SSTIC
10 - 12 juin 2003 À RENNES
Supélec - École Supérieure d'électricité

O. Courtay

O. Heen

F. Veysset

Détection des systèmes d'exploitation avec **Cron-OS**

ENST Bretagne
THOMSON
france telecom R&D

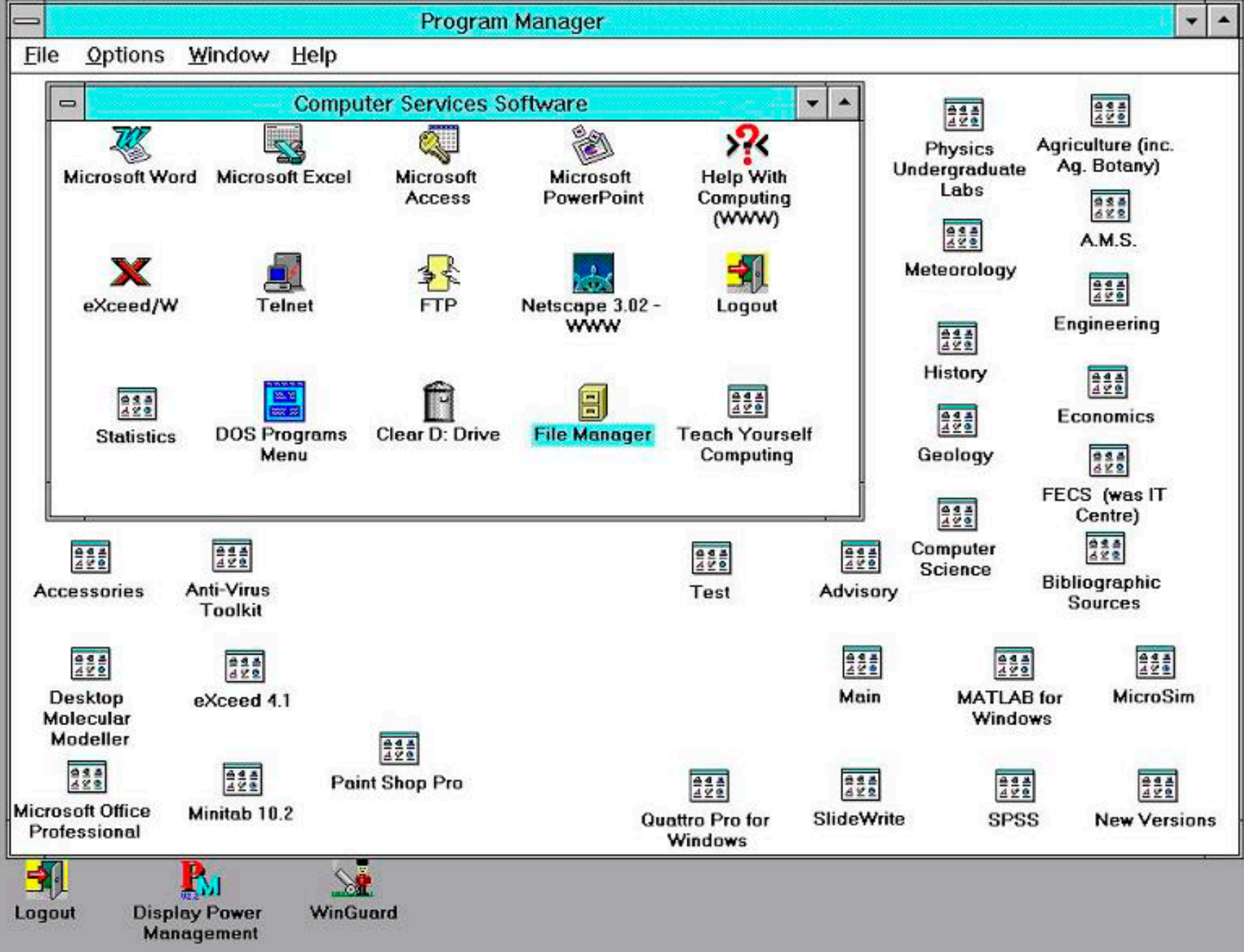
Utilité

Pourquoi reconnaître des OS ?

- Auditer des configurations
- Administrer un parc
- Aider d'autres logiciels

Mais aussi...

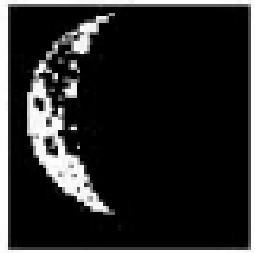
- Savoir ce que *voient* les pirates
- Fabriquer de meilleurs leurres


Program Manager
File Options Window Help
Computer Services Software
Microsoft Word
Microsoft Excel
Microsoft Access
Microsoft PowerPoint
Help With Computing (WWW)
eXceed/W
Telnet
FTP
Netscape 3.02 - WWW
Logout
Statistics
DOS Programs Menu
Clear D: Drive
File Manager
Teach Yourself Computing
Physics Undergraduate Labs
Agriculture (inc. Ag. Botany)
A.M.S.
Meteorology
Engineering
History
Economics
Geology
FECS (was IT Centre)
Computer Science
Bibliographic Sources
Accessories
Anti-Virus Toolkit
Test
Advisory
Desktop Molecular Modeller
eXceed 4.1
Main
MATLAB for Windows
MicroSim
Paint Shop Pro
Microsoft Office Professional
Minitab 10.2
Quattro Pro for Windows
SlideWrite
SPSS
New Versions
Logout
Display Power Management
WinGuard

File Edit Options 0:41 PM

MacMoon

Julian date: 2451574.65372
Universal time: 3:41:21 31 January 2000
Local time: 20:41:21 30 January 2000



Age of moon: 24 days, 16 hours, 0 minutes
Moon phase: 24% (0% = New, 100% = Full)
Phase name: Waning Crescent.
Moon's distance: 404720 kilometers, 63.5 Earth radii.
Moon subtends: 0.492

Sun's distance: 147.3
Sun subtends: 0.541

Last new moon: 18:1
First quarter: 13:34
Full moon: 4:41 UTC
Last quarter: 7:58 U
Next new moon: 13:0

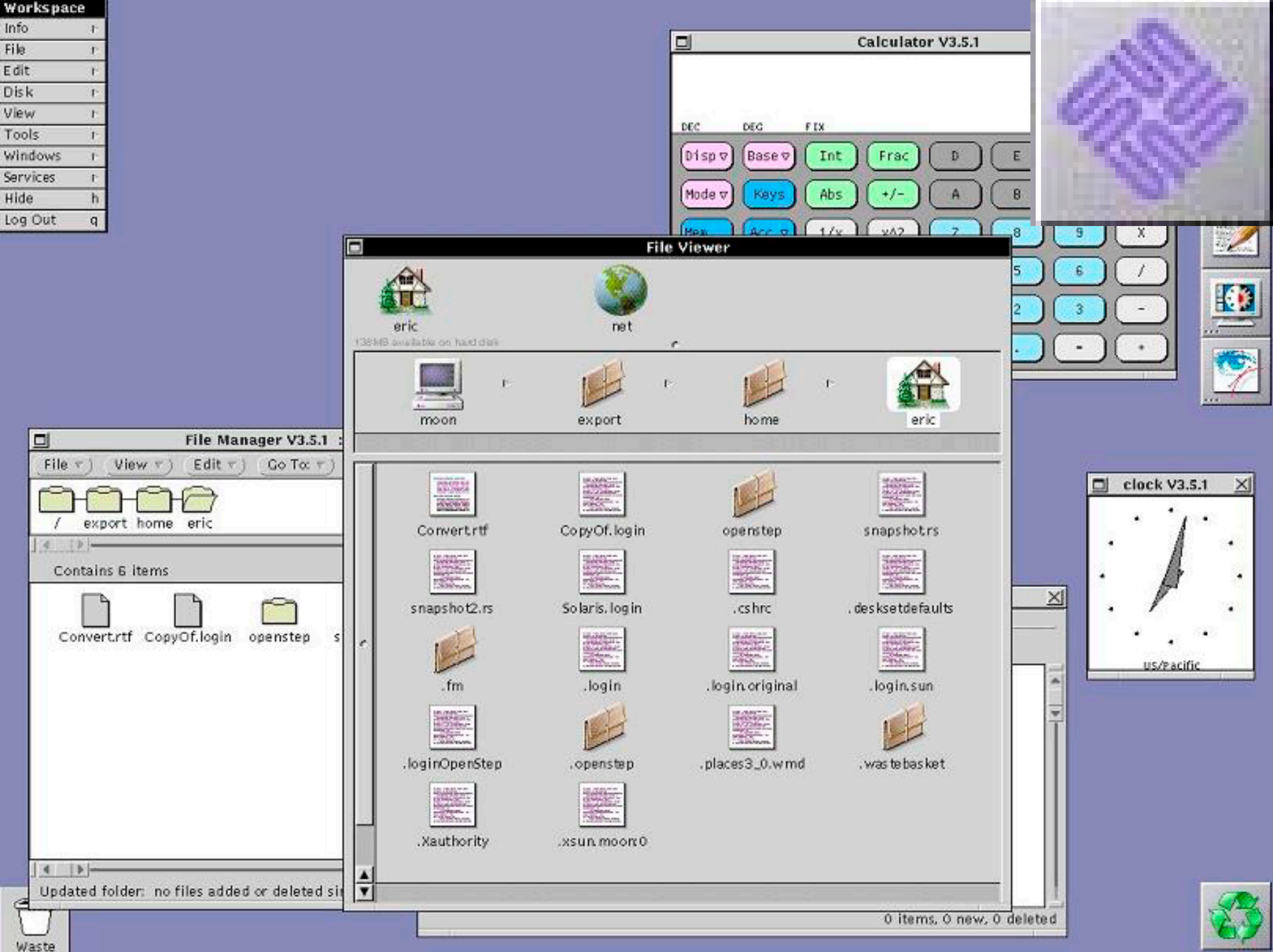
Enter Universal Time

Date: 31 / January / 2000

Time: 03 : 40 : 55

Now Set Time

Macintosh HD
FreeBSD boot
Netscape
Emacs
Trash


Workspace
Info
File
Edit
Disk
View
Tools
Windows
Services
Hide
Log Out
Calculator V3.5.1
DEC
DEG
FIX
Disp
Base
Int
Frac
Mode
Keys
Abs
+/-
File Viewer
eric
net
moon
export
home
eric
Convert.rtf
CopyOf.login
openstep
snapshot.rs
snapshot2.rs
Solaris.login
.cshrc
.desksetdefaults
.fm
.login
.login.original
.login.sun
.loginOpenStep
.openstep
.places3_0.wmd
.wastebasket
.Xauthority
.xsun.moon:0
File Manager V3.5.1
File
View
Edit
Go To:
/
export
home
eric
Contains 6 items
Convert.rtf
CopyOf.login
openstep
Updated folder: no files added or deleted si
clock V3.5.1
US/Pacific
0 items, 0 new, 0 deleted
Waste

xterm@celebris

rxvt

```
nark:{101}/home/nark % ppp
User Process PPP. Written by Toshiharu OHNO.
Log level is 281
can't open
Warning: No
Warning: Al
Using inter
Interactive
ppp ON cele
Dial attemp
Phone: 6516
dial failed
Dial attemp
Phone: 6516
dial OK!
login OK!
ppp ON cele
ppp ON cele
PPP ON cele
```

Motif CD Audio Player 0

10 01 +02:57

loc-db elapse play

the tragically hip

lets stay engaged

Netscape: Mark's FreeBSD Resource Site

File Edit View Go Bookmarks Options Directory Window

Back Forward Home Reload Images Open Print Find Stop

Location: http://vinyl.quickweb.com/nark/FreeBSD/index.html

Mark's FreeBSD Resource Site

Please stay tuned, this page is under contruction right now.. Reload often, a
regularly!

Things to look forward to:

- My controversial "Why I don't run Linux" article that was publishe
- How I got the Netscape Java interpreter running in FreeBSD – a st
- Java and FreeBSD, – you can do it! I'm also hoping to organize bug
  Alpha JDK1.0.2 so we can be ready for the Java craze.
- My wee little ports archive of some stuff I use. Get them here and be kind to freebsd.org's T1

FreeBSD – the ultimate workstation

The Gimp

File Edit Tools Brushes Color

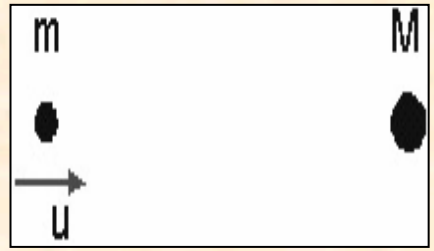
xconsole

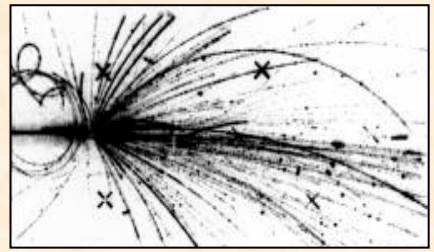
Acrobat Reader

Principes

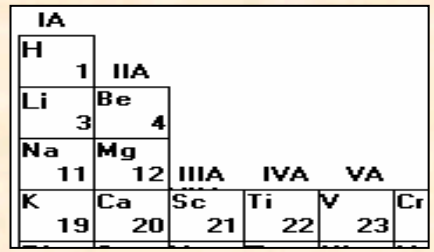
Operating System Finger Printing (OSFP)

- Stimuler la cible
- Capter ses réactions
- Analyser (base de référence)
- Réitérer si nécessaire





$$\Gamma_{12} = \frac{1}{\sqrt{1-\beta^2}}$$



Difficultés

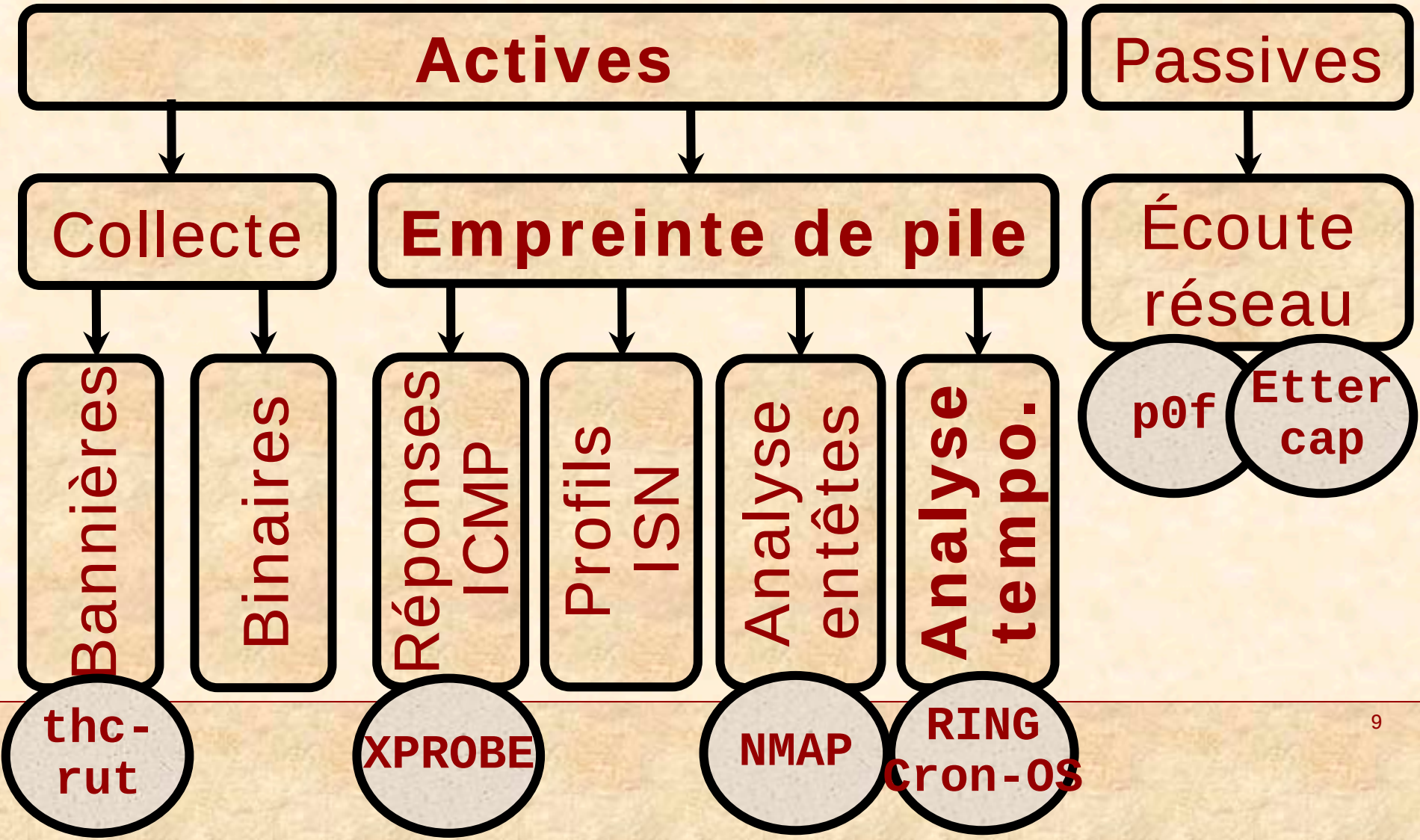
Beaucoup (trop) d'inconnues

- État initial de la cible
- Effet précis du stimulus
- Effet du médium…

Des cas d'échecs ambigus

- base incomplète ? Nouvelle protection ? Réseau perturbé ?

Techniques de détection



Ex : NMAP

Port ouvert

ISN (séquence TCP)

IP ID (ouvert)

TCP SYN + options

Port fermé

IP ID (fermé)

TCP SYN, TCP ACK

UDP (réponse ICMP)

TCP ACK

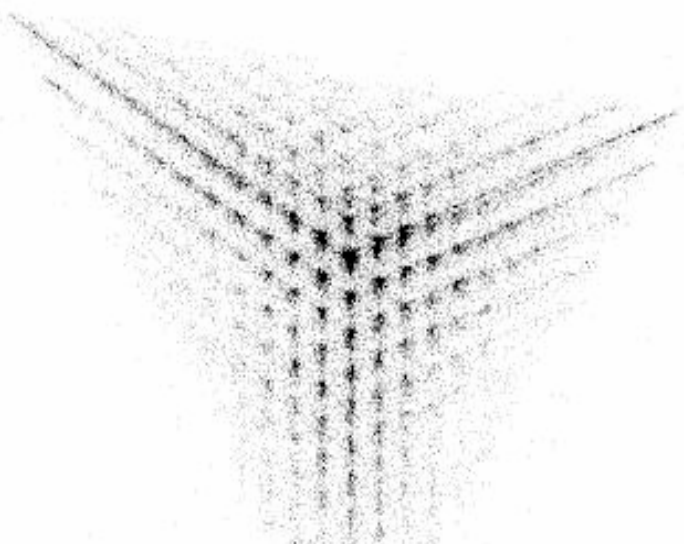
TCP S/F/P/U

TCP NULL

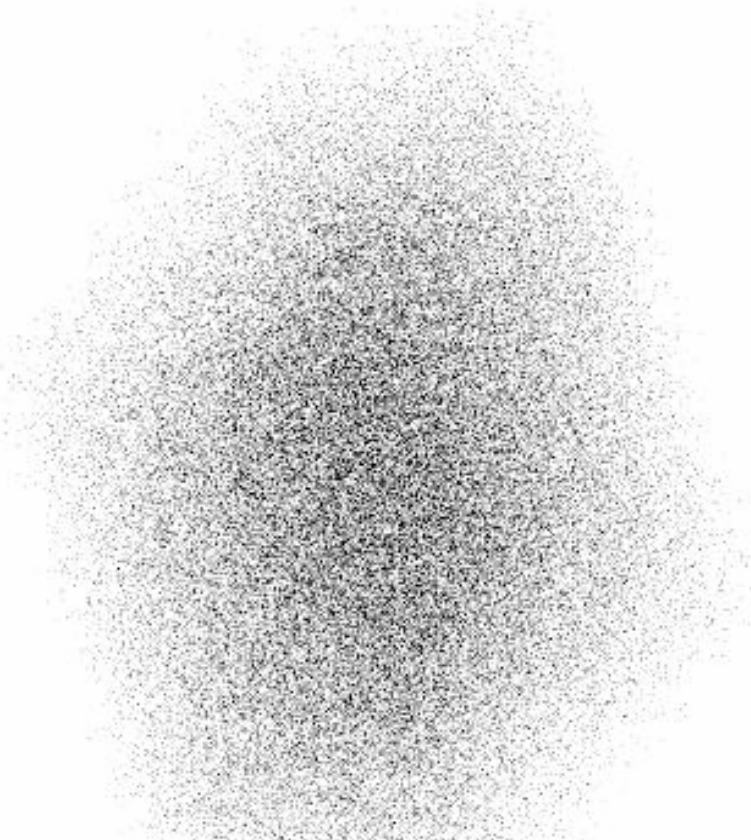
TCP Xmas (F/P/U)

Paquets non-standards

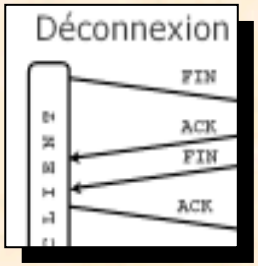
Ex : Profils ISN

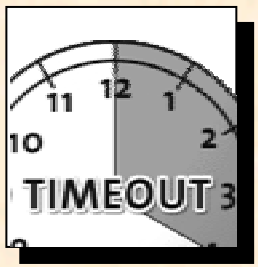


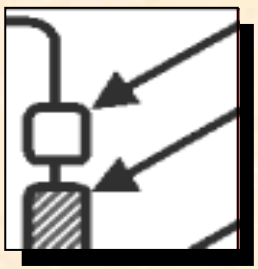
Cisco IOS 12.0 (unpatched)



Linux 2.2



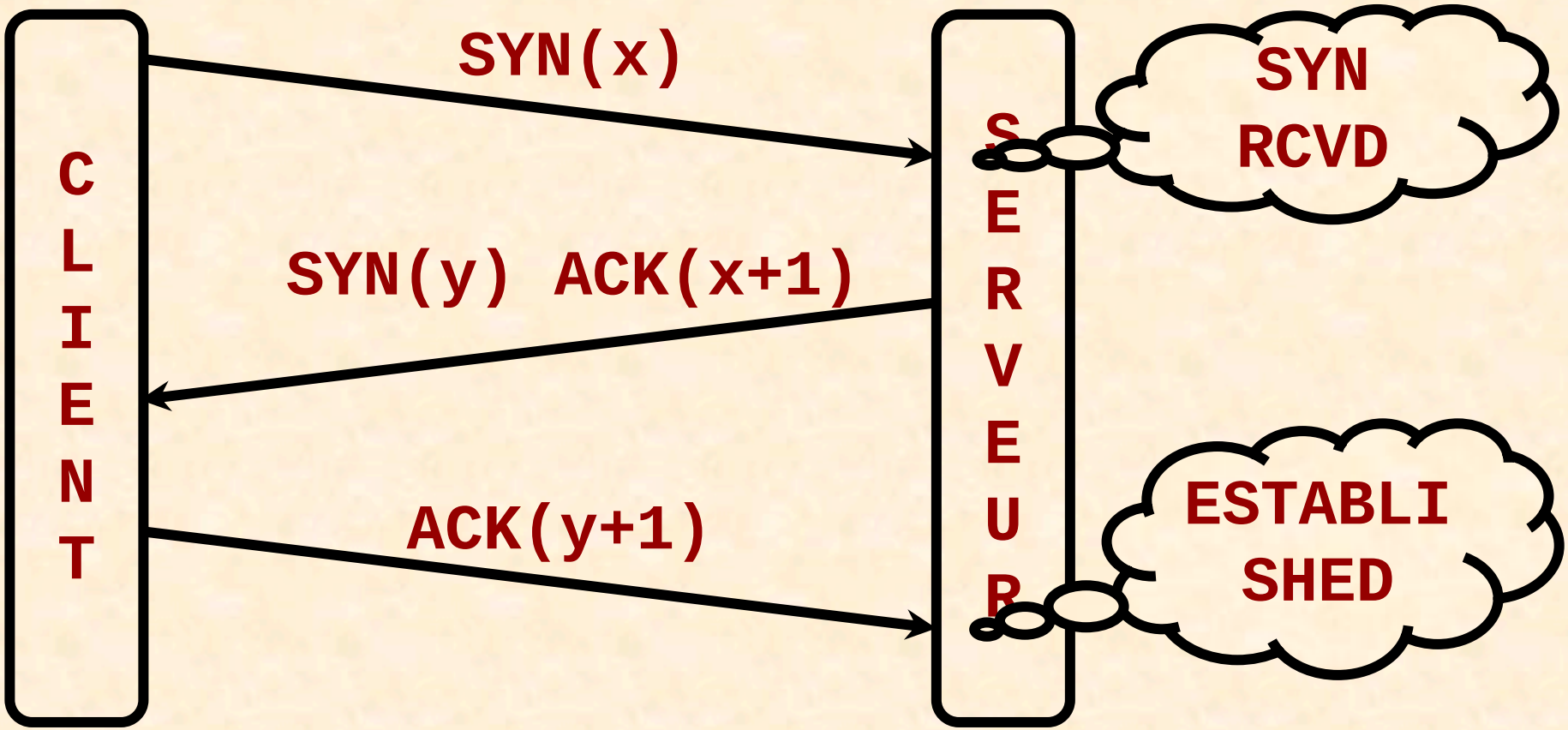




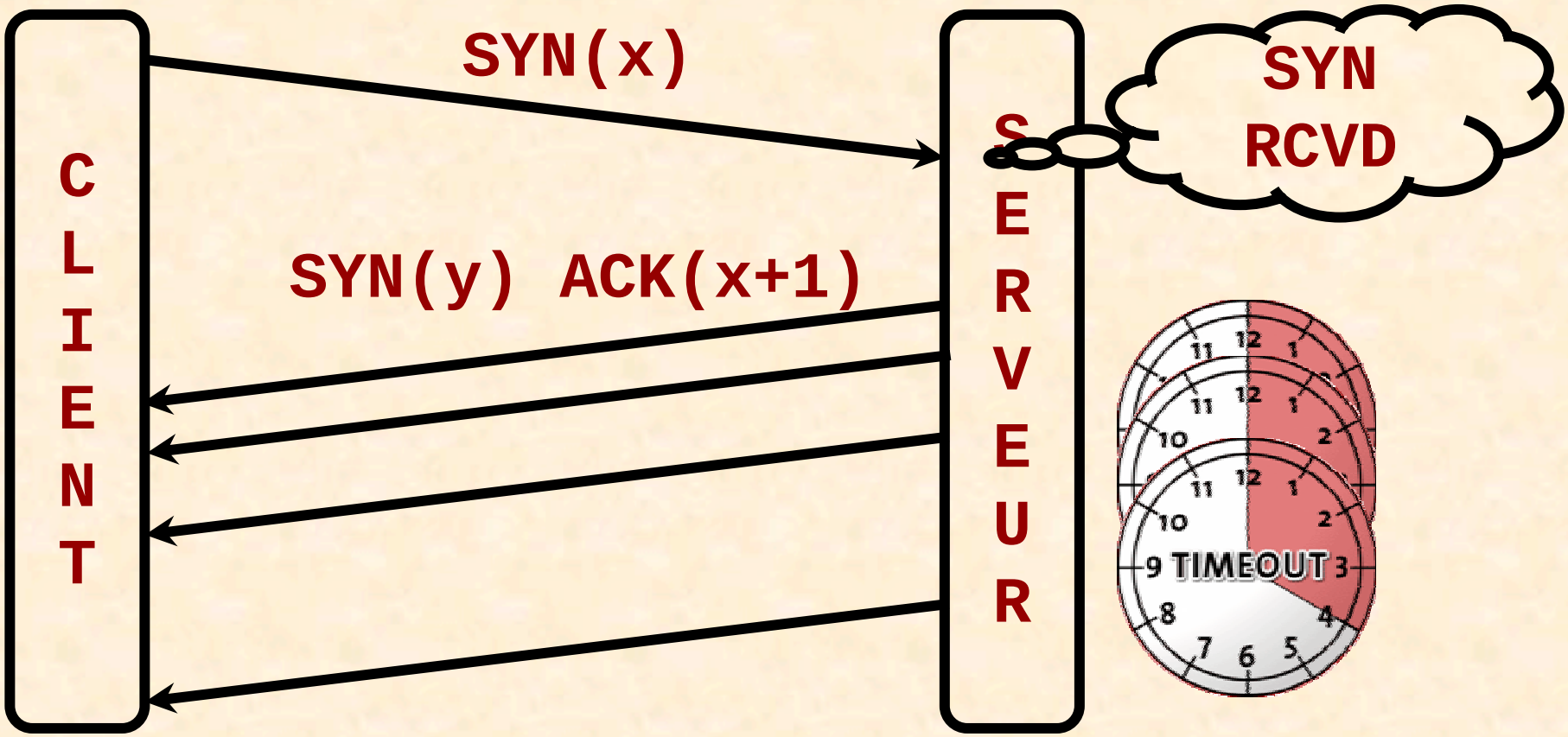
Principes de **Cron-OS**

Congestion TCP/IP, Stimuli, Mesures, Déductions, Erreurs

Connexion TCP/IP

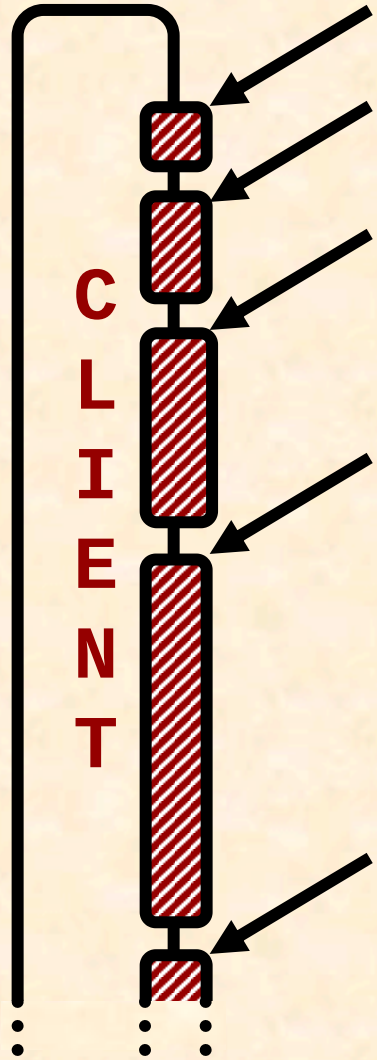


Avec congestion

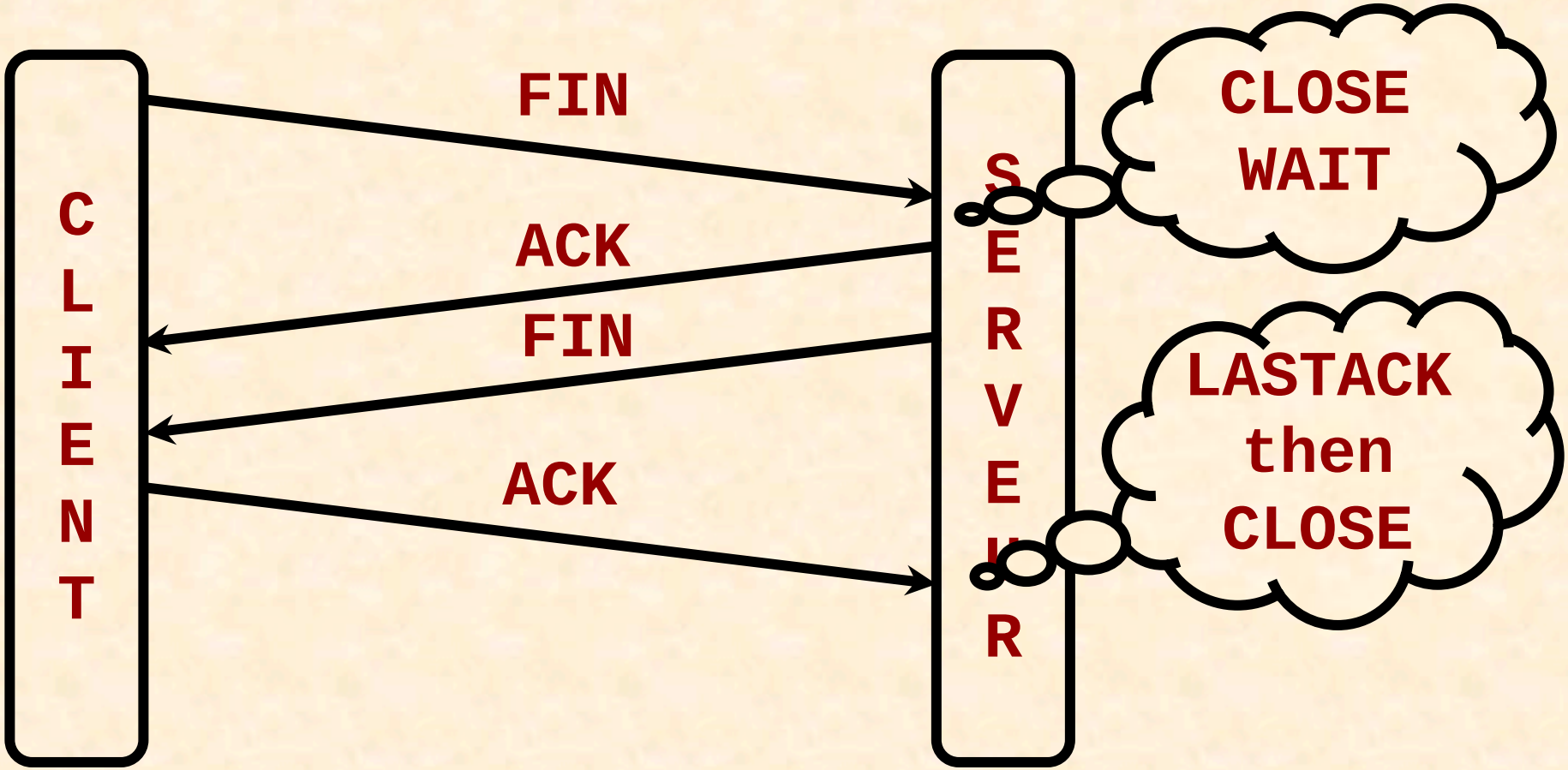


1er Principe

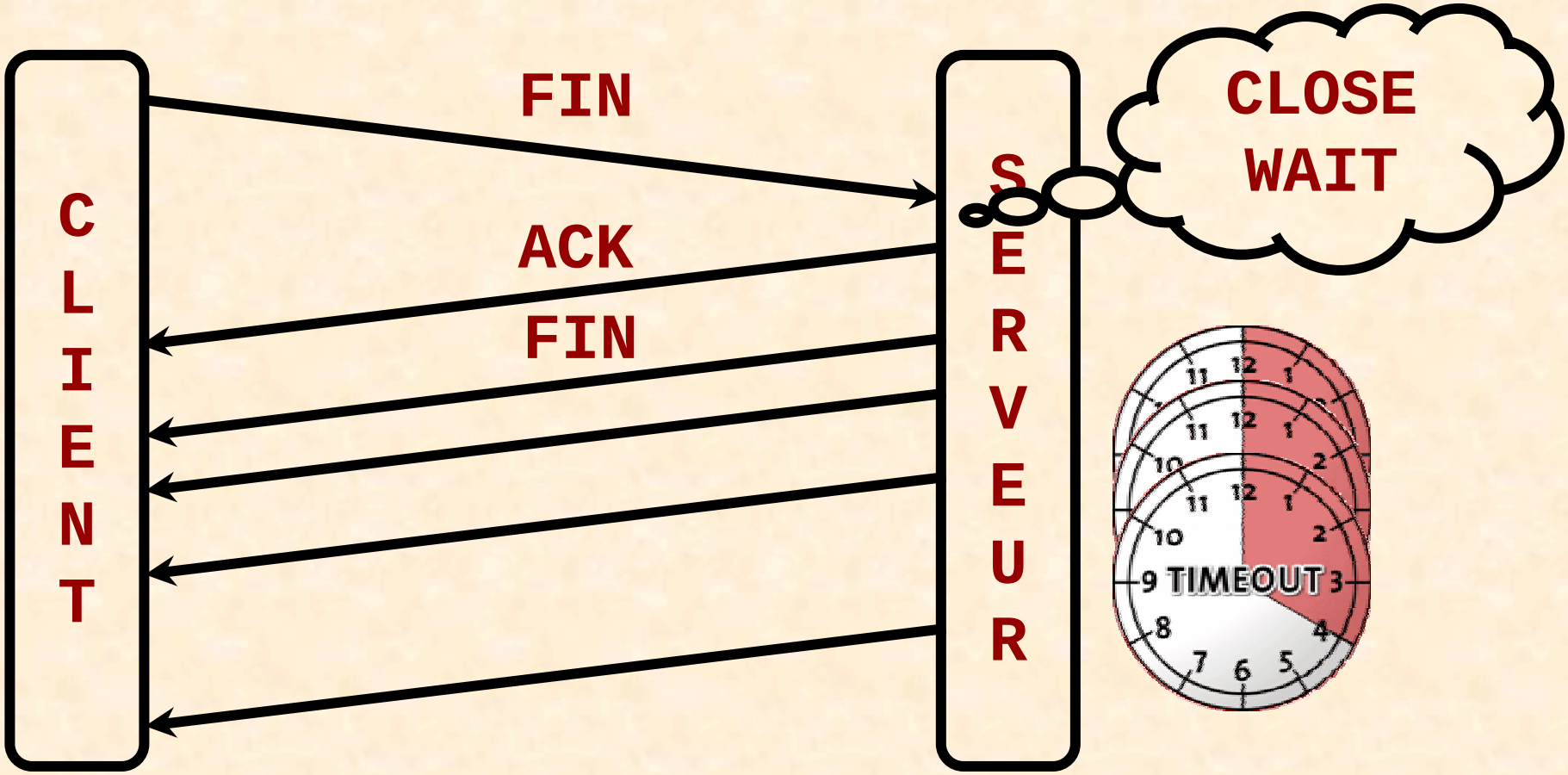
1. Amener le serveur dans l'état **SYN RCVD**
2. Ne pas répondre aux **SYN ACK**
3. Mesurer la suite des délais entre **SYN ACK**
4. Confronter à la base



Déconnexion TCP/IP active

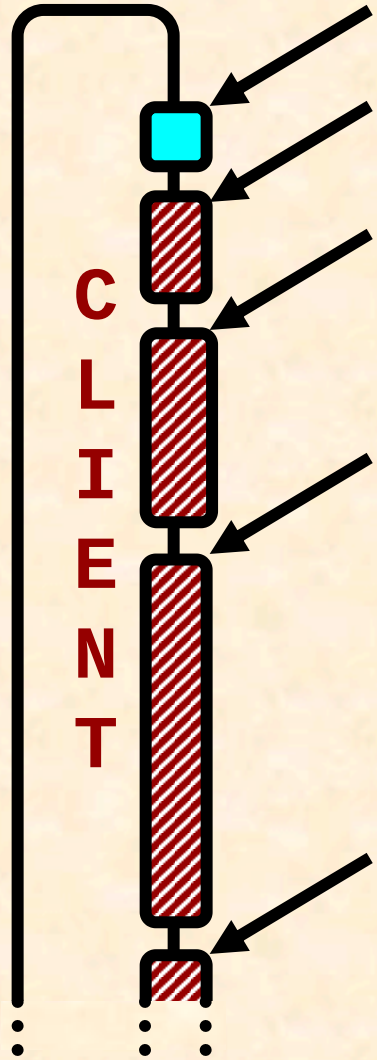


Avec congestion



2ème Principe

1. Amener le serveur dans l'état **CLOSE WAIT**
2. Ignorer le **ACK**, ne pas répondre aux **FIN**
3. Mesurer la suite des délais entre **FIN**
4. Confronter à la base

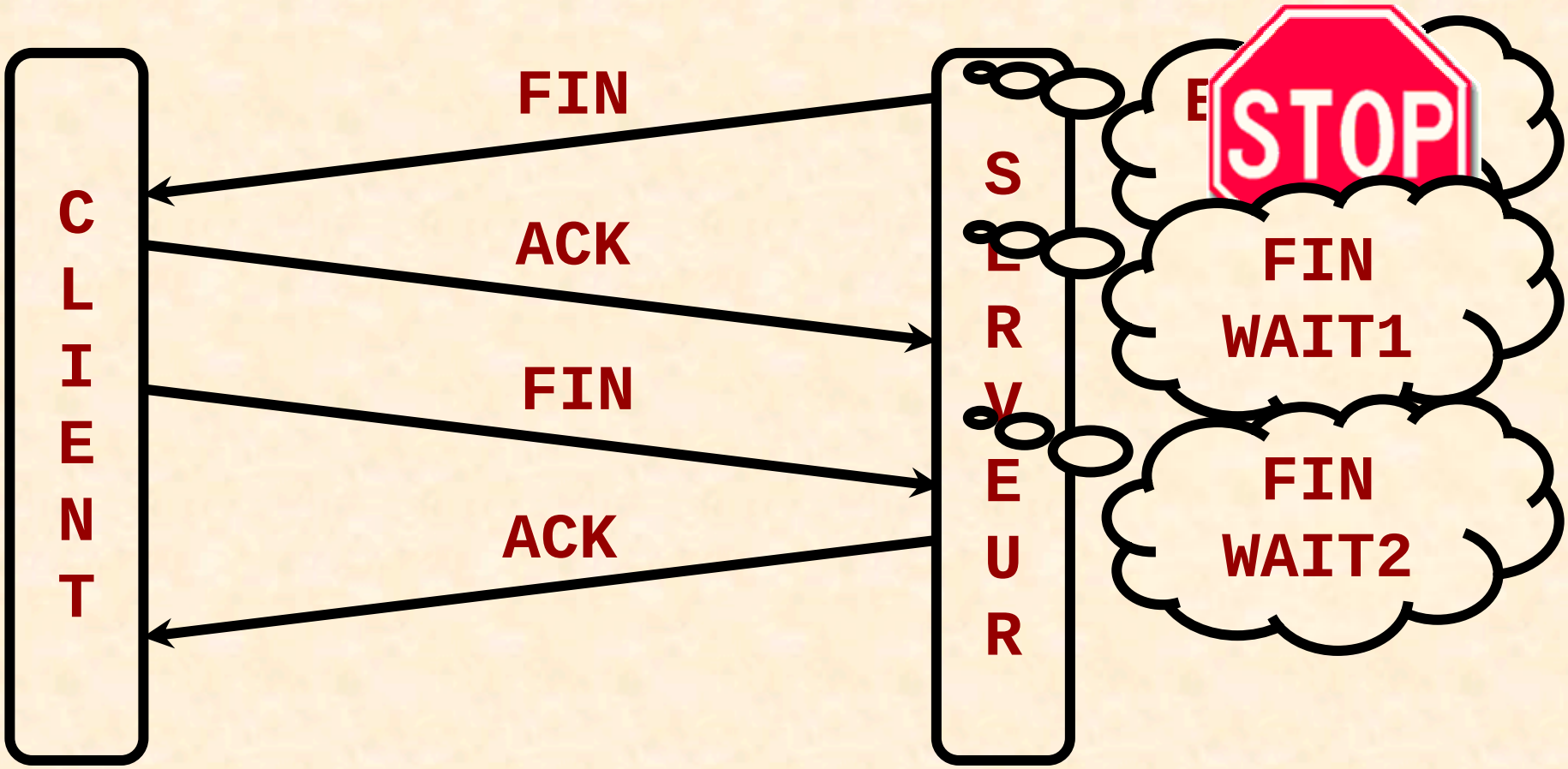


<QUOTE ’RFC 2988’>

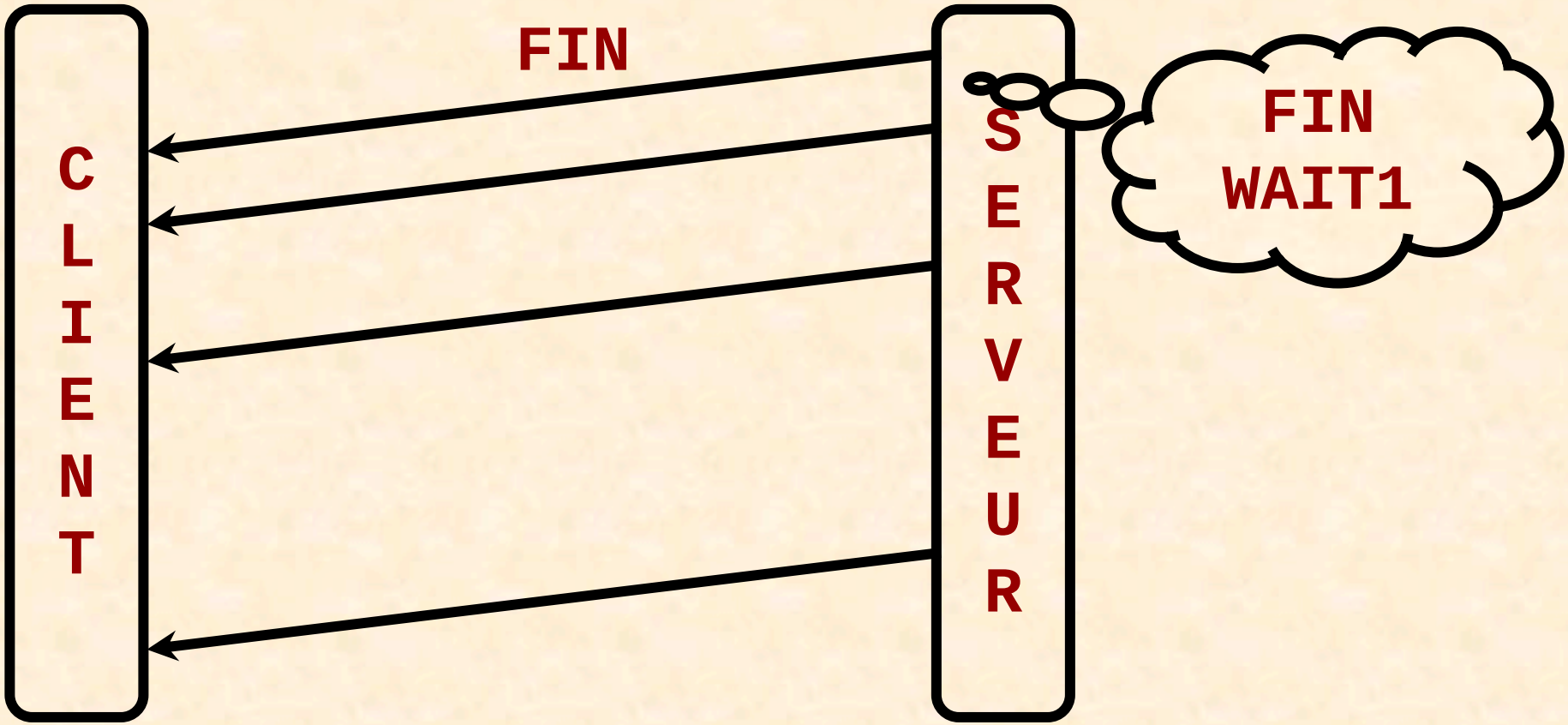
An implementation MUST manage the RTO in such a way that a segment is never retransmitted too early. The host MUST set RTO <- RTO * 2 ("back off the timer"). The maximum value (60s) may be used to provide an upper bound to these doubling operation.

</QUOTE ’RFC 2988’>

Déconnexion TCP/IP passive

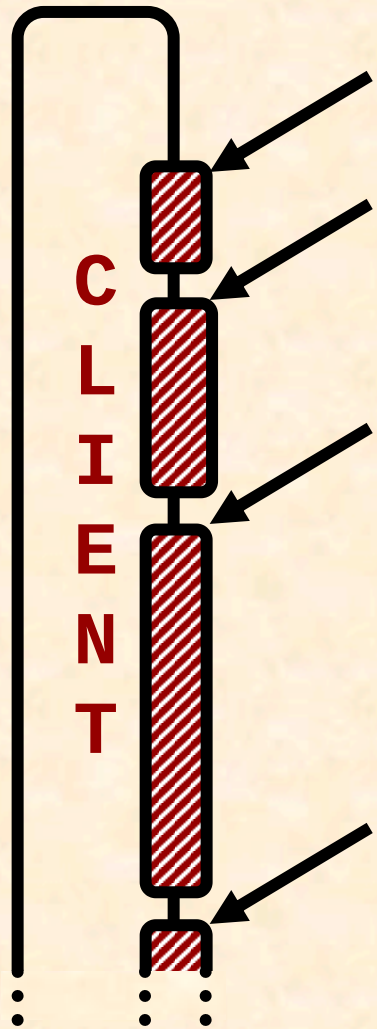


Avec congestion



3ème Principe

1. Espérer que le serveur passe en **FIN WAIT1**
2. Ignorer les **FIN**
3. Mesurer la suite des délais entre **FIN**
4. Comparer à la base



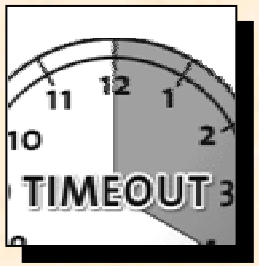
Justification du 3ème Principe

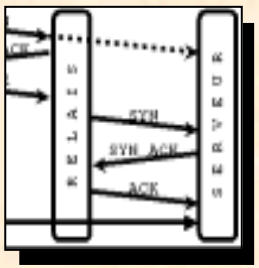
Les serveurs web ferment volontiers leur connexion

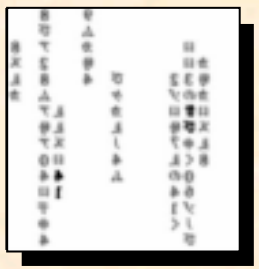
- Comportement HTTP 1.0 normal
- Envoyer **`GET / HTTP/1.0\r\n\r\n`**

Le serveur se comporte alors comme un client TCP/IP

- Et peut donc passer en **`FIN WAIT1`**







Exemples concrets

Cas typiques, cas particuliers, *SYNRelay*

Intégration **Cron-OS** / NMAP

```
# ./nmap-cron-OS shal.no-ip.org
        -p 80,1234
        --cron-OS slf
        --timeout 60  -O
```

Ports 80 et 1234 testés

Écoute de 60 secondes pour chaque état analysé

États **s**yn **l**ast-ack et **f**in-wait1 analysés

```
Fingerprint: Windows NT
TSeq(Class=RI%gcd=1%SI=3CC4%IPID=I...
T1(Resp=Y%DF=Y%W=FFFF%ACK=S++%Flags=...
...
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=...
CronOS_Syn(nbPkt=2%Time=30%p=2806316%p=
6010910)
CronOS_LastAck(nbPkt=3%Time=30%Connect=
134571%p=2918695%p=5909092%p=12014080)
CronOS_FinWait(nbPkt=0%Time=30%Connect=
136213)
```

Portabilité

Point faible de **Cron-OS**, mais

- Planb-security fournit une version en PERL appelée **Snacktime**
- LibNet 1.1 maintenant supportée

Cron-OS est en source libre

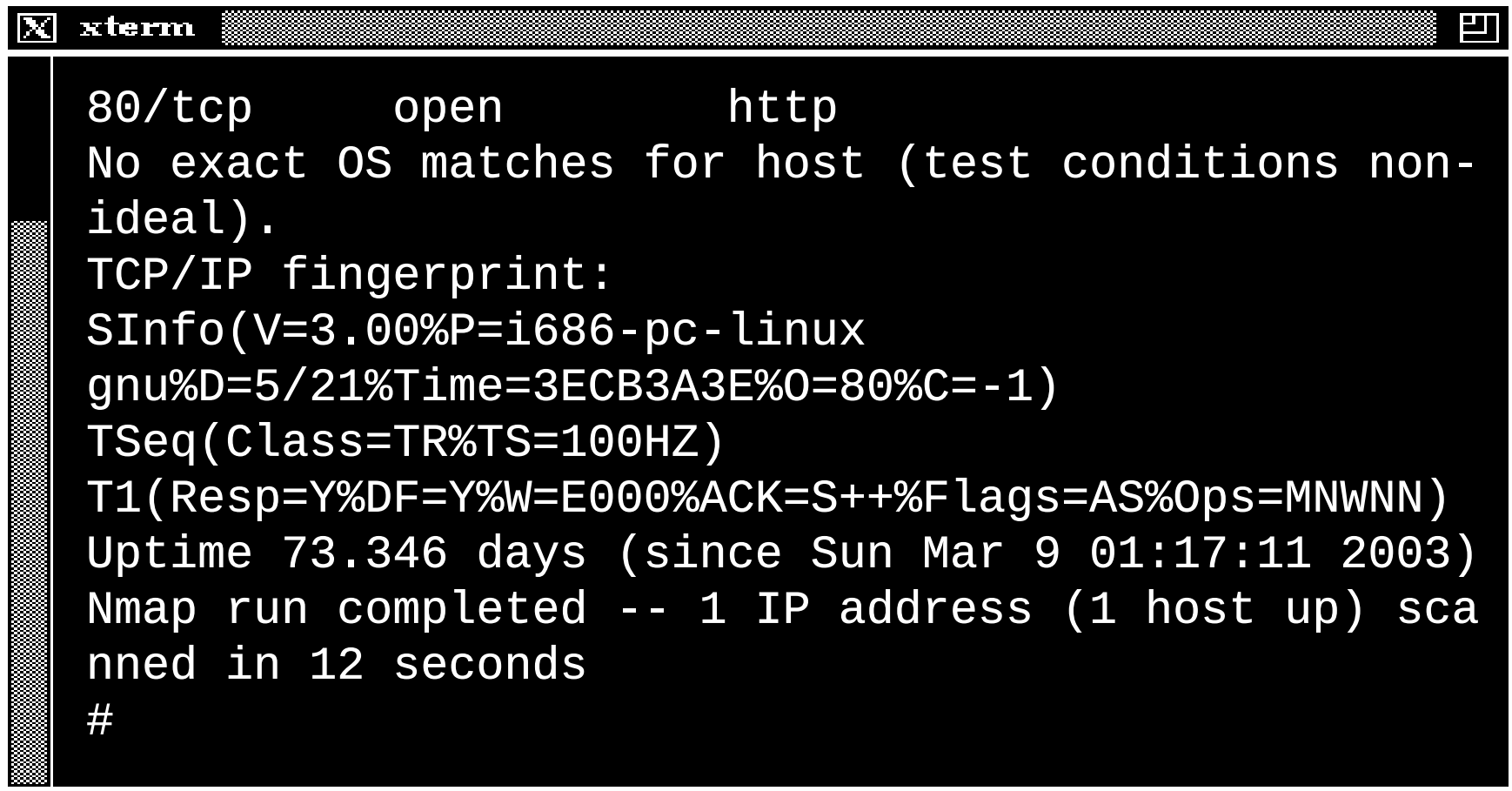
- Les bonnes volontés sont donc encouragées…

Fonctionnement simple

xterm

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
filtre pcap :src host xxx.xxx.xxx.xxx and src
port 80 and dst port 50101
Try Time: 2992758 5997554 12004378
Interesting ports on  (xxx.xxx.xxx.xxx):
Port       State       Service
80/tcp     open        http
Remote OS guesses: FreeBSD 4.5       (2success/2t
ests), FreeBSD 4.7-RELEASE - 4.8-RELEASE       (2
success/2tests), Windows 98 Second Edition
(2success/2tests), Windows NT 4 Workstation SP2/S
P3/SP4/SP5       (2success/2tests)
#
```

Fonctionnement simple

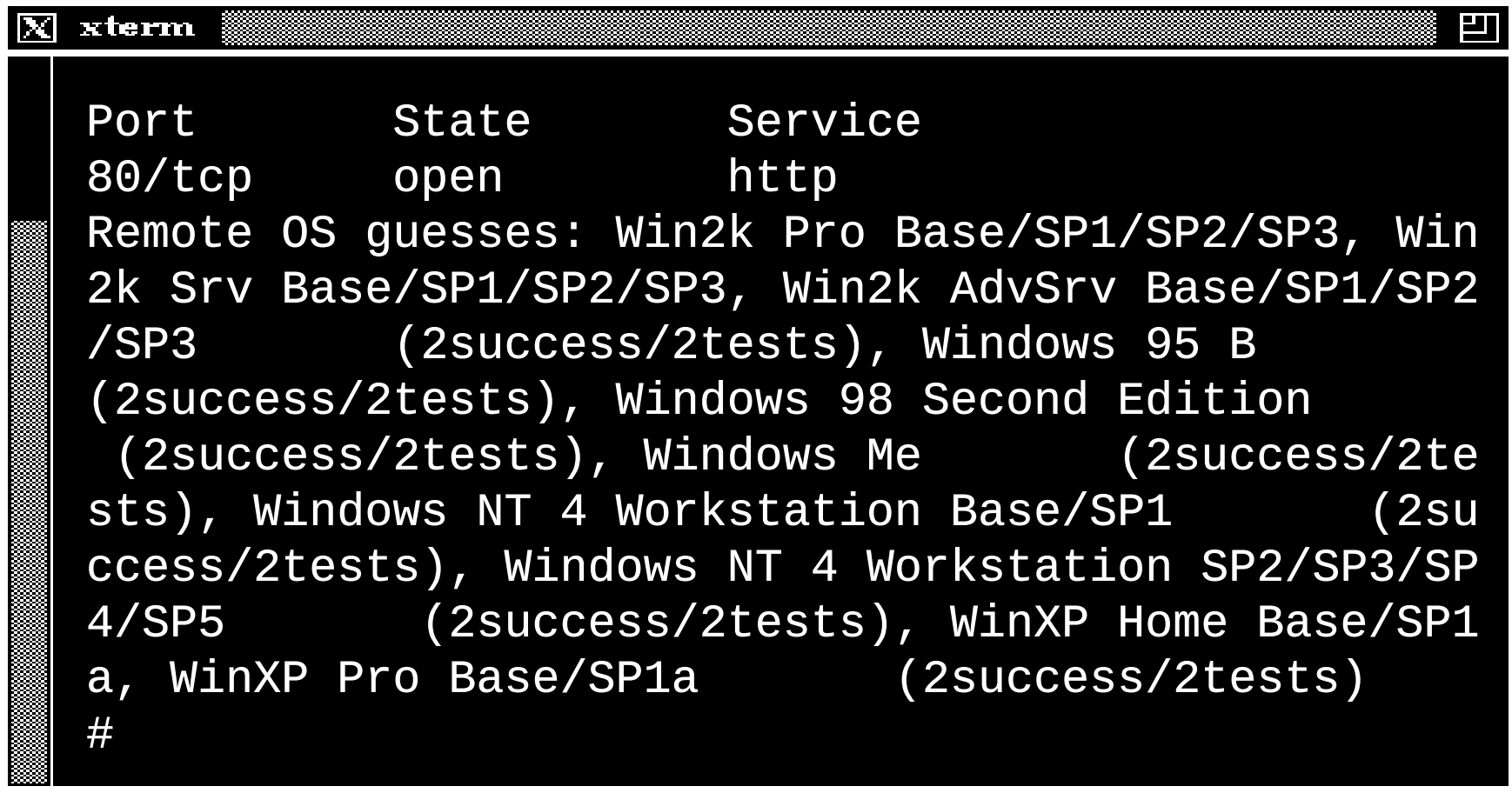


Fonctionnement simple

Les résultats diffèrent. Pourquoi ?

- Il y a un pare-feu « droppant »
- L'OS réel n'est pas dans les bases
- Les conditions réseau sont mauvaises
- ...

Fonctionnement avancé



Fonctionnement avancé

xterm

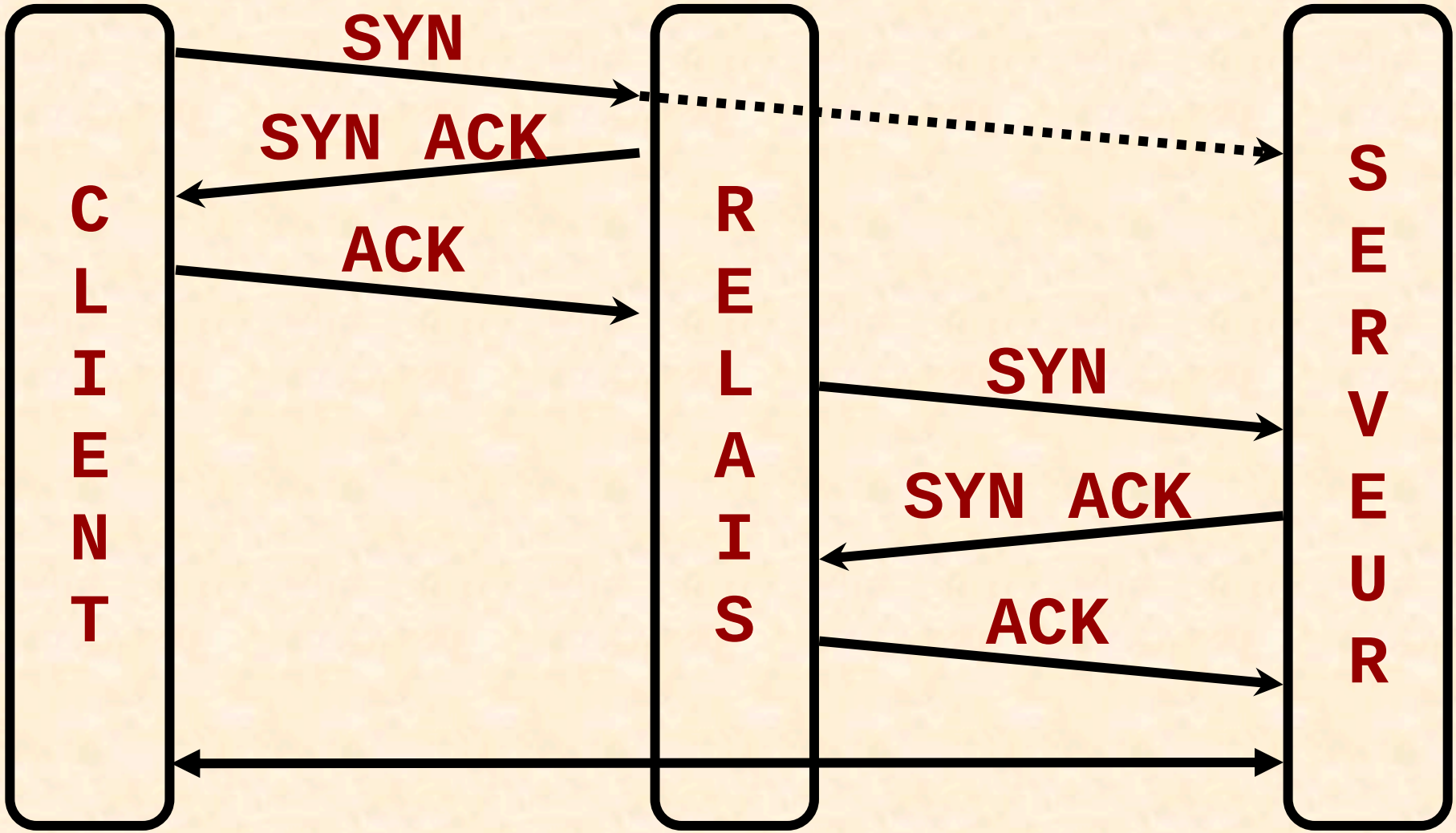
```
qq.part | grep -v "Resp=N"
Port        State       Service
80/tcp      open        http
Remote operating system guess: Nokia M1122 DSL Rou
ter
OS Fingerprint:
TSeq(Class=RI%gcd=1%SI=5937%IPID=I%TS=0)
T1(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T3(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)

Nmap run completed -- 1 IP address (1 host up) sca
nned in 4 seconds
```

Fonctionnement avancé

Les résultats diffèrent. Pourquoi ?

- Un équipement Nokia est utilisé en SYNRelay
- NMAP « voit » cet équipement
- **Cron-OS** « voit » au travers


CLIENT
SYN
SYN ACK
ACK
RELAIS
SYN
SYN ACK
ACK
SERVEUR

Fonctionnement avancé

Les résultats sont complémentaires

- Tout seul, **Cron-OS** ne voit pas le SYNRelay
- Tout seul, NMAP ne voit pas la machine protégée
- Ensemble, **Cron-OS** et NMAP voient les OS et l'architecture

Vos questions...

olivier.courtay@enst-bretagne.fr
olivier.heen@thomson.net
franck.veysset@francetelecom.com

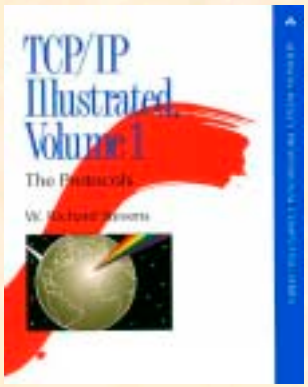
Bibliographie et annexes

Livres, articles, sites, outils

Bibliographie

W. Richard Stevens,

TCP/IP illustrated



Autres sources de connaissance

- RFC 793, Transmission Control Protocol
- RFC 1122, Requirements for Internet Hosts -- Communication Layers
- RFC 2988, Computing TCP's Retransmission Timer

IETF

Bibliographie

R. Spangler, Analysis of Remote Active Operating System Fingerprinting Tools
www.packetwatch.net/documents/papers/osdetection.pdf

O. Arkin, F. Yarochkin, 2002. XProbe2 – A 'Fuzzy' Approach to Remote Active Operating System Fingerprinting
www.xprobe2.org/archive/papers/Xprobe2.pdf

T. Beardsley, Plan B Security, 2002. RING Out The Old, RING In The New: OS Fingerprinting through RTOs. www.planb-security.net/wp/ring.html

D. Comer, J. Lin, USENIX Summer Conf. 1994. Probing TCP Implementations
www.bell- labs.com/user/johnlin/probing-TCP.pdf

Fyodor, Phrack 1998. Remote OS detection via TCP/IP Stack FingerPrinting
www.insecure.org/nmap/nmap-fingerprinting-article.txt

P. Karn, C. Partridge, SIGCOMM 87. Improving Round-Trip Time Estimates in Reliable Transport Protocols

Bibliographie

B. Morin, L. Mé, H. Debar, M. Ducassé. M2D2 : A Formal Data Model for IDS Alert Correlation. RAID 2002 : 115-127

J. Padhye, S. Floyd, SigComm 2001. Identifying the TCP Behavior of Web Servers www.icir.org/tbit/nanog-tbit.pdf

M. Smart, G. R. Malan, F. Jahanian, 9th USENIX Security Symp. Defeating TCP/IP Stack Fingerprinting

F. Veysset, O. Courtay, O. Heen RING : New Tool and Technique For Remote OSFP www.intranode.com/site/techno/techno-articles.htm

M. Zalewski, 2001. Strange Attractors and TCP/IP Sequence Number Analysis lcamtuf.coredump.cx/newtcp/

Outils

www.insecure.org

www.intranode.com

www.xprobe.org

Xprobe2

www.stearns.org/p0f

ettercap.sourceforge.net

ettercap

Annexe 1 Difficultés

Annexe 2
États TCP/IP