Libre Software Meeting
Metz July 9 - 12

OSFP based on temporal analysis with **Cron-OS**

Franck Veysset (France Télécom)
Olivier Courtay (ENST Bretagne)
Olivier Heen (Thomson)

OS Finger Printing?

Why doing OSFP?

- Network survey
- Audits
- Intelligence / to be nosey!

Other reasons...

- Learn what hackers really know about you
- Build better traps

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)
Meteorology
A.M.S.
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
Microsoft Office Professional
Minitab 10.2
Paint Shop Pro
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

Trash

Workspace
Info
File
Edit
Disk
View
Tools
Windows
Services
Hide
Log Out
Calculator V3.5.1
DEC
DEG
FIX
Disp
Base
Int
Frac
D
E
Mode
Keys
Abs
+/-
A
B
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
```

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

Motif CD Audio Player 0

10 01 +02:57

loc-db elapse play

the tragically hip
lets stay engaged

The Gimp

File Edit Tools Brushes Color

xconsole Acrobat Reader

12:46am SUN 23 FEB

Pager

```
            DSR CTS
*** STOP:  0x0000000A  (0x00000000, 0x0000001a, 0x00000000, 0x00000000)
IRQL_NOT_LESS_OR_EQUAL

p4-0300 irql:1f  SYSVER:0xf000030e

Dll Base DateStmp - Name              Dll Base DateStmp - Name
80100000 2e53fe55 - ntoskrl.exe       80400000 2e53eba6 - hal.dll
80010000 2e41884b - Aha154x.sys       80013000 2e4bc29a - SCSIPORT.SYS
8001b000 2e4e7b6b - Scsidisk.sys      80220000 2e53f238 - Ntfs.sys
fe420000 2e406607 - Floppy.SYS        fe430000 2e406618 - Scsicdrm.SYS
fe440000 2e406659 - Fs_Rec.SYS        fe450000 2e40660f - Null.SYS
fe460000 2e4065f4 - Beep.SYS          fe470000 2e40663  - Sermouse.SYS
fe480000 2e42a4a4 - i8042prt.SYS      fe490000 2e4066   - Mouclass.SYS
fe4a0000 2e40660c - Kbdclass.SYS      fe4c0000 2e406    - VIDEOPRT.SYS
fe4b0000 2e53d49d - ati.SYS           fe4d0000 2e40     - vga.sys
fe4e0000 2e406655 - Msfs.SYS          fe4f0000 2e41     - Npfs.SYS
fe510000 2e53f222 - NDIS.SYS          fe500000 2e40     - elnkii.sys
fe550000 2e406697 - TDI.SYS           fe[illegible]e47  - nbf.sys
fe560000 2e5279d9 - nwlnkipx.sys      fe[illegible]e53  - nwlnknb.sys
fe580000 2e494973 - tcpip.sys         fe5a0000 2e52     - afd.sys
fe5b0000 2e5279d3 - netbt.sys         fe5d0000 2e41     - netbios.sys
fe5e0000 2e4066b3 - mup.sys           fe5f0000 2e4f     - rdr.sys
fe630000 2e53f24a - srv.sys           fe660000 2ef16    - nwlnkspx.sys

Address     dword dump Build [1057]                                  - Name
FF541E4c    fe5105df  fe5105df  00000001  ff640128  fe4a82[illegible]  000002fe - NDIS.SYS
ff541e60    fe501368  fe501368  00000246  00004002  00000000  00000000 - elnkii.sys
ff541eb4    fe481509  fe481509  ff6688c8  ff668288  00000000  ff668138 - i8042prt.SYS
ff541ee0    fe481ea8  fe481ea8  fe482078  00000000  ff541f04  8013c58a - i8042prt.SYS
ff541ee4    fe482078  fe482078  00000000  ff541f04  8013c58a  ff6688c8 - i8042prt.sys
ff541ef0    8013c58a  8013c58a  ff6688c8  ff668040  80405900  00000031 - ntoskrnl.exe
ff541efc    80405900  80405900  00000031  06060606  06060606  06060606 - hal.dll

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option if this message reappears,
contact your system administrator or technical support group.
CRASHDUMP: Initializing miniport driver
CRASHDUMP: Dumping physical memory to disk:   2000
CRASHDUMP: Physical memory dump complete
```

Principles

Operating System Finger Printing (OSFP)

- Trigger the target
- Record its reactions
- Analyze (vs database)
- Dig further if needed

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

Caveats

Many things are unknown

- Initial state of the target
- Effect of the stimulation
- Effect inducted by the environment…

Some pitfalls lead to doubt

- Incomplete reference base?
- Network problems?
- New countermeasure

Difficulties

	The tool gives a result		No result	
OS in the database	OK	KO error	KO false negative	
OS not in the database	KO false positive		OK	
OS unknown (often the case)	OK	KO	OK	KO

Different Techniques

Ex: NMAP

Open Port

ISN (TCP sequences)

IP ID

TCP SYN + options

Close Port

IP ID

TCP SYN, TCP ACK

UDP (ICMP answer)

TCP ACK

TCP S/F/P/U

TCP NULL

TCP Xmas (F/P/U)

Non standard packets

Ex: ISN generation

Cisco IOS 12.0 (unpatched)

Linux 2.2

Cron-OS principles

TCP/IP Congestion, Stimuli, Measures, Errors

TCP/IP Connection

With congestion (packet losses)

1st Principle

1. Server has to be in **SYN RCVD** state
2. Ignore **SYN ACK** packets
3. Measure delays between **SYN ACK** packets
4. Compare results with signature database

<QUOTE ’RFC 2988’>

Until a round-trip time (RTT) measurement has been made for a segment sent between the sender and receiver, the sender **SHOULD** set RTO <- 3 seconds…

</QUOTE ’RFC 2988’>

TCP/IP active disconnection

With congestion

2nd Principle

1. Server has to be in **CLOSE WAIT** state
2. Ignore **ACKs**, ignore **FINs**
3. Measure delays between **FIN** packets
4. Compare results with signature database

<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’>

TCP/IP passive disconnection

With congestion

3rd Principle

1. The server has to be in **FIN WAIT1** state
2. Ignore **FINs**
3. Measure delays between FIN packets
4. Compare results with signature database

Why the 3rd Principle?

Web servers often close the connection

- HTTP 1.0 normal behavior
- Send **`GET / HTTP/1.0\r\n\r\n`**

The server will then send data and close its connection

- It is now in **`FIN WAIT1`** state

Inside **Cron-OS** sigs

For 2nd and 3rd Cron-OS methods:

- As seen in RFC 2988, RTO depends on RTT
- We need to compute the RTT (*connect* in signature file)
- Then, match the signature using the *connect* value (scale)

Example

The sig contains:

- CronoOSs_LastAck(nbPkt=2%Time=30%Connect=20000%p=150000%p=300000)

Measure is:

- Connect=38900%p=301050%p=598000

38900/20000 = 1.945 ;

So, sig scales to :

- Connect=38900%p=291750%p=583500

Practical Example

Typical use, Special case, *SYNRelay*

Cron-OS/NMAP Integration

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

Test ports 80 & 1234

Listen 60 s. for each analyzed state

Analyze **s**yn **l**ast-ack & **f**in-wait1 states

```
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)
```

Portability

Main **Cron-OS** drawback, but

- Planb-security made a PERL version called **Snacktime**
- Also LibNet 1.1 is now supported

Cron-OS is Open Source

- Anyone can contribute!

Typical use

```
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)
#
```

Typical use

```
xterm
80/tcp     open        http                          -v "R
No exact OS matches for host (test conditions non-
ideal).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-linux
gnu%D=5/21%Time=3ECB3A3E%O=80%C=-1)
TSeq(Class=TR%TS=100HZ)
T1(Resp=Y%DF=Y%W=E000%ACK=S++%Flags=AS%Ops=MNWNN)
Uptime 73.346 days (since Sun Mar 9 01:17:11 2003)
Nmap run completed -- 1 IP address (1 host up) sca
nned in 12 seconds
#
```

Typical use

Results are different. Why?

- Maybe there's a dropping firewall
- Maybe the real OS is not already in the database
- Maybe network conditions are poor
- …

Special case

```
xterm

Port        State       Service
80/tcp      open        http
Remote OS guesses: Win2k Pro Base/SP1/SP2/SP3, Win
2k Srv Base/SP1/SP2/SP3, Win2k AdvSrv Base/SP1/SP2
/SP3        (2success/2tests), Windows 95 B
(2success/2tests), Windows 98 Second Edition
 (2success/2tests), Windows Me       (2success/2te
sts), Windows NT 4 Workstation Base/SP1       (2su
ccess/2tests), Windows NT 4 Workstation SP2/SP3/SP
4/SP5       (2success/2tests), WinXP Home Base/SP1
a, WinXP Pro Base/SP1a       (2success/2tests)
#
```

Special case

```
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
```

Special case

Results are different. Why?

- A Nokia device is use as a SYN Relay
- NMAP “sees” this device
- **Cron-OS** “sees” across

CLIENT
RELAY
SERVER
SYN
SYN ACK
ACK
SYN
SYN ACK
ACK

Special case

Results are complementary

- Alone, **Cron-OS** cannot detect the SYN Relay
- Alone, NMAP cannot detect the protected host
- Together, **Cron-OS** and NMAP detect both OS and the architecture

http://cron-os.tuxfamily.org

Questions?

olivier.courtay@enst-bretagne.fr
olivier.heen@thomson.net

franck.veysset@francetelecom.com

Bibliography & appendix

Books, papers, sites, tools

Bibliography

W. Richard Stevens,

TCP/IP illustrated

Other information sources

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

Bibliography

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

Bibliography

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/

Tools

www.insecure.org

www.xprobe.org

www.stearns.org/p0f

ettercap.sourceforge.net

Appendix
TCP/IP States