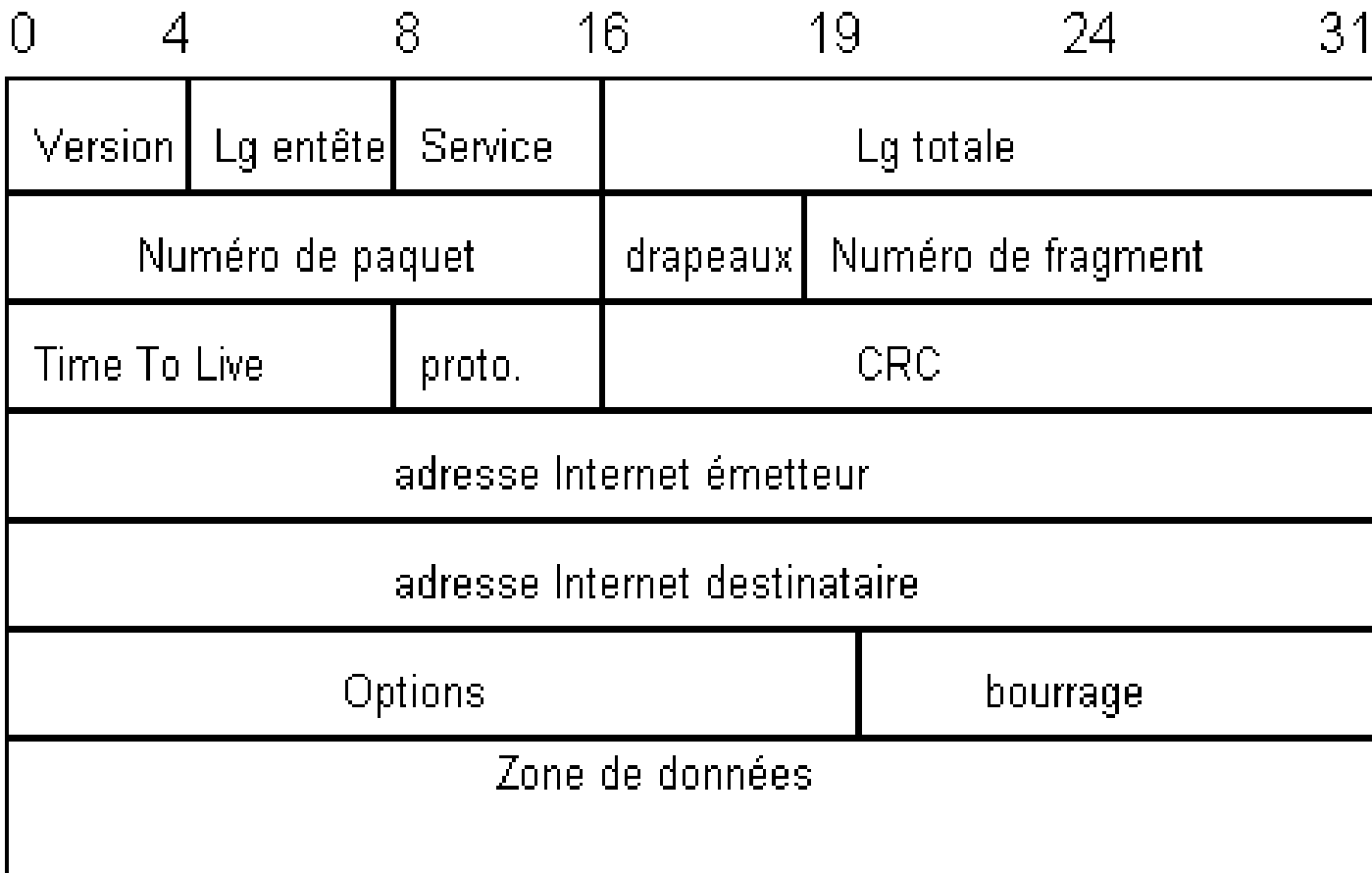


Rappel : trame TCP





Rappel : trame IP





DoS



Dénis de service

ou Deny of Service (DoS)

2 types:

- DoS : attaque venant d'une seule machine
- DDoS (Distributed Denial of Service):
attaque provenant de plusieurs machines



Dénis de service

exploitent plusieurs méthodes

- utilisation de ressources (cycles CPU, mémoire)
- consommation de la bande passante (bloquage du trafic réseau)
- faille de programmation (faille dans l'implémentation de la pile TCP/IP ..)
- routage et attaques sur les DNS (non étudié ici)



Cibles

Cas connus:

- 7 février 2000 : Yahoo, eBay, Amazon, CNN ..
- 21 octobre 2002 : attaque contre les serveurs de noms racines
- 2004 : extorsion de fond des sites de jeux en lignes (genre casino, poker..)



Cibles

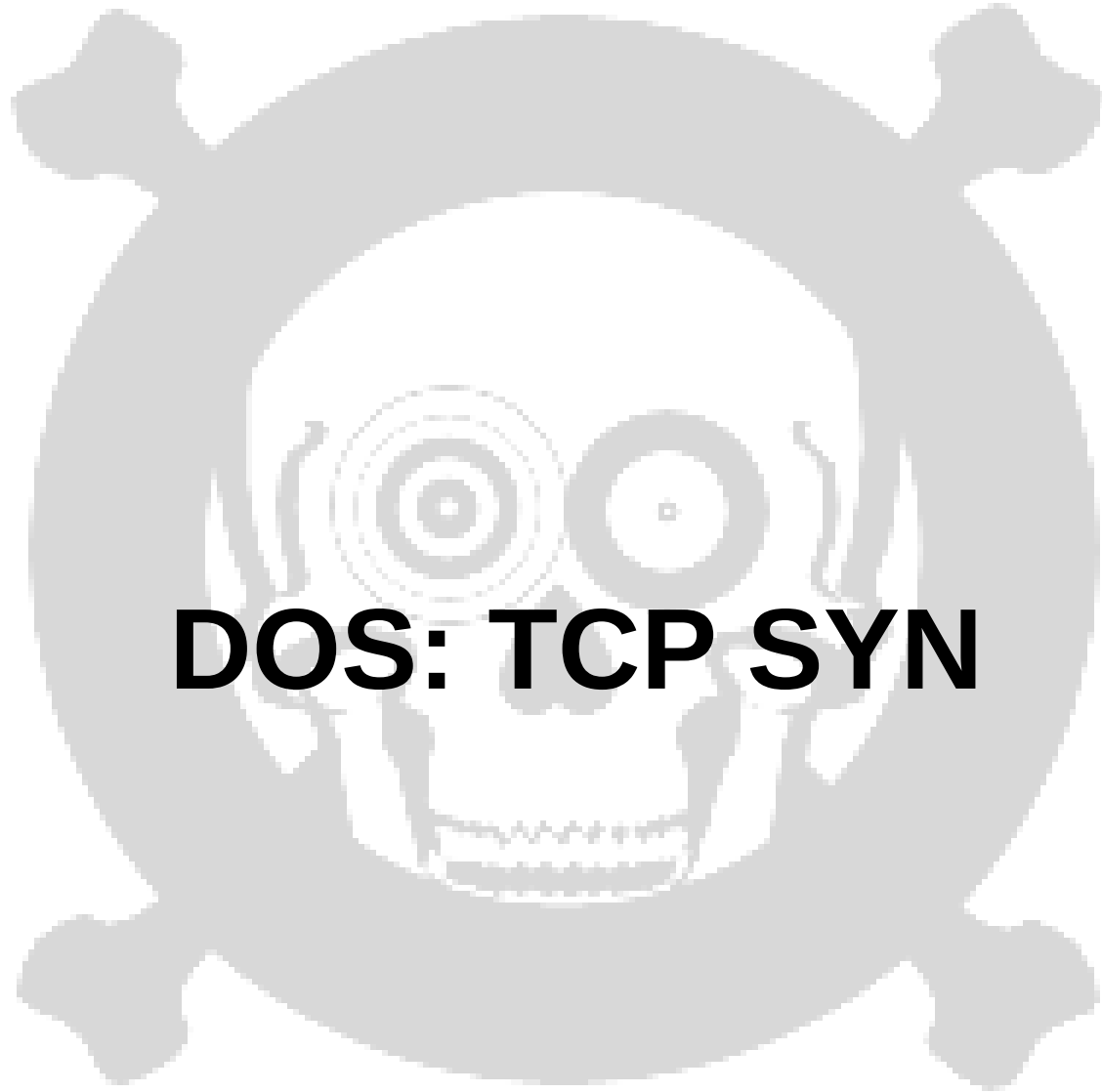
Rapport du CSI/FBI Computer Crime & Security Survey en 2007 :

- 25% des entreprises interrogées subissent des DoS
- Pertes évaluées à 2,8 millions de dollars



Intérêts du DoS

- Revanche
- Extorsion de fond
- ...



DOS: TCP SYN



Principe

Exploite le protocole d'initialisation de connexion TCP

Envoi d'un grand nombre de paquets SYN vers la cible (mais pas de ACK)

La cible initie l'ouverture d'un nombre important de connexions (état: à moitié ouverte)



Principe

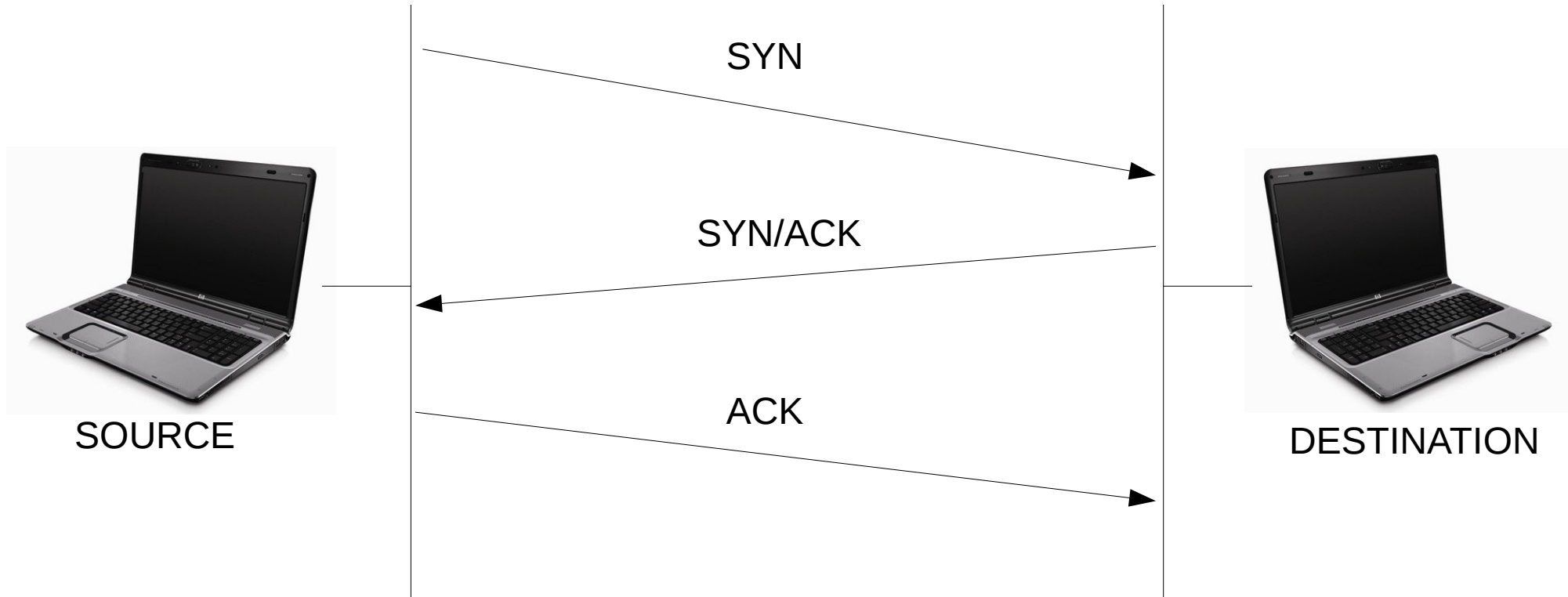
Mais le nombre de connexions à moitié ouvertes est limité !

=> la cible ne peut plus ouvrir de connexions



Détails

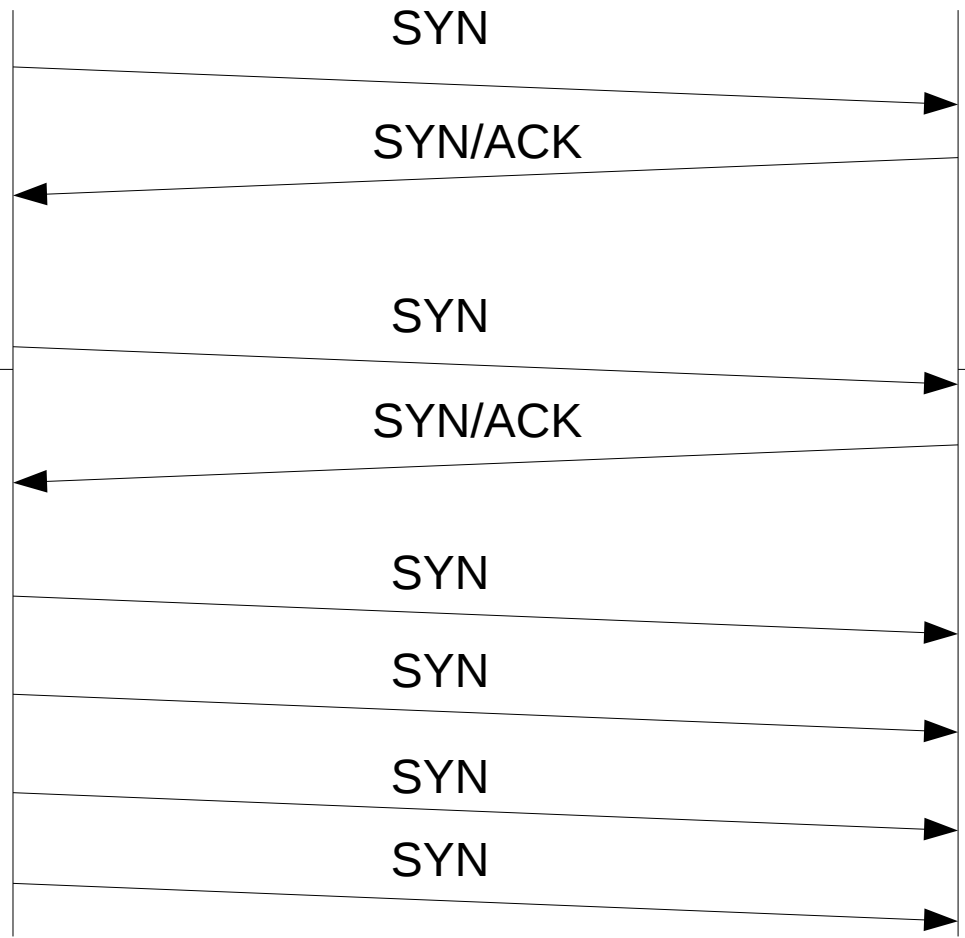
Rappel : 3 Way HandShake





Détails

Attaque SYN



Queue TCP pleine:
ne répond plus aux
demandes de
connexion



Mise en oeuvre

génération de paquet SYN avec la librairie dpkt

Connexion au serveur
telnet avant attaque
SYN

```
thaifooff@ubuntu-server:~$ telnet 192.168.1.14
Trying 192.168.1.14...
Connected to 192.168.1.14.
Escape character is '^]'.
Ubuntu 6.06.1 LTS
ubuntu-server login: thaifooff
Password:
Last login: Sun Jan 20 14:28:28 2008 on tty1
Linux ubuntu-server 2.6.15-26-server #1 SMP Thu Aug 3 04:09:15
~/Linux

The programs included with the Ubuntu system are free software
the exact distribution terms for each program are described in
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permit
applicable law.
thaifooff@ubuntu-server:~$ exit
logout
Connection closed by foreign host.
thaifooff@ubuntu-server:~$ telnet 192.168.1.14
Trying 192.168.1.14...
```

Nouvelle connexion
impossible pendant le
DoS SYN



Protection

- Comment détecter une attaque SYN ?

un grand nombre de connexions sont dans l'état à demi-ouverte (SYN_RECEIVED)

```
# netstat -n -p TCP
tcp    0    0 192.168.1.14:23      237.177.154.8:25882  SYN_RECV -
tcp    0    0 192.168.1.14:23      236.15.133.204:2577  SYN_RECV -
tcp    0    0 192.168.1.14:23      127.160.6.129:51748  SYN_RECV -
tcp    0    0 192.168.1.14:23      230.220.13.25:47393  SYN_RECV -
tcp    0    0 192.168.1.14:23      227.200.204.182:60427 SYN_RECV -
tcp    0    0 192.168.1.14:23      232.115.18.38:278    SYN_RECV -
tcp    0    0 192.168.1.14:23      229.116.95.96:5122   SYN_RECV -
{...}
```



Protection

- Se protéger sous Windows (2000,XP,2003)

SynAttackProtect

Mise en place de la protection :

Ajout de la valeur DWORD SynAttackProtect dans
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters



Protection

Modifie le comportement de la pile TCP/IP

- OS supporte plus de requêtes SYN
- désactive certaines options des sockets
- ajoute des délais pour les indications de connexions
- modifie le timeout des requêtes de connexion



Protection

- Se protéger sous Linux

SYN cookies

Mise en place de la protection :

```
# echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

Remarque : nécessite que le noyau ait été compilé avec l'option
CONFIG_SYNCOOKIES



Protection

Crée un paquet avec les drapeaux SYN et ACK ainsi qu'un numéro de séquence initiale spécifique (le cookie)

La valeur du cookie est le résultat d'une fonction de hachage (sur différentes informations: adresse source, ports, .. ainsi que sur des valeurs secrètes)



Protection

Mécanisme (pendant une attaque SYN):

- génère une réponse avec le cookie (au lieu de rejeter la connexion)
- vérifie le cookie à la réception du ACK (terminant le 3-WAY HANDSHAKE)
- crée la connexion après vérification de la valeur



DOS: LAND



Principe

- Première attaque en octobre 1997
- Tire son nom de land.c (exploit)
- Consiste à démarrer une connexion TCP sur un port ouvert de la cible
- Usurpation de l'adresse IP
- Dans la trame on modifie :
 - IP destination = IP source = IP de la cible
 - Port destination = Port source = Port de la cible



Principe

- Conséquences : La cible pense discuter avec elle même => boucle
- Quelques systèmes vulnérables :
 - windows 95/2003/XP SP2



Détails



10.0.0.3

nmap



10.0.0.6

Récupération des ports ouverts



Détails

Le port 80 est ouvert, on lance l'attaque dessus



10.0.0.3

SYN
IP source = 10.0.0.6
IP dest = 10.0.0.6
PORT source = 80
PORT dest = 80



10.0.0.6



Détails

La cible tourne en boucle



10.0.0.3



10.0.0.6



Mise en oeuvre

- Démonstration avec Windows 95
- Script python réalisé avec la librairie dpkt



Protection

- Bloquer les paquets ayant la même source et destination
- Se protéger de l'IP spoofing
- Beaucoup de firewall la détecte



DOS: TEARDROP



Principe

Exploite le principe de fragmentation du protocole IP

Insertion, dans des paquets fragmentés,
d'informations de décalage erronées

=> Provoque le crash des systèmes vulnérables
qui ne réassemblent pas correctement les
paquets



Détails

Rappel:

Le protocole IP fragmente les paquets de taille importante en plusieurs paquets IP possédant chacun un numéro de séquence et un numéro d'identification commun.

A réception des données, le destinataire réassemble les paquets grâce aux valeurs de décalage qu'ils contiennent.



Détails

Attaque Teardrop

Envoi d'un paquet fragmenté



id=1 offset=0 flag=more fragment

id=1 offset=1400 flag=more fragment

id=1 offset=3000 flag=more fragment

id=1 offset=4500 flag=more fragment

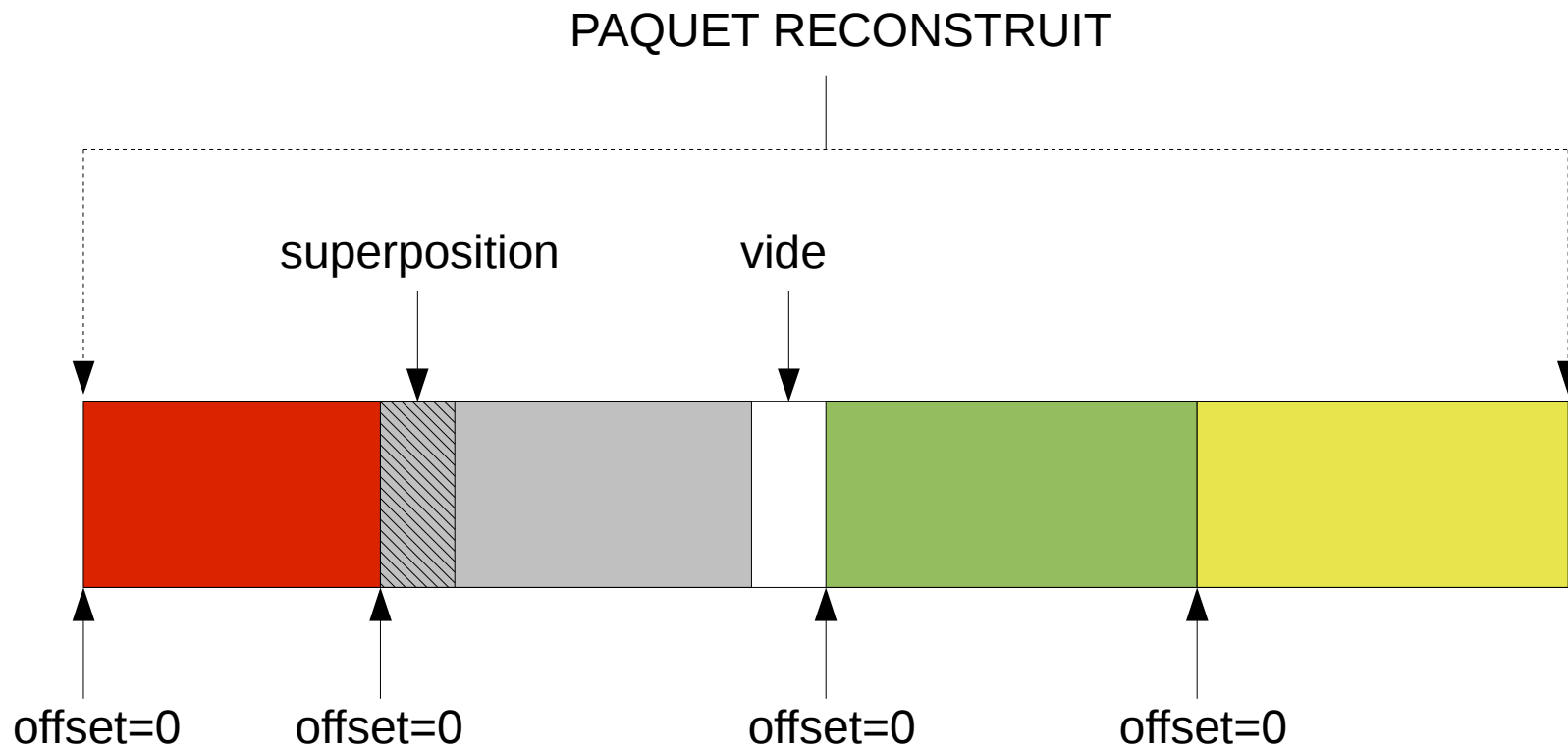


→ Fragment



Détails

Réception et reconstruction du paquet





Mise en oeuvre

Démonstration avec la librairie dpkt



Protection

- Gestion de ces paquets dans l'implémentation de la pile TCP/IP



DOS: SMURF



Principe

- Apparition de l'attaque en juillet 97
- Envoi d'une trame à destination d'un broadcast réseau un ping par exemple
- IP de la cible = IP source
- Le flux de réponse est envoyé sur la cible



Détails

10.0.0.0



▲ PING 10.0.0.255
IP source = 10.0.0.6



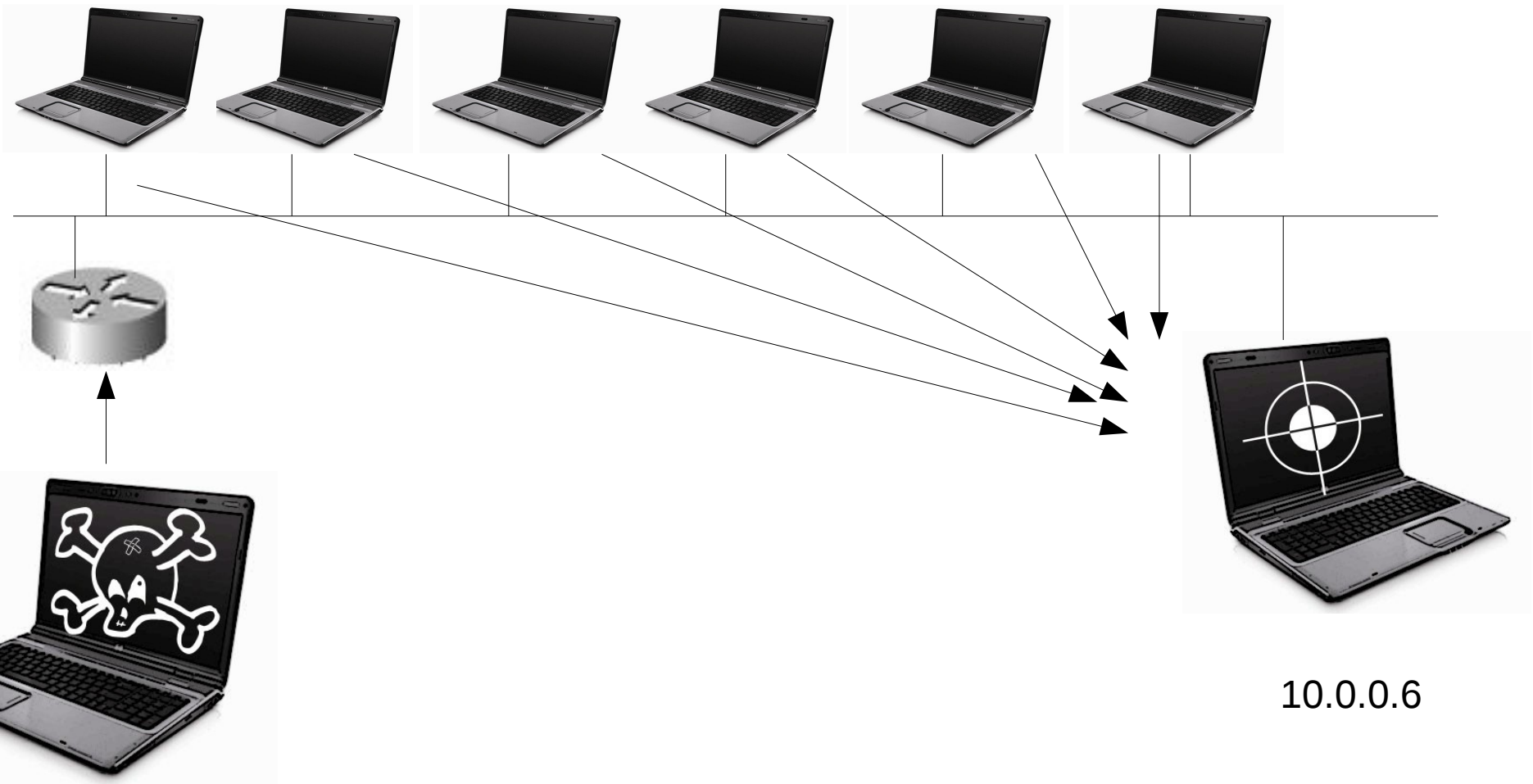
10.0.0.6





Détails

10.0.0.0



10.0.0.6



Mise en oeuvre

eth0: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Effacer Appliquer

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.253.254	172.16.255.255	ICMP	Echo (ping) request
2	0.000293	172.16.0.250	172.16.253.254	ICMP	Echo (ping) reply
3	0.000301	172.16.110.86	172.16.253.254	ICMP	Echo (ping) reply
4	0.000369	172.16.255.255	172.16.0.250	ICMP	Echo (ping) request
5	0.001047	172.16.110.96	172.16.0.250	ICMP	Echo (ping) request
6	0.001282	172.16.3.5	172.16.0.250	ICMP	Echo (ping) request
7	0.001722	172.16.110.74	172.16.0.250	ICMP	Echo (ping) request
8	0.001971	172.16.3.1	172.16.0.250	ICMP	Echo (ping) request
9	0.002024	172.16.3.2	172.16.0.250	ICMP	Echo (ping) request
10	0.002462	172.16.3.3	172.16.0.250	ICMP	Echo (ping) request
11	0.004566	172.16.0.233	172.16.0.250	ICMP	Echo (ping) request

capture1.png - KSnapshot <2>

Nouvelle capture

Enregistrer sous...

Copier vers le presse-papiers

Imprimer...

Mode de capture : Plein écran

Délai de capture : Aucun délai

Inclure la décoration des fenêtres

Aide Quitter

▸ Frame 1 (46 bytes on wire, 46 bytes captured)

▸ Ethernet II, Src: Vmware_f5:7e:55 (00:0c:29:f5:7e:55), Dst: 01:00:5e:00:00:01

▸ Internet Protocol, Src: 172.16.253.254 (172.16.0.254), Dst: 172.16.0.250

▸ Internet Control Message Protocol

```
0000 ff ff ff ff ff ff 00 0c 29 f5 7e 55 08 00 45 00 ..... )~U..E.
0010 00 20 00 00 00 00 40 01 24 be ac 10 fd fe ac 10 .....@. $......
0020 ff ff 08 00 75 01 00 7b 00 01 41 41 41 41 .....u..{ ..AAAA
```

eth0: <live capture in progress> File: /root/tmp/etherXXXXQm5BL1 846 Bytes Packets: 11 Displayed: 11 Marked: 0

Menu

ASR - Konc En chantie emilie@lo Windows 9 eth0: Capt NEdit [2] Ksnaps

18:02



Protection

- Bloquer le ping sur le firewall



DOS: Ping of Death



Principe

- Envoi d'un message ping
- Caractéristiques de ce message :
 - Longueur des données supérieure à celle autorisée (65536)
 - Le message est fragmenté
- Conséquences :
 - La cible doit réassembler le message
 - La taille du buffer est dépassée
 - Plantage de la cible



Détails



10.0.0.3



10.0.0.6

Message Ping

taille > 56536

dest = 10.0.0.6



Détails



10.0.0.3



10.0.0.6

Message Ping			
taille > 56536			
dest = 10.0.0.6			

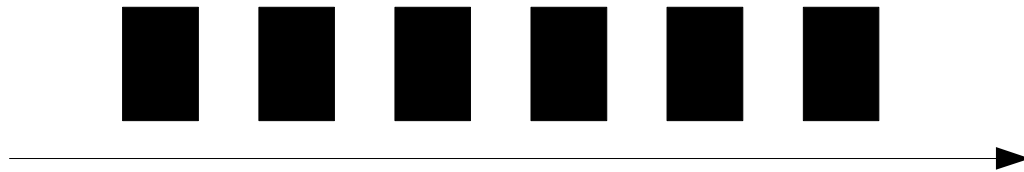
Le message est fragmenté



Détails



10.0.0.3



10.0.0.6

Envoi des fragments du message

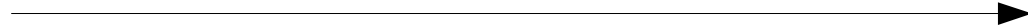


Détails

La cible reassemble les morceaux reçus dans un buffer



10.0.0.3



10.0.0.6

Buffer de la cible



dépassement du buffer :
crash



Mise en oeuvre

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Effacer Appliquer

No.	Time	Source	Destination	Protocol	Info
88	32.286330	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=0)
89	32.304076	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=1480)
90	32.322236	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=2960)
91	32.337873	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=4440)
92	32.350132	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=5920)
93	32.367572	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=7400)
94	32.384827	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=8880)
95	32.398171	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=10360)
96	32.414008	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=11840)
97	32.430855	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=13320)
98	32.448296	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=14800)
99	32.460034	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=16280)
100	32.477935	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=17760)
101	32.491957	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=19240)
102	32.508875	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=20720)
103	32.524060	172.16.253.253	172.16.253.254	IP	Fragmented IP protocol (proto=ICMP 0x01, off=22200)

▶ Frame 168 (1514 bytes on wire, 1514 bytes captured)

▶ Ethernet II, Src: HewlettP_5e:8c:fe (00:1a:4b:5e:8c:fe), Dst: Vmware_f5:7e:55 (00:0c:29:f5:7e:55)

▶ Internet Protocol, Src: 172.16.253.253 (172.16.253.253), Dst: 172.16.253.254 (172.16.253.254)

▶ Data (1480 bytes)

```
0000 00 0c 29 f5 7e 55 00 1a 4b 5e 8c fe 08 00 45 00  ..).~U.. K^....E.
0010 05 dc 00 01 3c 2f 40 01 e4 d3 ac 10 fd fd ac 10  ...</@. ....
0020 fd fe 58 58 58 58 58 58 58 58 58 58 58 58 58 58  ..XXXXXXXXXXXXXXXX
0030 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58  XXXXXXXXXXXXXXXXXXXX
0040 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58  XXXXXXXXXXXXXXXXXXXX
```

Frame (frame), 1514 bytes

Packets: 174 Displayed: 174 Marked: 0 Dropped: 0

Menu

ARS - Kon DOS-Usur emilie@lo Windows (Untitled) scapy_pa littleschri 14:07



Protection

- Bloquer le ping
- Vérifier la taille des paquets



USURPATION D'IDENTITE:
TCP HIJACKING
(vol de session TCP)



Principe

Intercepter une connexion TCP établie

Se faire passer pour l'une des parties (spoofing)

Injecter des données dans le flux de communication



Intérêt du TCP Hijacking

- outrepasser une authentification par mot de passe
- se faire passer pour un serveur



Principe

2 manières de mettre en place cette attaque:

- Man-in-the-middle
- Blind Attack

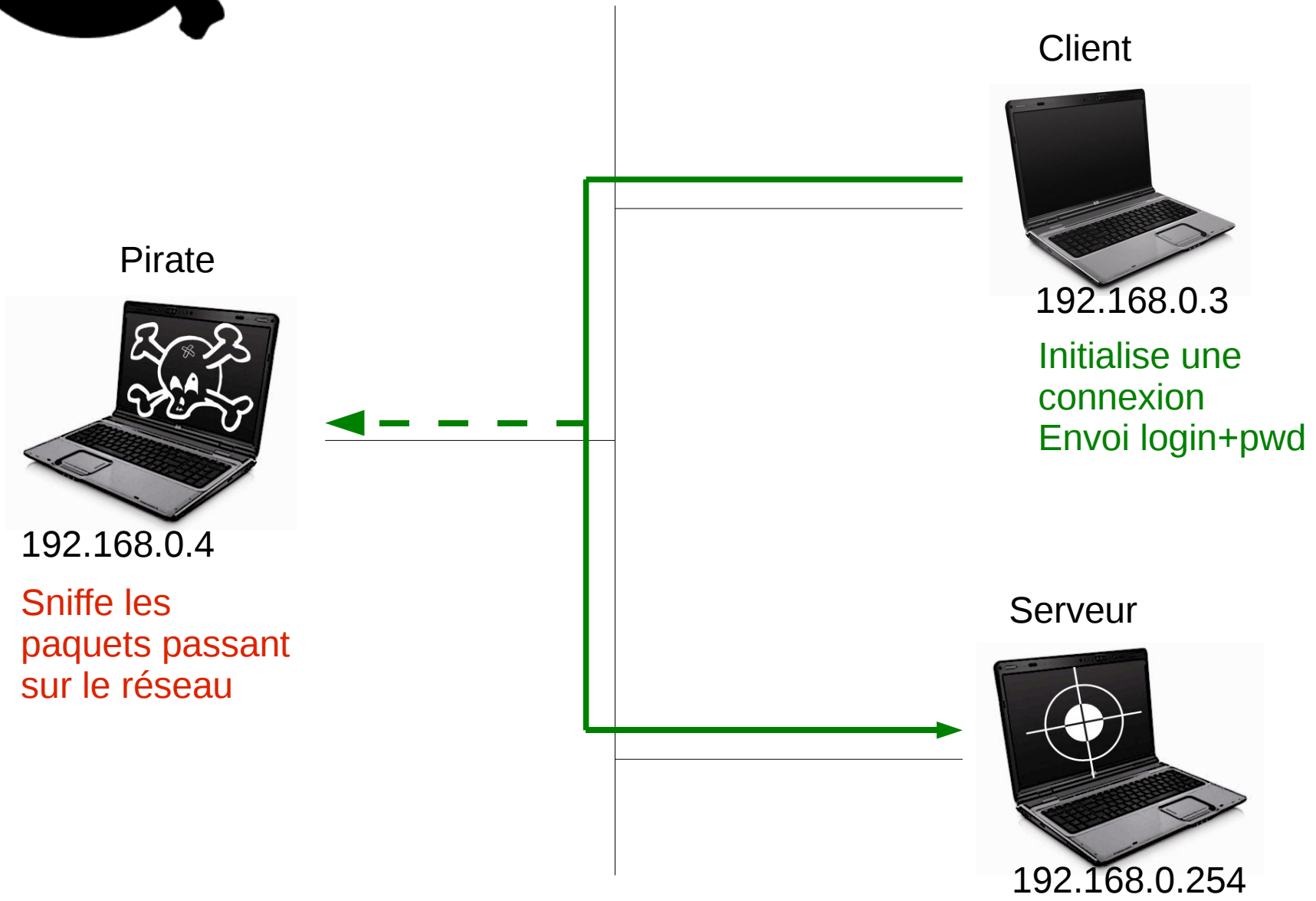


Principe [Man-in-the-Middle]

- Sniffer
 - > récupération des entêtes TCP
 - > connaissance du numéro de séquence attendu, numéro de l'accusé, port et numéro de protocole
- Forger le paquet avant le client (ou empêcher le client de répondre)



Détails [Man-in-the-Middle]





Détails [Man-in-the-Middle]



Sniffe les
paquets passant
sur le réseau



Login+pwd OK
Début de
session



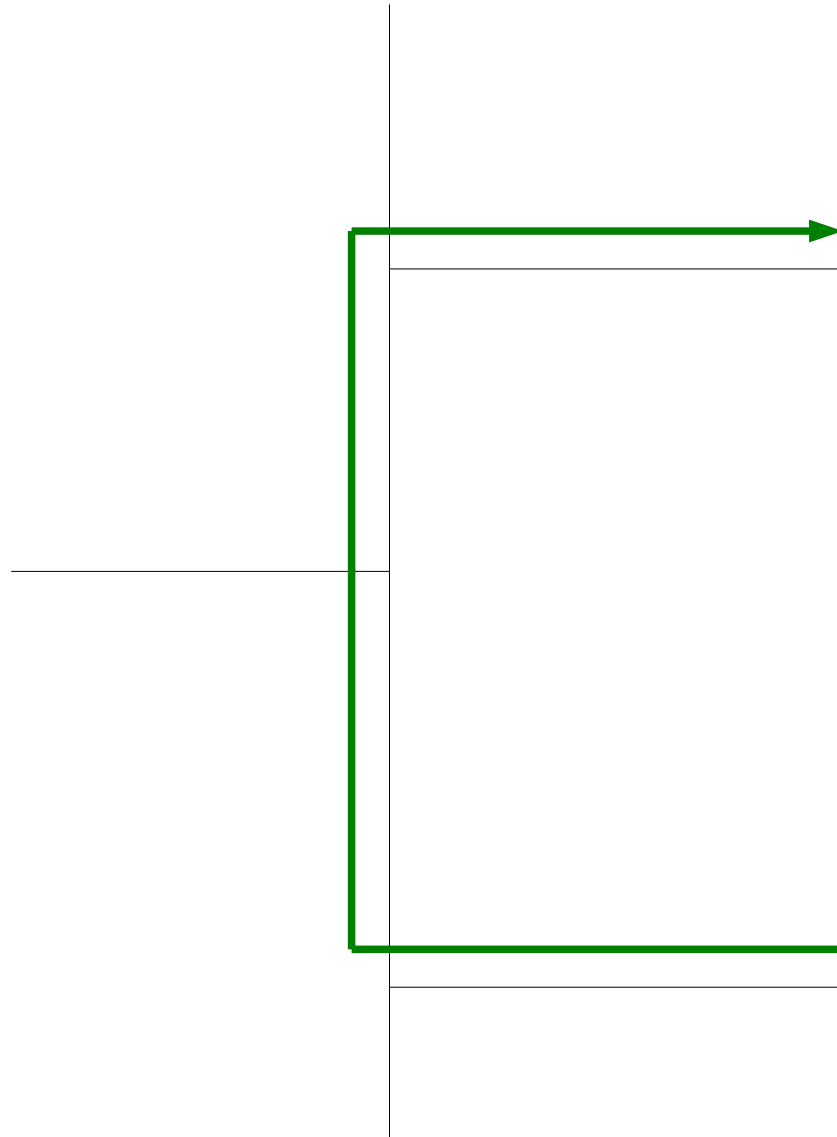
Détails [Man-in-the-Middle]



Sniffe les
paquets passant
sur le réseau



Login+pwd OK
Début de
session





Détails [Man-in-the-Middle]

Le pirate a intercepté les paquets transitant sur le réseau.

Il a donc en sa possession:

- prochain numéro de séquence attendu



Détails [Man-in-the-Middle]

Il doit donc répondre à la place du client.

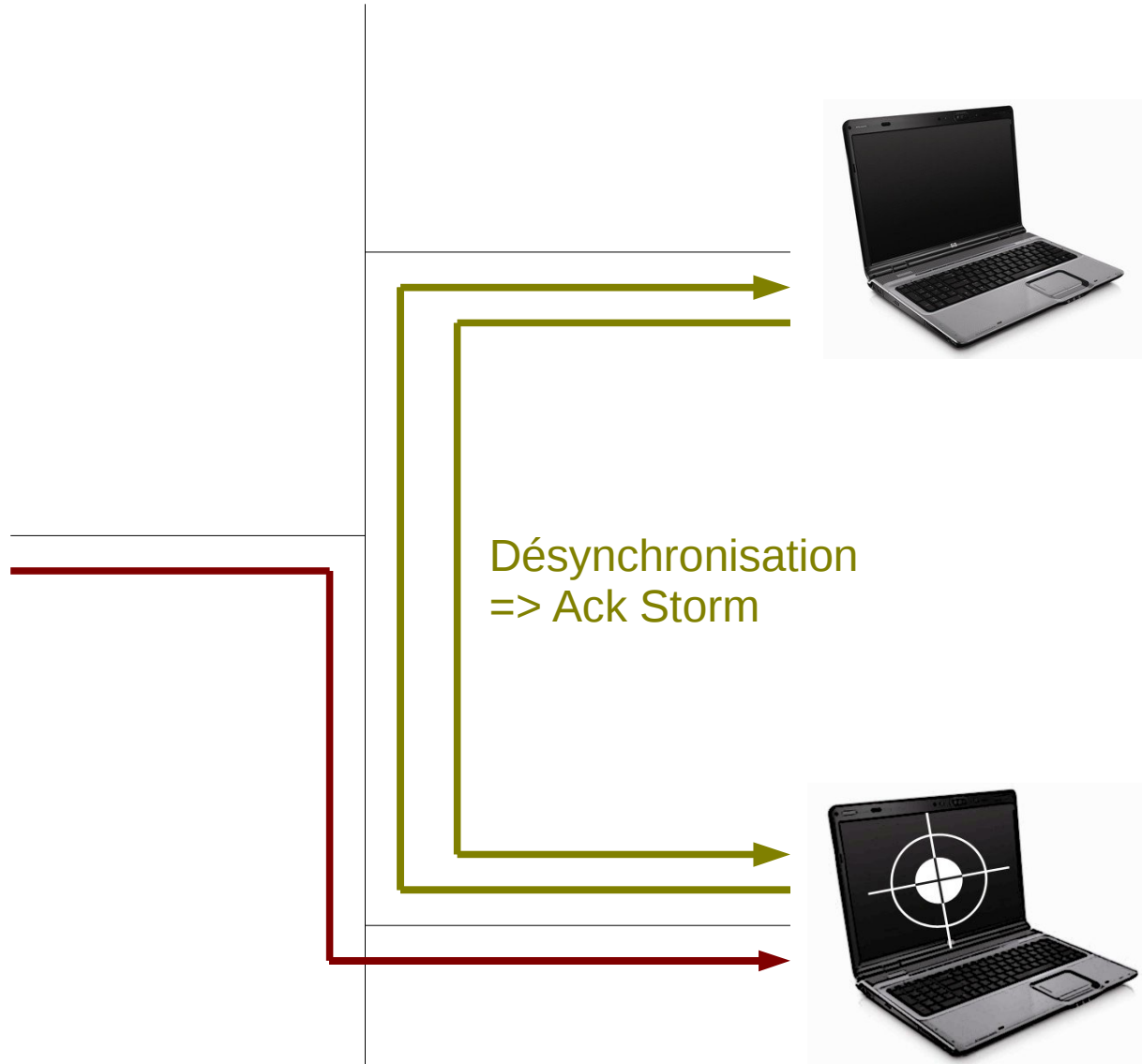
- Possibilité de mettre le client hors-service(avec un DoS par exemple)
- Désynchroniser le client/serveur (en fonction du but)
- Mise en place de l'IP SPOOFING (avec si nécessaire un ARP poisoning/relaying)
- Forger les paquets



Détails [Man-in-the-Middle]



Envoi de paquet
provoquant la
désynchronisation





Détails [Man-in-the-Middle]



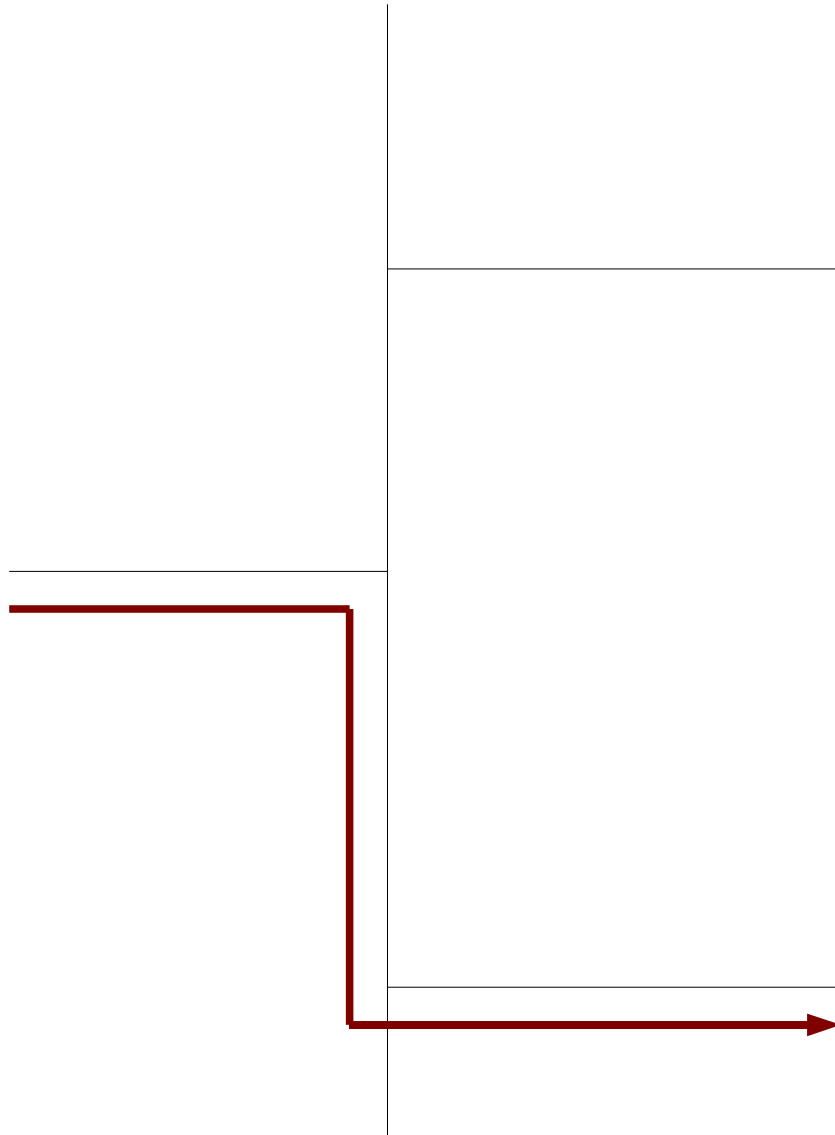
Synchronisation
avec le pirate



Détails [Man-in-the-Middle]



Connexion volée,
envoi de données





Mise en oeuvre

- Outils : Hunt, Juggernaut, P.A.T.H

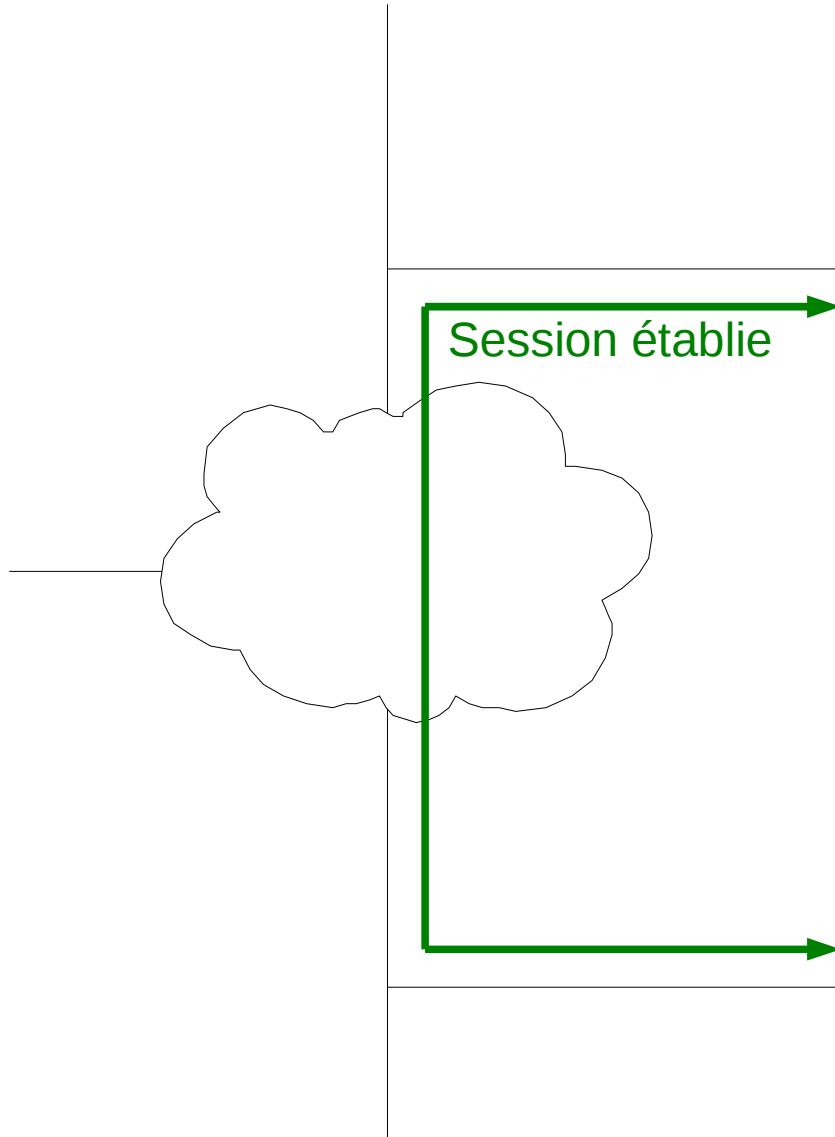


Principe [Blind Attack]

- Trouver le port du client (aléatoire)
- Deviner le numéro de séquence (peu de systèmes récents vulnérables)
- Injecter des données



Détails [Blind Attack]

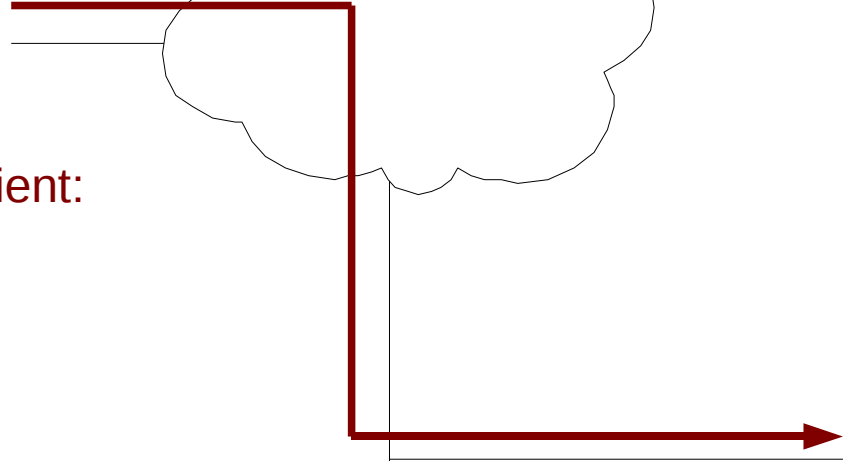
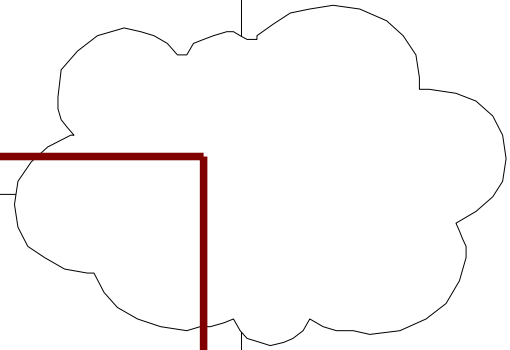




Détails [Blind Attack]

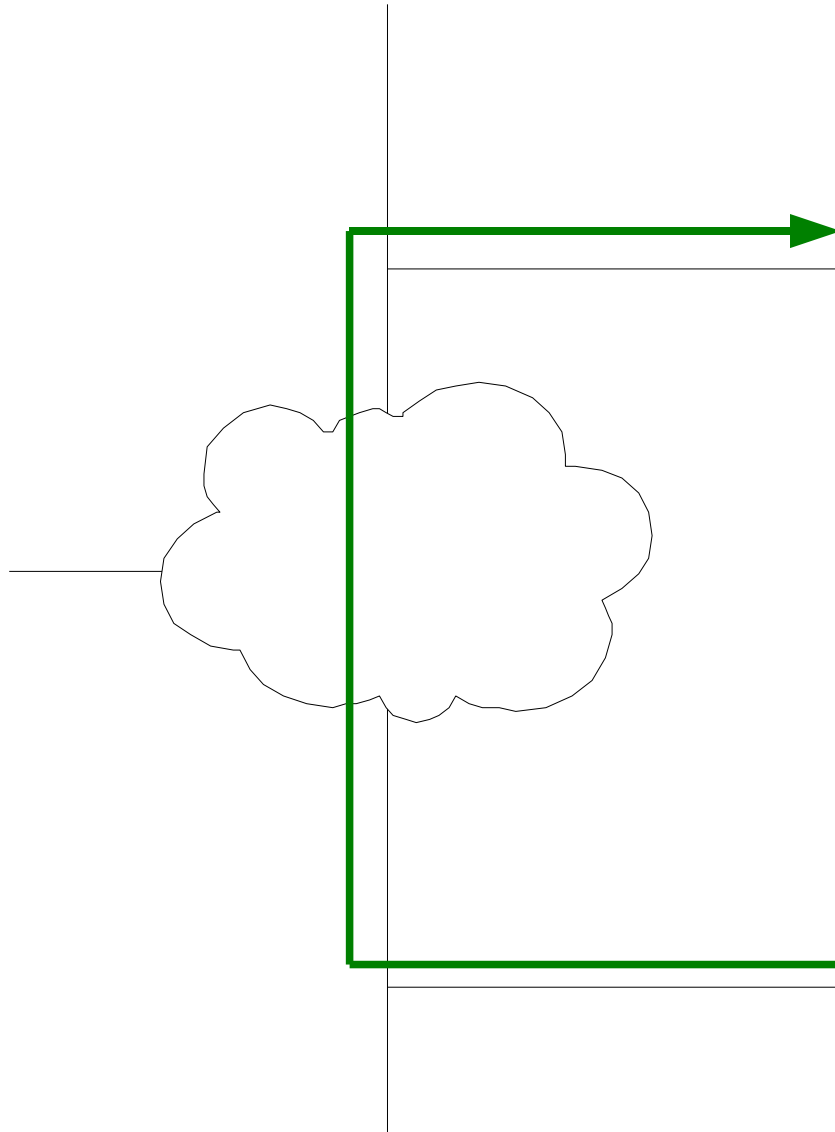


Découverte du port client:
Envoi un paquet SYN
'spoofé'





Détails [Blind Attack]



Réponse au client par un ACK



Détails [Blind Attack]

- Trouver le port du client :
 - Envoi d'un ping sur le client
 - Envoi du paquet SYN spoofé
 - Envoi d'un nouveau ping sur le client
 - Comparaison des numéros de séquences récupérés lors des pings précédents



Détails [Blind Attack]

Il reste ensuite à deviner le prochain numéro de séquence du client ;p

-> utilisation de la technique pour trouver le port

-> $(\text{guessed_ACK} - \text{SND.NEXT}) \leq 0$



Protection

- Générateur de nombres pseudos aléatoires pour la génération des ISN (initial sequence number)
- Crypter les communications

Références

Hardening the TCP/IP stack to SYN attacks, *Mariusz Burdach* [<http://www.securityfocus.com/infocus/1729>]

Blind TCP/IP hijacking is still alive, *Phrack* [<http://www.phrack.org/issues.html?issue=64&id=15>]

Simple Active Attack Against TCP, *Laurent Joncheray* [<http://insecure.org/stf/iphijack.txt>]

Session Hijacking Packet Analysis, *Lee Lawson* [<http://www.securitydocs.com/library/3479>]

TCP Exploits, *Prabhaker Mateti* [<http://www.cs.wright.edu/~pmateti/Courses/499/TCPexploits/>]

Séminaire de détection d'intrusions Dos, Ddos Attaque du Syn Flooding, *Yannick BLEUWART, Éric FAGOT, Grégory GIEMZA et Yanick PIGNOT* [<http://www.student.montefiore.ulg.ac.be/~bleuwart/>]

Attaques - Attaque par fragmentation [<http://www.commentcamarche.net/attaques/attaque-teardrop.php3>]

Les attaques externes [<http://www.linux-pour-lesnuls.com/attack.php>]

2006 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY [http://americas.utimaco.com/encryption/fbi_csi_2006_p3.html]

Logiciels et bibliothèques utilisés et cités

- DPKT [<http://code.google.com/p/dpkt/downloads/list>]
- NMAP [<http://nmap.org/>]
- HPING [<http://www.hping.org/>]
- HUNT [<http://lin.fsid.cvut.cz/~kra/index.html>]
- P.A.T.H [<http://p-a-t-h.sourceforge.net/>]
- Juggernaut [?]

