

Building a Secure Environment for Free !

HP World 2002

James G. McIntyre

McIntyre & Associates, Inc.

Radford, VA 24141

jmcintyr@i-plus.net

540-633-6379



Suggested Strategy

- Use freeware tools to gain experience with your system/network environment.
- Gain experience with the features provided by these tools in order to better analyze a vendor tool.
- Freeware tools provide a good *short-term* solution.
- Vendor tools may provide better *long-term* solution.
- Resolves \$\$\$ problem.



The Tools

- Port Scanning Tools
 - Nessus, Nmap
 - Saint, Sara, Satan
- Audit Tools
 - Tripwire
 - TCP Wrappers
 - Portentry
- System Firewalls
 - ipfilters, iptables, ipchains
- Personal Firewalls
 - ZoneAlarm, BlackIce, Tiny



The Tools

- Syslog Scanners
 - Logcheck
 - Swatch
- Sniffers
 - Snoop, iptrace
 - Tcpdump, Windump
 - Ethereal, Netwatch, Analyzer
- IDS
 - Snort (SnortSnarf, SnortSort)
 - Shadow
- Connectivity Tools
 - SSH, Putty, TeraTerm



The Tools

- Sysadmin Tools
 - Big Brother
 - Password Checkers -
 - Crack, l0phtcrack, John the Ripper
 - Lsof, inzider/fport (NT)
 - Sudo (unix)
- Remote Control Tools
 - VNCviewer
- System Security Analyzers
 - CIS Benchmarks



Audit/Port Scan Tools

- These tools can be used to scan your systems and network for vulnerabilities.
- Some tools can perform integrity checks on designated files.
- They have very good reporting tools usually based on HTML.



Port Scanning Tools

- Nmap is the more sophisticated grandson of strobe
 - Available from www.insecure.org &
 - <http://hpux.cs.utah.edu/>



```
root@bigguy:~# nmap -v -i 1024 red.cirt.vt.edu
Starting nmap V. 2.54BETA2 ( www.insecure.org/nmap/ )
No top,udp, or IDP scanflags specified, assuming vanilla tcp connect() scan, use -sP if you really don't want to p
an (and just want to see what hosts are up).
Host red.cirt.vt.edu (128.173.54.103) appears to be up ... good.
Initiating Connect() Scan against red.cirt.vt.edu (128.173.54.103)
Adding IDP port 22 (state open).
Adding IDP port 111 (state open).
Adding IDP port 1024 (state open).
The Connect() Scan took 8 seconds to scan 1024 ports.
For ISScan assuming that port 22 is open and port 1 is closed and neither are firewallled
For ISScan assuming that port 22 is open and port 1 is closed and neither are firewallled
For ISScan assuming that port 22 is open and port 1 is closed and neither are firewallled
Interesting ports on red.cirt.vt.edu (128.173.54.103):
(The 1021 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open   ssh
111/tcp   open   sunrpc
1024/tcp  open   ksh

No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-subel
).
TCP/IP fingerprint:
SInfo(V=2.54BETA2P=1356-rodhat-11nrc-gn.60=7/188Tloc=3038278580-220C=1)
TSeq(CIass=RIdgc=183I=3000CFX(IPID=CITB=100C)
TSeq(CIass=RIdgc=183I=3000CFX(IPID=CITB=100C)
TSeq(CIass=RIdgc=183I=31251X(IPID=CITB=100C)
T1(Resp=VDF=VU=16/020C)=S+XF Lags=630Ops=996(N4)
T2(Resp=N)
T3(Resp=VDF=VU=16/020C)=S+XF Lags=630Ops=996(N4)
T4(Resp=VDF=VU=06/2C)=CF Lags=630Ops=)
T5(Resp=VDF=VU=06/2C)=S+XF Lags=630Ops=)
T6(Resp=VDF=VU=06/2C)=CF Lags=630Ops=)
T7(Resp=VDF=VU=06/2C)=S+XF Lags=630Ops=)
T8(Resp=VDF=VU=06/2C)=S+XF Lags=630Ops=)
T9(Resp=VDF=VU=06/2C)=S+XF Lags=630Ops=)

Notice 53,078 dops (since Sat Apr 27 06:55:52 2002)
TCP Sequence Prediction: Class/window positive increments
Diffjoulty=3222829 (Good Luck!)
IPID Sequence Generation: Duplicated Iid (1)

Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
root@bigguy:~#
```



Nessus

- Best of the scanning tools
- Easy to build for Linux, harder for Solaris & HPUX, need to work on other OS.
- Requires GNU tools
- Provides HTML based reports
- Has distributed architecture: clients (Windows, Unix) & engines (Unix only)



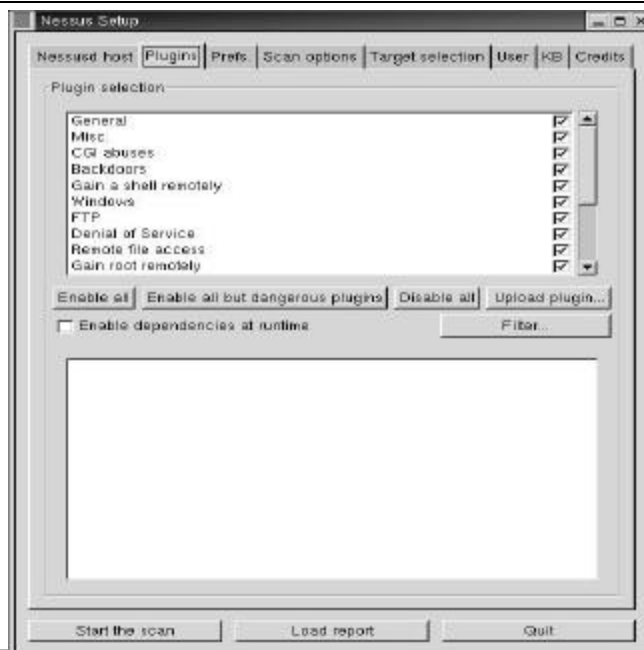
Nessus – Building It

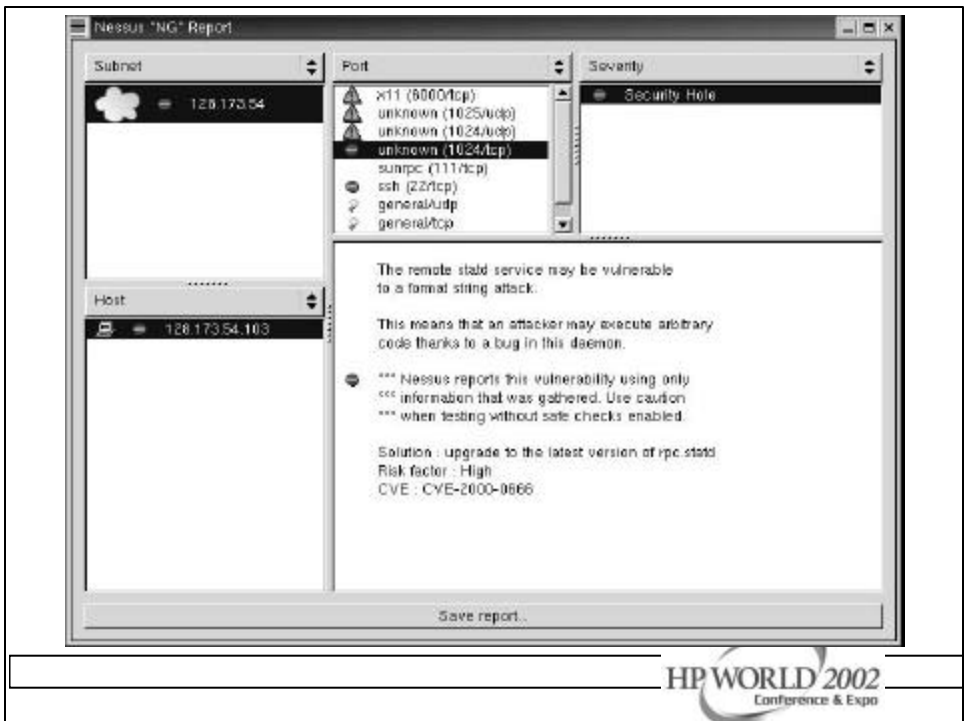
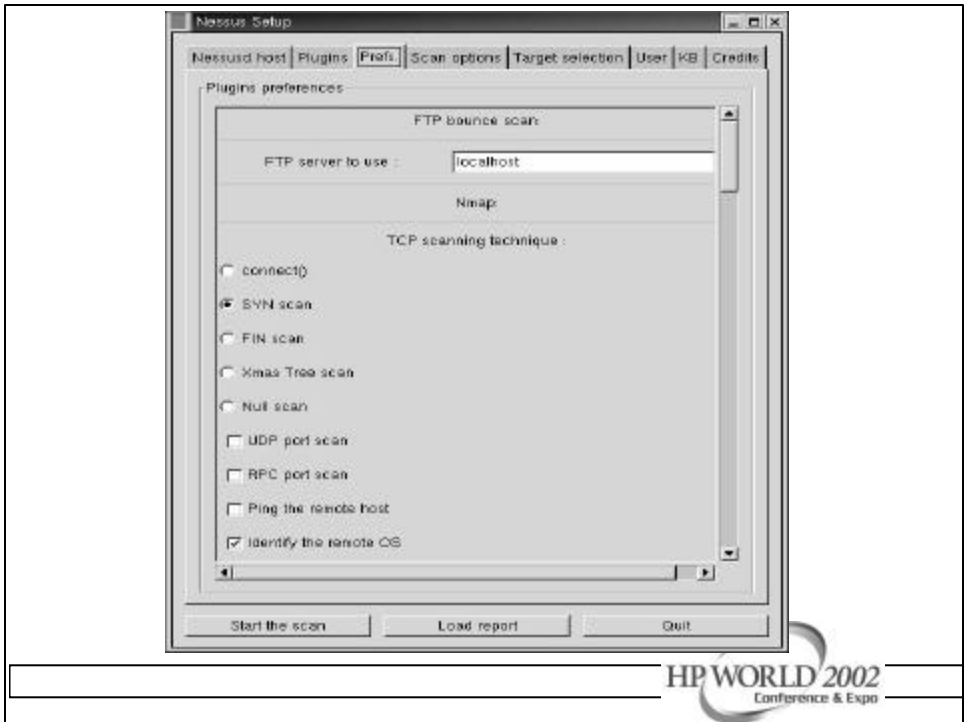
- Linux
 - Download the RPMs
 - Add nessus user
 - Start up nessusd daemon
 - Start up nessus client
 - Start testing
- Windows Client
 - Download executable & run



Nessus – Pros/Cons

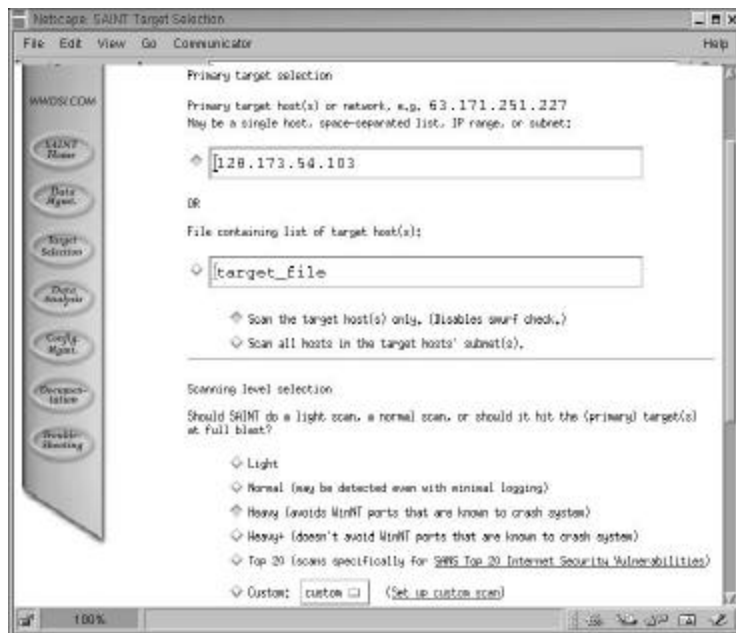
- Pros
 - Easy to install if you have linux
 - Most comprehensive tests for your money
- Cons
 - Not that easy to understand at first
 - Non-linux builds require GNU software
 - Some inconsistency in quality of checks
 - Must use Unix server for specific user accounts

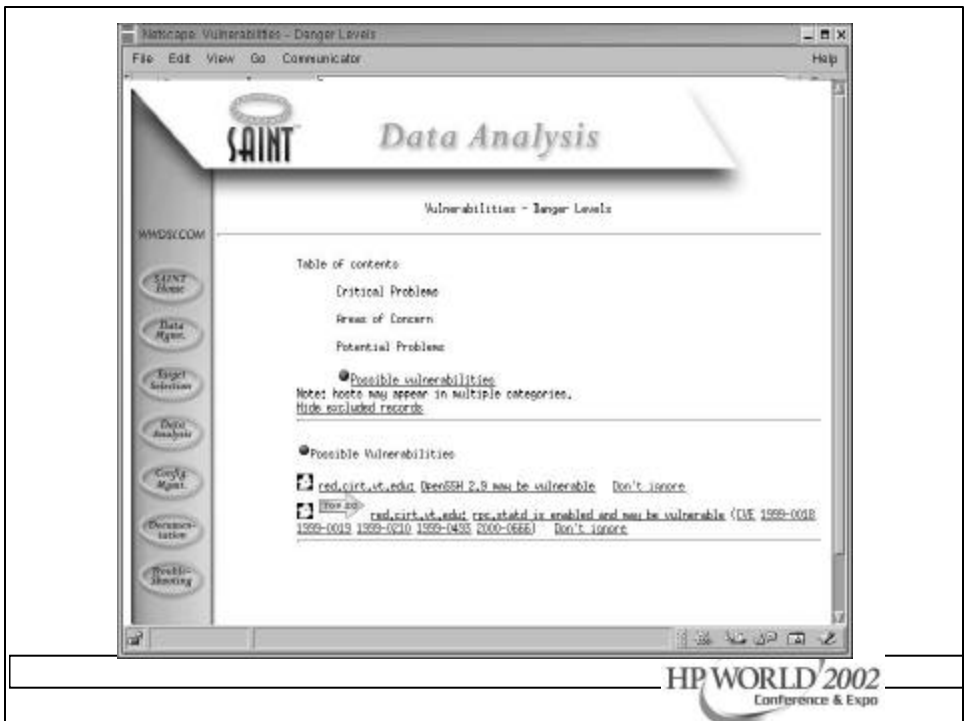
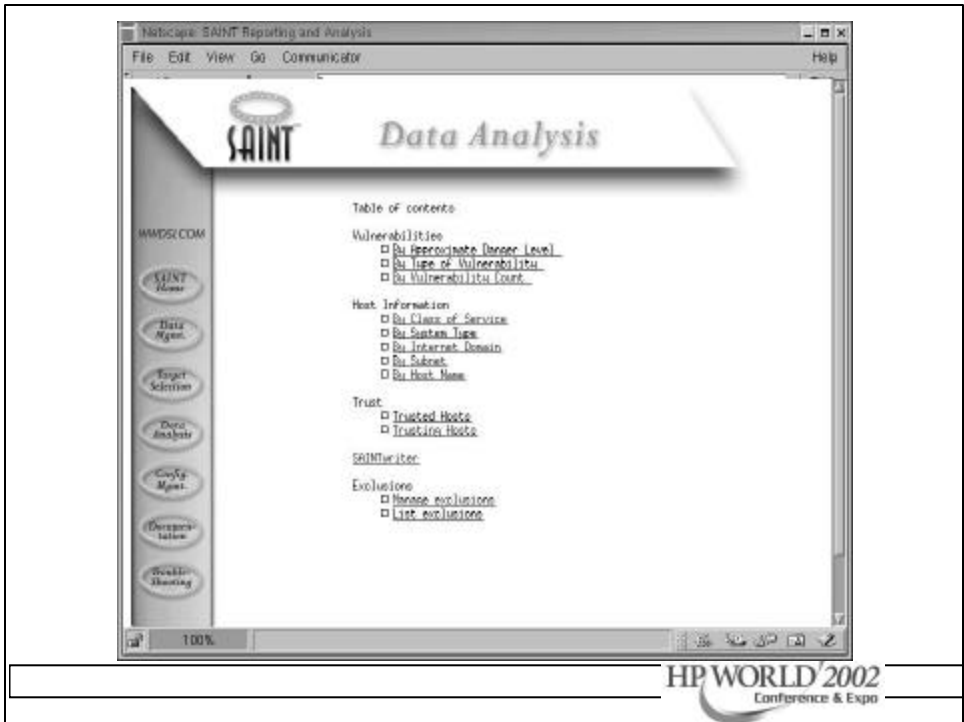




SAINT

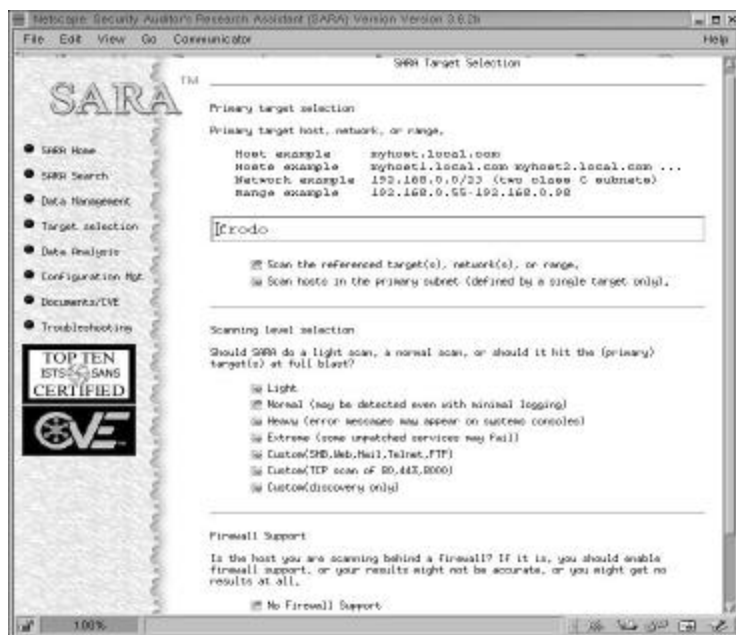
- Based on SATAN
- Security Administrator's Integrated Network Tool
 - Gathers info on remote hosts/nets
 - Looks at finger, NFS, NIS, ftp, tftp, rexd, statd
 - Can run heavy, moderate or light probes on targets.
- Will check for the SANS Top 20 Threats

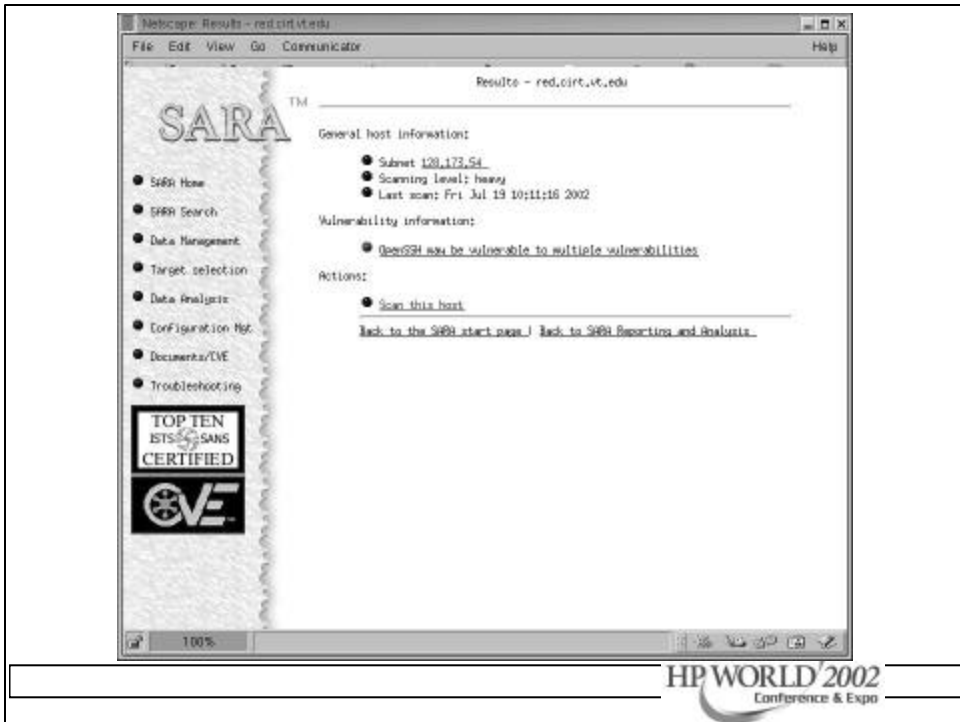




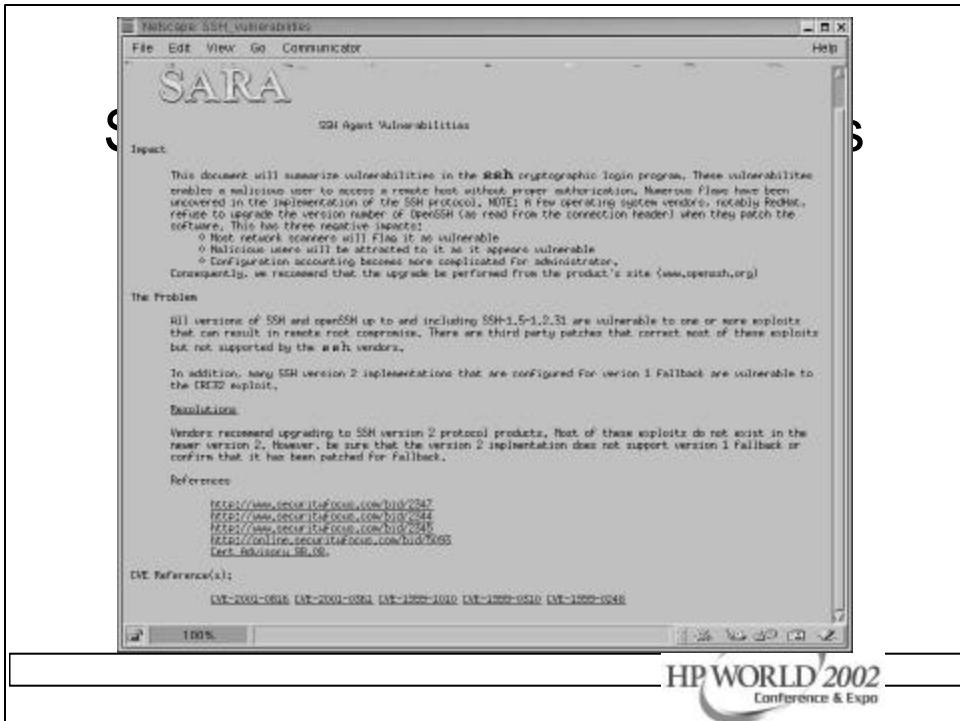
SARA

- Security Auditor's Research Assistant
- Checks for SANS Top 20 Threats
- Does Unix/Windows vulnerability tests
- Has CVE dictionary support
- Search engine for post audit analysis
- Uses CIS Benchmarks
- Has a Report Writer

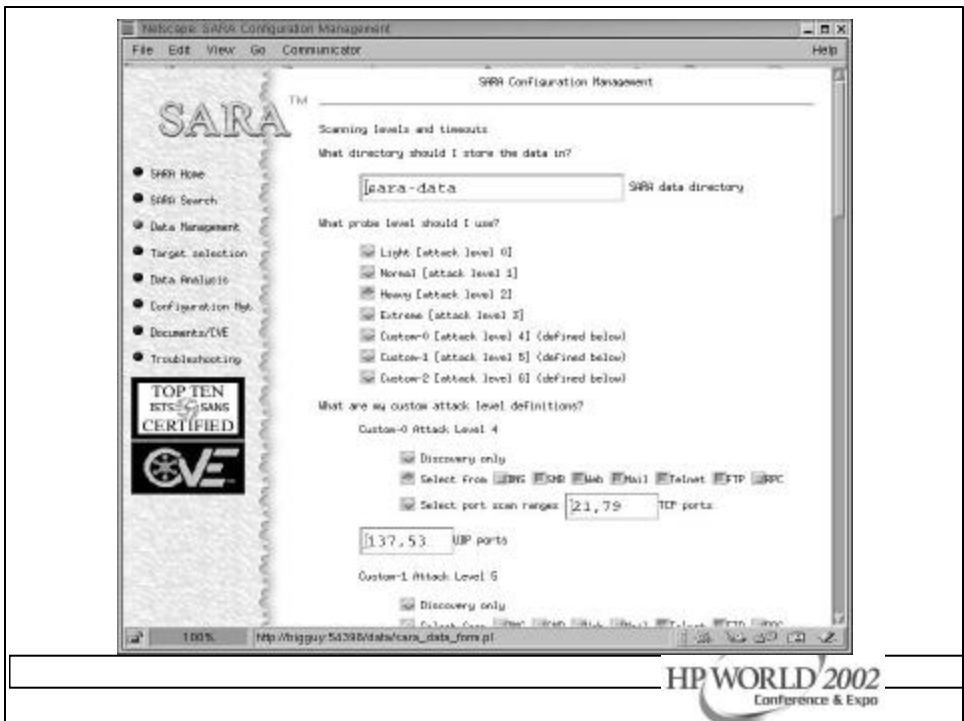
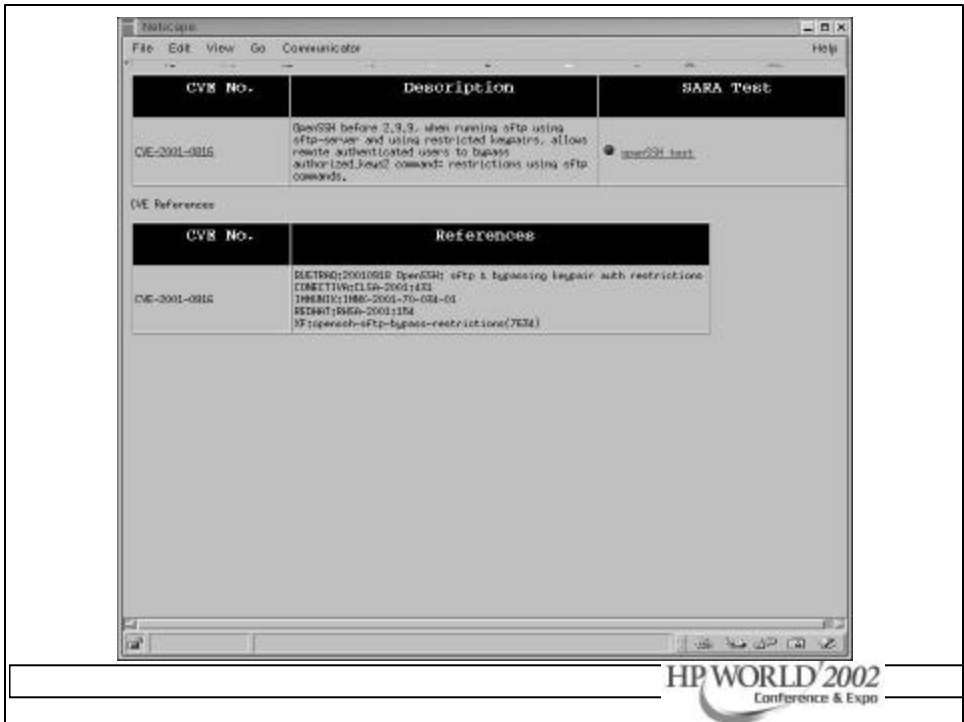




HP WORLD 2002
Conference & Expo



HP WORLD 2002
Conference & Expo



Tripwire

- First of the file integrity checkers
- Useful in finding trojan programs
- Unix and NT versions available
 - Network capable versions available
- Academic version & back level versions are free. Commercial and NT versions are not.



Tripwire

- Generates a "signature" for each file based on checksums and other characteristics.
- These signatures are stored in a database file that should be kept offline.
- This is the baseline.
- Latest threat involves dynamic exec redirection. This is part of the newer Kernel Module Rootkits.



Tripwire

- Security Issues
 - Need to protect the DB
 - Need to protect the vulnerable executables
- Advantages
 - Simple interface, good choice of crypto hash functions, good all-around tool
- Disadvantages
 - Kernel mod attacks, initial tw.config takes some time to customize, NT version is good but costs \$\$\$, no network security



```
Window Edit Options Help
Tripwire(TM) Tripwire Detection Software v1.3
This release is for single CPU, single site, and use purposes. For commercial
applications or product information, please visit the Visual Computing
Corporation web site at http://www.visualcomputing.com/tripwire, or call us
at (203) 223-0280.

Tripwire(TM) Copyright 1997-98 by The Purdue Research Foundation of Purdue
University, and distributed by Visual Computing Corporation under exclusive
licensing arrangements.

*** Phase 1: Reading configuration file
*** Phase 2: Generating file list
/usr/local/bin/tw/temporal: /etc/hosts: No such file or directory
/usr/local/bin/tw/temporal: /usr/profile: No such file or directory
/usr/local/bin/tw/temporal: /usr/logout: No such file or directory
/usr/local/bin/tw/temporal: /usr/utmp: No such file or directory
/usr/local/bin/tw/temporal: /kernel/unix: No such file or directory
/usr/local/bin/tw/temporal: /etc/hosts-equiva: No such file or directory
/usr/local/bin/tw/temporal: /hfsboot: No such file or directory
/usr/local/bin/tw/temporal: /ufsboot: No such file or directory
*** Phase 3: Creating file information database
*** Phase 4: Searching for inconsistencies
***
*** Total files scanned: 36238
*** Files added: 0
*** Files deleted: 0
*** Files changed: 7
*** Total file violations: 7
***
changed: -rw-r--r-- root 0 Aug 18 14:56:41 2000 /etc/.mrttab.lock
changed: -rw-r--r-- root 5702 Aug 16 15:14:26 2000 /etc/inet/inetd.conf
changed: prw----- root 0 Aug 18 11:28:59 2000 /etc/inetdps
changed: -rw-r--r-- root 767 Aug 18 14:56:41 2000 /etc/mrttab
changed: -rw-rw-rw root 8 Aug 18 14:58:46 2000 /etc/tripwire.11
changed: -rw-r--r-- root 512 Aug 16 17:58:36 2000 /etc/ssh_random_seed
changed: prw----- root 0 Aug 18 11:38:50 2000 /etc/utmpipr
*** Phase 5: Generating observed/expected pairs for changed files
***
*** Attr Observed (what it is) Expected (what it should be)
***
/etc/.mrttab.lock
at_mtime: Fri Aug 16 14:56:41 2000 Wed Aug 9 15:07:47 2000
at_mtime: Fri Aug 18 14:56:41 2000 Wed Aug 9 15:07:47 2000
/etc/inet/inetd.conf
st_size: 5702 S699
at_mtime: Wed Aug 16 15:14:26 2000 Mon Feb 21 10:11:29 2000
More files...
```



Portsentry/TCP Wrappers

- TCP Wrappers available from a ton of sites
- Any host that scans a list of “banned” ports is placed in an /etc/hosts.deny file
- Need TCP Wrappers installed on the machine
 - Tcprawappers logs attempts to connect to services



TCP Wrappers

- Purpose
 - Log network connections to a system
 - Allow you to filter who connects to the system
- Needs an inetd-like program to act as the dispatcher of network services
- Everyone should buy Wietse Venema dinner for writing this tool. 😊



TCP Wrappers Features

- Allows you to monitor/filter incoming requests for SYSTAT, FINGER, FTP, TELNET, R-Commands, TFTP, TALK and other network services.
- Provides access control to restrict what systems connect to what network daemons.
- Provides some protection from host spoofing



TCP Wrappers

- Access Control is enabled by default.
- 2 files
 - /etc/hosts.deny – restrict access if IP addr here
 - /etc/hosts.allow – allow access if IP addr here
 - Can restrict to username@host if services are enabled
- Reverse lookup is done. Paranoid selection terminates the connection immediately if there's a mismatch.
- Set KILL_IP_OPTIONS in Makefile to refuse connections that use source routing. This prevents IP spoofing although your routers should do this.



TCP Wrappers

- **Advantages**
 - Logs and applies access controls to remote connections
 - Lets you define which daemons are wrapped
 - Does good reverse lookup on hosts
- **Disadvantages**
 - Ident service not reliable
 - Only looks at network daemons spawned by inetd
 - Doesn't wrap ALL services (RPC)
 - Could give a false sense of security



Port Sentry

- Monitors ports and performs an action when an attempt to access the port is made.
- Usually access is denied to the probing systems.
- Monitors TCP and UDP traffic. A little more flexible than TCP Wrappers



```
Window Edit Options Help
# I like to always keep some ports at the "low" end of the spectrum.
# This will detect a sequential port sweep really quickly and usually
# these ports are not in use (i.e. tcpmux port 1)
#
# ** X-Windows Users **: If you are running X on your box, you need to be sure
# you are not binding PortSentry to port 6000 (or port 2000 for OpenWindows users).
# Doing so will prevent the X-client from starting properly.
#
# These port bindings are *ignored* for Advanced Stealth Scan Detection Mode.
#
# Un-comment these if you are really anal:
#TCP_PORTS="1,7,9,11,15,70,70,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,
2001,4000,4001,5742,6000,6001,6667,12345,12346,20034,30303,32771,32772,32773,32774,31337,40421,40425
,49724,54320"
#UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,32770,327
71,32772,32773,32774,31337,54321"
#
# Use these if you just want to be aware:
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,31337,32771,327
72,32773,32774,40421,49724,54320"
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,32770,32771,32772,32773,32774,31337,54321"
#
# Use these for just bare-bones
#TCP_PORTS="1,11,15,110,111,143,540,635,1080,524,2000,12345,12346,20034,32771,32772,32773,32774,4972
4,54320"
#UDP_PORTS="1,7,9,69,161,162,513,640,700,32770,32771,32772,32773,32774,31337,54321"
#####
# Advanced Stealth Scan Detection Options #
#####
#
# This is the number of ports you want PortSentry to monitor in Advanced mode.
# Any port *below* this number will be monitored. Right now it watches
# everything below 1023.
#
#portsentry.com: (206)
```

HP WORLD 2002
Conference & Expo

Personal Firewall Tools

- These tools monitor connection attempts to your system and give you the option of allowing or denying the access
- They log the connection attempt to standard log files
- Each system must be configured.

IP Filter/HP IPFILTER 9000

- Software package that can do NAT and other basic firewall services.
- Designed to be used as a loadable kernel module but can be incorporated into a Unix kernel
- Can be configured to do IP Accounting (count # bytes), IP Filtering or IP authentication or NAT.
- swinstall-able – HP Product # B9901-90001



```
File Edit View Go Communicator Help
@Members @WebMail @Connections @BizJournal @Smartupdate @FTPbase
...$ bookmarks & Location http://occebs.snu.edu.au/~awaion/rules.html
Back Forward Reload Home Search Netscape Print Security Shop Stop

# block all incoming TCP packets on tcp from host "foo" to any destination.
Block in on tcp proto tcp from foo/32 to any

#
# block all outgoing TCP packets on tcp from any host to port 23 of host bar.
Block out on tcp proto tcp from any to bar/32 port 23

#
# block all inbound packets.
Block in from any to any
# pass through packets to and from localhost.
pass in from 127.0.0.1/32 to 127.0.0.1/32
# allow a variety of individual hosts to send any type of IP packet to any
# other host.
pass in from 10.1.1.1 to any
pass in from 10.1.1.2 to any
pass in from 10.1.1.3 to any
pass in from 10.1.1.4 to any
pass in from 10.1.1.5 to any
pass in from 10.1.0.1/24 to any
pass in from 10.1.1.1/32 to any
pass in from 10.1.0.1/32 to any
#
# block all outbound packets.
Block out from any to any
# allow any packets destined for localhost out.
pass out from any to 127.0.0.1/32
#
# allow any host to send any IP packet out to a limited number of hosts.
#
pass out from any to 10.1.1.1/32
pass out from any to 10.1.1.2/32
pass out from any to 10.1.1.3/32
pass out from any to 10.1.1.4/32
pass out from any to 10.1.1.5/32
pass out from any to 10.1.0.1/24
pass out from any to 10.1.1.1/32
pass out from any to 10.1.1.1/32
```

“Ipfiler
Commands”



Ipfiler output

```
Jul 30 01:46:52 myhost.      ipmon[147]: [ID
702911local0.warning] 01:46:52.196772 hme0 @0:5 b
194.143.66.126,21 ->198.82.255.255,21 PR tcp len 20 40 -S IN

Jul 30 01:47:03 myhost.      ipmon[147]: [ID
702911local0.warning] 01:47:03.269595 hme0 @0:5 b
194.143.66.126,21 ->198.82.255.255,21 PR tcp len 20 40 -S IN

Jul 30 05:53:51 myhost.      ipmon[147]: [ID
702911local0.warning] 05:53:50.699235 hme0 @0:5 b
203.90.84.163,1781 ->198.82.255.255,21 PR tcp len 20 60 -S IN
```



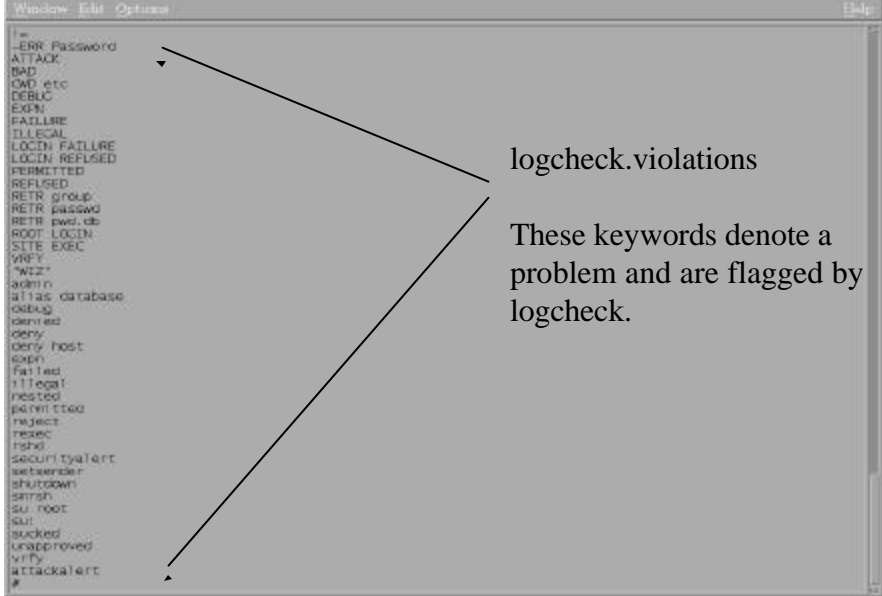
```
root@stguyv:~#
File Edit Settings Help
=====
echo "Building INPUT: LAN Interface Chain"
-----
#
# LAN interface restrictions:
# - ssh - Secure shell access from the LAN to the firewall
# - sftp - Secure file transfer from the LAN to the firewall
#
# Allow related packets
$IPTABLES -A input-lan-if -m state --state ESTABLISHED,RELATED -j ACCEPT
#
# ftp - (20/21/TCP) ftp
$IPTABLES -A input-lan-if -p tcp -m state --state NEW --dport ftp -j ACCEPT
$IPTABLES -A input-lan-if -p tcp --dport auth -j ACCEPT
#
# SSH - (22/TCP) Secure shell access
$IPTABLES -A input-lan-if -p tcp -m state --state new --dport ssh -j ACCEPT
#
# NTP - (123/TCP) NTP connections from local to External
echo " NTP (123/TCP) local -> External"
$IPTABLES -A input-lan-if -p udp -m state --state NEW -d 10.2.2.1 --dport ntp -j ACCEPT
#
# SFTP - (115/TCP) Secure ftp (over ssh)
$IPTABLES -A input-lan-if -p tcp -s BLANKUNET --dport sftp -j ACCEPT
#
# printer - (515/TCP-UDP) printer talk
$IPTABLES -A input-lan-if -p tcp -s BLANKUNET --dport printer -j ACCEPT
#
# SYSLOG - (514/UDP) System and kernel logging to central logging host.
#
$IPTABLES -A lan-if -p udp -s BLAN_IF_ADDR \
-d $SYSLOGHOST --dport syslog -j ACCEPT
#
# ICMP Chain Jump
$IPTABLES -A input-lan-if -j icmp-acc
#
# Reject remaining traffic
$IPTABLES -A input-lan-if -j LOG --log-prefix "input-lan-if BLKED PKT: "
$IPTABLES -A input-lan-if -j DROP
:~#
```

Iptable Commands



Logcheck

- Syslog keyword scanner
- When it matches something, it does something
 - Send email
 - Page someone
 - Run a command



A screenshot of a terminal window titled "Window Edit Options" showing a list of keywords. The list includes: -ERR Password, ATTACK, BAD, OAD etc, DEBUG, EXPI, FAILURE, ILLEGAL, LOGIN FAILURE, LOGIN REJECTED, PERMITTED, REJECTED, RETR group, RETR passwd, RETR pwd,db, ROOT LOGIN, SITE EXEC, VERIFY, *WIZ*, admin, alias database, onbug, denied, deny, deny host, expn, failed, illegal, rejected, permitted, reject, rexec, rshd, securityalert, selfsender, shutdown, smrsh, su root, su, sucked, unapproved, vrfy, attackalert, #. A large black arrow points from the text "logcheck.violations" to the list of keywords. Another arrow points from the text "These keywords denote a problem and are flagged by logcheck." to the same list.

logcheck.violations

These keywords denote a problem and are flagged by logcheck.



logcheck.ignore

Phrases listed in this file are ignored by the logcheck program.

```

Window Edit Options
-----
ftpd.*FTP LOGIN FROM
ftpd.*retrieved
ftpd.*stored
http-gw.*: exit host
http-gw.*: permit host
mail.local
nfsd.*Lane delegation
nfsd.*Response from
nfsd.*Answer queries
nfsd.*points to a CHASE
nfsd.*reloading
nfsd.*starting
netcat.*: exit host
netcat.*: permit host
popper.*Unable
popper: -ERR POP server at
gnat.*Free msg
gnat.*Info msg
gnat.*Starting delivery
gnat.*Delivery
gnat.*End msg
rlogin-gw.*: exit host
rlogin-gw.*: permit host
sendmail.*User Unknown
sendmail.*alias database.*rebuild
sendmail.*aliases.*longest
sendmail.*trace
sendmail.*last input channel
sendmail.*message-id
sendmail.*outgoing
sendmail.*return to sender
sendmail.*stats
sendmail.*timeout waiting
smtp.*Hosts
smtpd.daemon running
smtpd.*delivered
telnetd.*tloop: peer died
tftp-gw.*: exit host
tftp-gw.*: permit host
x-gw.*: exit host
x-gw.*: permit host
xntp.*Previous time adjustment didn't complete
xntp.*time reset
#
  
```

HP WORLD 2002
Conference & Expo

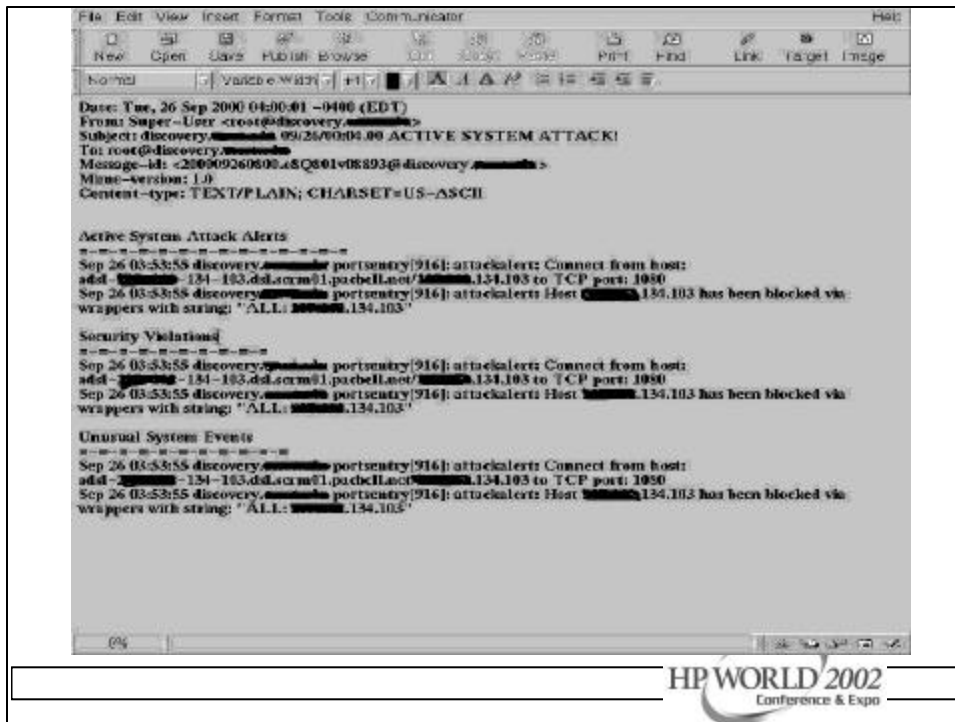
logcheck.hacking

Keywords in this file indicate an attack is taking place

```

Window Edit Options
-----
vrfy lp
vrfy daea
vrfy guest
vrfy root
vrfy uuap
vrfy oracle
vrfy sybase
vrfy games
vrfy dsx
vrfy dacode
vrfy uudecode
vrfy lp
vrfy daea
vrfy guest
vrfy root
vrfy uuap
vrfy oracle
vrfy sybase
vrfy games
exrn dacode
exrn uudecode
exrn wheel
exrn root
EXRN dacode
EXRN uudecode
EXRN wheel
EXRN root
LOGIN root REFUSED
rlognd.*: Connection from .* an illegal port
rshd.*: Connection from .* on illegal port
sendmail.*: user .* attempted to run daemon
uuap.*: refused connect from .*
tftpd.*: refused connect from .*
login.*: *LOGIN FAILURE.* FROM .*root
login.*: *LOGIN FAILURE.* FROM .*guest
login.*: *LOGIN FAILURE.* FROM .*bin
login.*: *LOGIN FAILURE.* FROM .*uuap
login.*: *LOGIN FAILURE.* FROM .*ads
login.*: *LOGIN FAILURE.* FROM .*bbs
login.*: *LOGIN FAILURE.* FROM .*games
login.*: *LOGIN FAILURE.* FROM .*sync
login.*: *LOGIN FAILURE.* FROM .*oracle
login.*: *LOGIN FAILURE.* FROM .*sybase
attackalert
#
  
```

HP WORLD 2002
Conference & Expo



Sniffers: snoop, iptrace, tcpdump, snort, windump

- Some systems have builtin sniffers
 - Solaris - snoop
 - AIX - iptrace
 - Linux/HP-UX – tcpdump, ethereal
 - 98/NT/2000 – netwatch, windump
- Tcpdump is the generic sniffer for those systems with no builtin sniffer

```

root@p03guy:~# tcpdump -i eth0 -s 1500 -w tcpdump.pcap 'port 110 or port 143'
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
14:47:37.676401 NHT-062.NRWDC.ORG.1622 > mail.i-plus.net.pcp3: S 19384468:19384468(0) win 8192 (res
1460, rnp, rnp, sackOK) (DF)
0x0000  4500 0030 207c 4000 8006 7e05 0a01 013e  E...0-|0...?....>
0x0010  d836 8bd1 0656 006e 012f 6964 0000 0000  .k...V.n./i.....
0x0020  7012 2000 e231 0000 0204 0564 0101 0402  p...i.....
14:47:37.733959 mail.i-plus.net.pcp3 > NHT-062.NRWDC.ORG.1622: S 1568728878:1568728878(0) ack 193844
68 win 17520 (res 1460, rnp, rnp, sackOK) (DF)
0x0000  4500 0030 7541 4000 7106 4540 d836 8bd1  E...0u0q,EO,k..
0x0010  0a01 013e 006e 0656 5680 e72e 012f 6965  ...n.V]..../i.
0x0020  7012 4470 3901 0000 0204 0564 0101 0402  p.Dp.....
14:47:37.733959 NHT-062.NRWDC.ORG.1622 > mail.i-plus.net.pcp3: . ack 1 win 8760 (DF)
0x0000  4500 0028 2e7c 4000 8006 7d8d 0a01 013e  E...|0...|....>
0x0010  d836 8bd1 0656 006e 012f 6965 5880 e72f  .k...V.n./i././
0x0020  5010 2230 87fd 0000 0000 0000 0000  P..%.....
14:47:37.810894 mail.i-plus.net.pcp3 > NHT-062.NRWDC.ORG.1622: P 1:56(56) ack 1 win 17520 (DF)
0x0000  4500 005f 7543 4000 7106 450f d836 8bd1  E...u00q,EO,k..
0x0010  0a01 013e 006e 0656 5680 e72f 012f 6965  ...n.V].../i.
0x0020  5018 4470 a65f 0000 2b4f 4b20 5831 204e  P.Dp...kK,kl,N
0x0030  542d 904f 5033 2053 6572 7665 7220 692d  T-POP3,Server,i-
0x0040  706c 7573 2e6e 6574 2028 494d 6168 6c20  plus.net.(Pmail.
0x0050  7e2e 8036 2034 3339 3538 2d36 2904 0a  6.06.42658-6)...
14:47:37.811447 NHT-062.NRWDC.ORG.1622 > mail.i-plus.net.pcp3: P 1:16(16) ack 56 win 8706 (DF)
0x0000  4500 0037 2f7c 4000 8006 7b7e 0a01 013e  E...7|0...|....>
0x0010  d836 8bd1 0656 006e 012f 6965 5880 e766  .k...V.n./i./..f
0x0020  5018 2201 057e 0000 5553 4552 206a 6d63  P...".USER,jc
0x0030  696e 7479 723d 0a  intgr..
14:47:38.012796 mail.i-plus.net.pcp3 > NHT-062.NRWDC.ORG.1622: . ack 16 win 17506 (DF)
0x0000  4500 0028 7959 4000 7106 4530 d836 8bd1  E...(u)0q,EO,k..
0x0010  0a01 013e 006e 0656 5680 e766 012f 69c4  ...n.V]...F./i.
0x0020  5010 4461 629e 0000 1401 0000 0a00  P.Dae.....

```

TCPDUMP Command



```

tcpdump -i eth0 -s 1500 -w tcpdump.pcap 'port 110 or port 143'
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
14:47:37.676401 NHT-062.NRWDC.ORG.1622 > mail.i-plus.net.pcp3: S 19384468:19384468(0) win 8192 (res
1460, rnp, rnp, sackOK) (DF)
14:47:37.733959 mail.i-plus.net.pcp3 > NHT-062.NRWDC.ORG.1622: S 1568728878:1568728878(0) ack 193844
68 win 17520 (res 1460, rnp, rnp, sackOK) (DF)
14:47:37.733959 NHT-062.NRWDC.ORG.1622 > mail.i-plus.net.pcp3: . ack 1 win 8760 (DF)
14:47:37.810894 mail.i-plus.net.pcp3 > NHT-062.NRWDC.ORG.1622: P 1:56(56) ack 1 win 17520 (DF)
14:47:37.811447 NHT-062.NRWDC.ORG.1622 > mail.i-plus.net.pcp3: P 1:16(16) ack 56 win 8706 (DF)
14:47:38.012796 mail.i-plus.net.pcp3 > NHT-062.NRWDC.ORG.1622: . ack 16 win 17506 (DF)

```

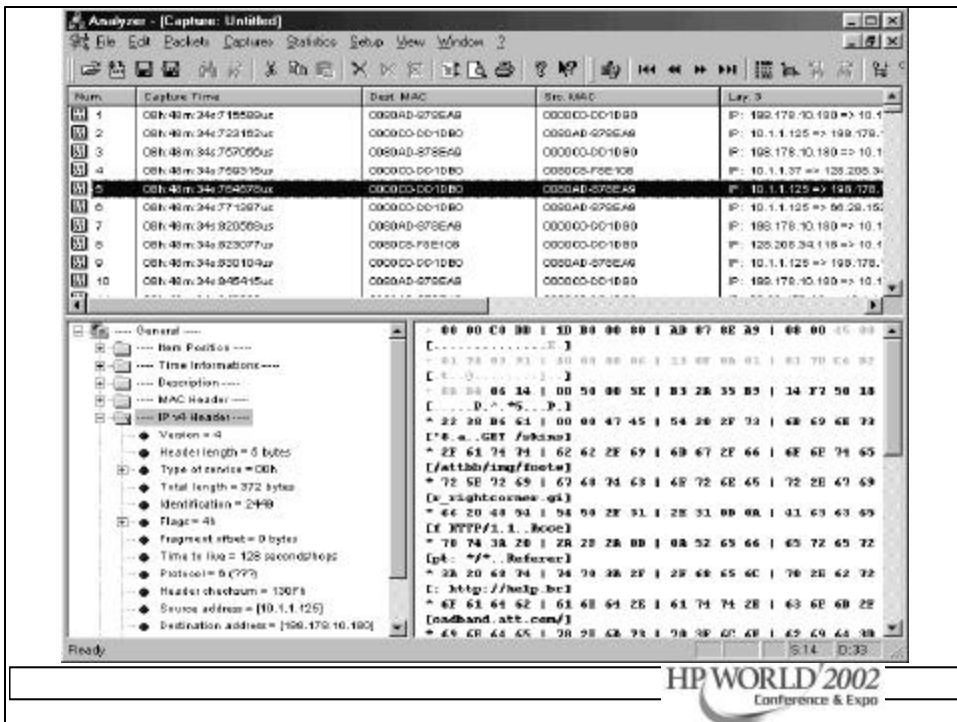
No.	Time	Source	Destination	Protocol	Info
282	2001-09-15 10:42:11.9610	10.1.1.69	10.1.1.69	TCP	1464 > pop3 [ACK] Seq=69657659 Win=4
283	2001-09-15 10:42:12.6237	10.1.1.69	10.1.1.69	TCP	Response: 408 DPOP Version: 3.4a. 4
284	2001-09-15 10:42:12.6240	10.1.1.69	10.1.1.69	TCP	Request: USER a
285	2001-09-15 10:42:13.2394	10.1.1.69	10.1.1.69	TCP	pop3 > 1464 [ACK] Seq=2574009280 A
286	2001-09-15 10:42:13.2396	10.1.1.69	10.1.1.69	TCP	Response: 408 al nice to hear from
287	2001-09-15 10:42:13.8810	10.1.1.69	10.1.1.69	TCP	Request: PASS shony
288	2001-09-15 10:42:13.9611	10.1.1.69	10.1.1.69	TCP	Response: 408 al hat O mail server
289	2001-09-15 10:42:13.9638	10.1.1.69	10.1.1.69	TCP	Request: STAT
290	2001-09-15 10:42:14.6079	10.1.1.69	10.1.1.69	TCP	Response: 408 O n
291	2001-09-15 10:42:14.6082	10.1.1.69	10.1.1.69	TCP	Request: QUIT
292	2001-09-15 10:42:15.2332	10.1.1.69	10.1.1.69	TCP	Response: 408 POP a
303	2001-09-15 10:42:15.2541	10.1.1.69	10.1.1.69	TCP	pop3 > 1464 [FIN, ACK] Seq=15740000
304	2001-09-15 10:42:15.2542	10.1.1.69	10.1.1.69	TCP	1464 > pop3 [ACK] Seq=69657660 Ac
305	2001-09-15 10:42:15.2612	10.1.1.69	10.1.1.69	TCP	1464 > pop3 [FIN, ACK] Seq=6965766
306	2001-09-15 10:42:15.9249	10.1.1.69	10.1.1.69	TCP	pop2 > 1464 [ACK] Seq=2574009280 A

```

Frame 297 (67 on wire, 67 captured)
Ethernet II
  Destination: 00:00:c0:00:00:00 (00:00:c0:00:00:00)
  Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Type: IP (0x0900)
  Internet Protocol Version 4, Src Addr: 10.1.1.69 (10.1.1.69), Dest Addr: 10.1.1.69 (10.1.1.69)
  Transmission Control Protocol, Src Port: 1464 (1464), Dest Port: pop3 (110), Seq: 69657660, Ack: 2574009280
  Source seq#: 1464 (1464)
  Destination port: pop3 (110)
  Sequence number: 69657660
  Next sequence number: 69657661
  Acknowledgment number: 2574009280
  Header length: 20 bytes
  Flags: 0x0010 (FIN, ACK)
  0... .. * Congestion Window Reduced (CWR): Not set

```





Intrusion Detection Systems - IDS

- Snort
- Shadow
- HP IDS/9000

Microsoft Internet Explorer window: **SmartSnarf: Smart signatures in /var/log/smart/alert**

File Edit View Go Communicator Help

SILICON DEFENSE SmartSnarf start page
All Smart signatures
SmartSnarf v000816.1

[Signature section \(358\)](#) [Top 20 source IPs](#) [Top 20 dest. IPs](#)

358 alerts found using input module SmartFileInput, with sources:

- /var/log/smart/alert

Earliest alert at 14:25:42.98126 on 07/19/2002
Latest alert at 14:52:58.418651 on 07/19/2002

[Top 20 source IPs](#)
[Top 20 destination IPs](#)

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dest.	Detail link
2	MEB-HISC /doc/ access [sig]	1	1	1	Summary
2	NETBIOS SMB IPC\$access [sig]	2	2	1	Summary
2	NETBIOS NT NULL session [sig]	2	1	1	Summary
2	MEB-IIS scripts access [sig]	2	1	1	Summary
2	MEB-HISC search.dll access [sig]	6	1	2	Summary
2	SNMP public access sub [sig]	10	1	1	Summary
2	LOP PING WWP [sig]	330	3	2	Summary
1	SMTP RCPT TO overflow [sig]	1	1	1	Summary
1	FTP USER overflow attempt [sig]	4	1	1	Summary

100%

HP WORLD 2002
Conference & Expo

Microsoft Internet Explorer window: **SmartSnarf: All alerts going to 63.171.251.15 in /var/log/smart/alert**

File Edit View Go Communicator Help

SILICON DEFENSE SmartSnarf alert page
Destination: 63.171.251.15
SmartSnarf v000816.1

[Signature section \(358\)](#) [Top 20 source IPs](#) [Top 20 dest. IPs](#)

1 such alerts found using input module SmartFileInput, with sources:

- /var/log/smart/alert

Earliest: 14:49:07.090845 on 07/19/2002
Latest: 14:49:07.090845 on 07/19/2002

1 different signatures are present for 63.171.251.15 as a destination

- 1 instances of SMTP RCPT TO overflow

There are 1 distinct source IPs in the alerts of the type on this page.

Whois lookup at:	ARIN	RIPE	APNIC	Geotools
63.171.251.15	Amesnet	TELUME	Durincast	
Raw lookup links:	Whois	Sam Spade		

07/19-14:49:07.090845 [**] [1:654:5] SMTP RCPT TO overflow [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1] (TCP) 10.1.1.41:2380 -> 63.171.251.15:25

SmartSnarf brought to you courtesy of Silicon Defense
Authors: Jim Headland and Stuart Staniford
See also the [Sign Page](#) by Mark Roscoe
Page generated at Fri Jul 19 14:55:00 2002

HP WORLD 2002
Conference & Expo

ShortSnarf summary page
Top 10 destination IPs
ShortSnarf v020316.1

Signature section (356) Top 20 source IPs Top 20 dest IPs

This page provides summary information about alerts acquired using Inet module ShortFileInet, with sources:
• /var/log/short/alert

The most active destination IPs are shown. Rank is determined by the number of alerts with that IP as the destination. Within a rank, IPs are sorted by # of signatures, then by IP number.

Rank	Total # Alerts	Destination IP	# Signatures triggered	Originating sources
rank #1	328 alerts	207.26.131.137	1 signatures	10.1.1.79
rank #2	10 alerts	10.1.1.2	1 signatures	10.1.1.2
rank #3	6 alerts	216.35.157.20	1 signatures	10.1.1.45
rank #4	4 alerts	10.1.1.2	2 signatures	13 source IPs
		193.26.0.20	1 signatures	63,171,251,227
rank #5	2 alerts	216.35.22.215	1 signatures	10.1.1.106, 10.1.1.108
		216.58.231.57	1 signatures	10.1.1.79
rank #6	1 alerts	63.171.251.15	1 signatures	10.1.1.45
		66.130.134.131	1 signatures	10.1.1.45
		193.26.0.20	1 signatures	63,171,251,227

ShortSnarf brought to you courtesy of Silicon Defense
Authors: Jim Hoasland and Stuart Similford
See also the Short Page by Karu Roshni
Page generated at Fri Jul 19 14:53:00 2002

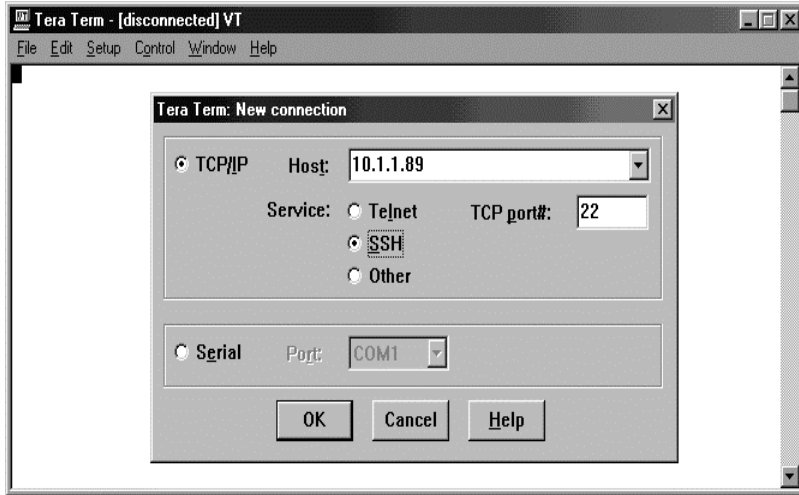
HP WORLD 2002
Conference & Expo

SSH Connectivity Tool

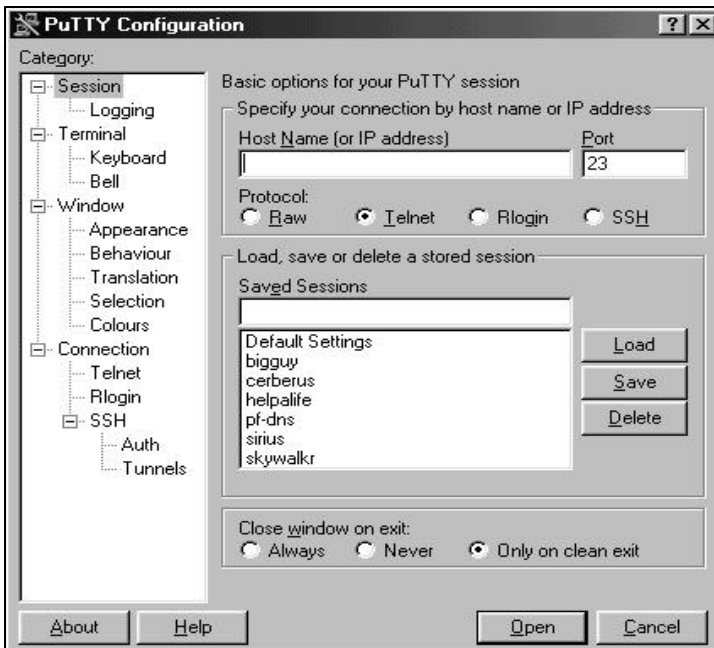
- Client / Server Application
- Encrypted Data Transmission
- Destination Host Verification
- Port forwarding via encrypted data channel
- Access authorization based on userid or IP address

HP WORLD 2002
Conference & Expo

SSH - TeraTerm



HP WORLD 2002
Conference & Expo



SSH -
Putty

HP WORLD 2002
Conference & Expo

Big Brother

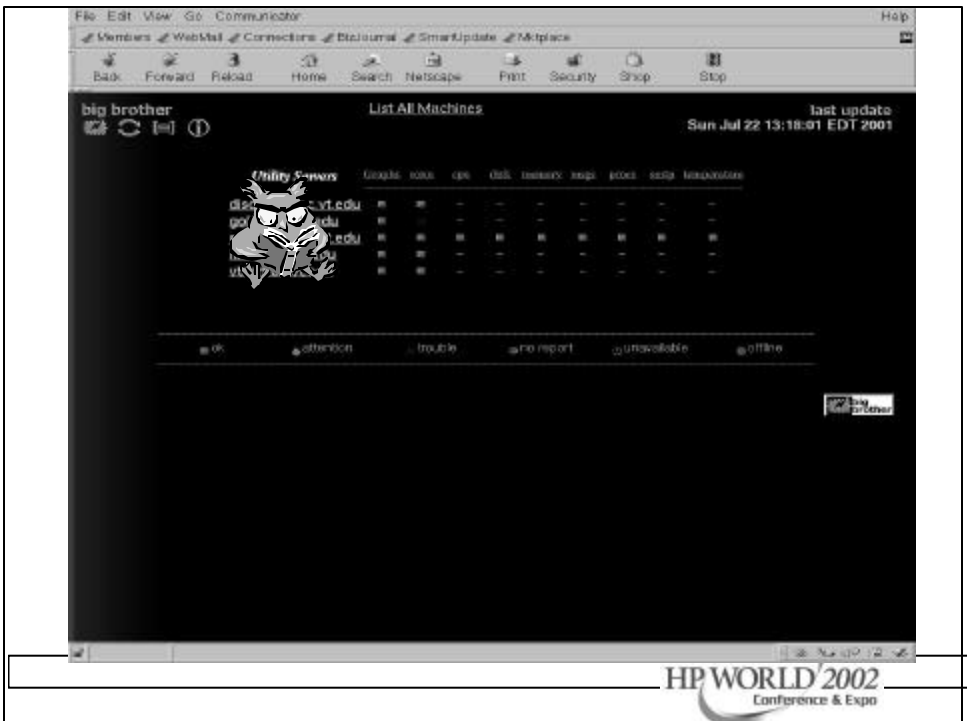
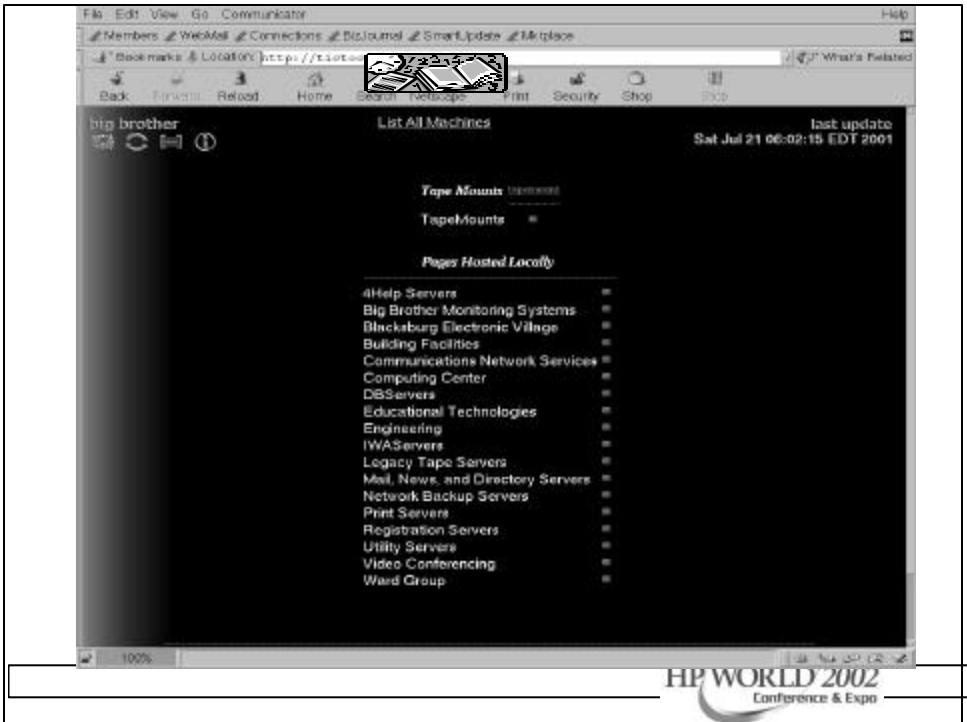
- Web based system and network monitor
- Client server model
 - Clients run on the systems you want to monitor
 - Simple shell scripts that monitor different aspects of your system and network
- What can it check?
 - Disk space, CPU Utilization, critical processes, weather parameters, building monitors

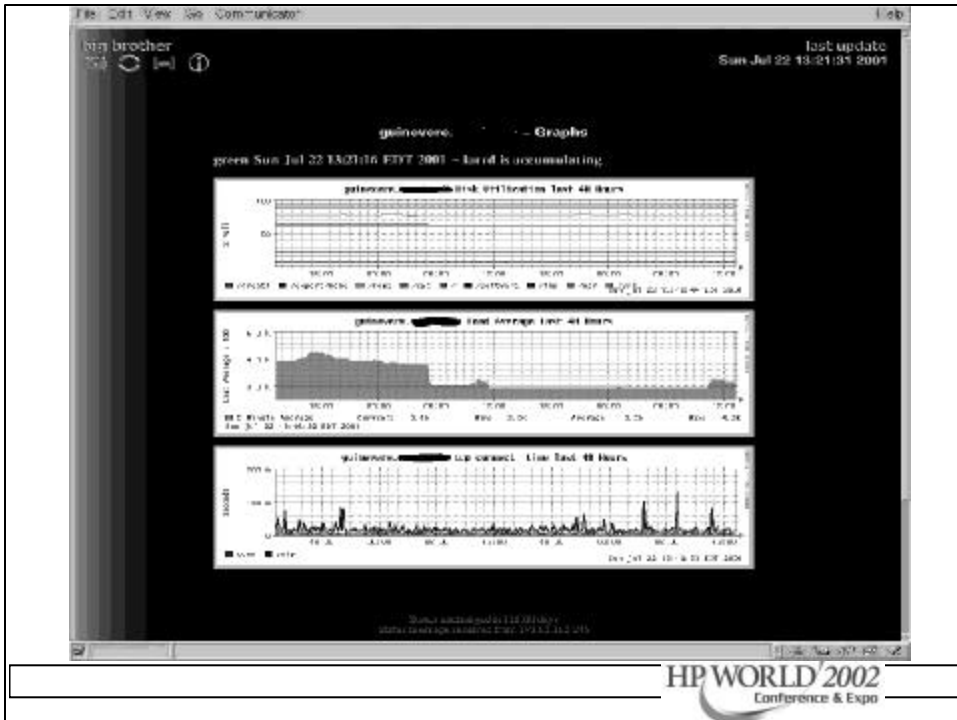


Big Brother

- Color coded WWW page showing a matrix of machines and monitored functions
- Notifies sysadmins by email, pager, SMS.
- System requirements
 - Unix – www server, /bin/sh, C compiler to port BB
 - NT – v4.0 with SP3 minimum, Intel or Alpha platforms.





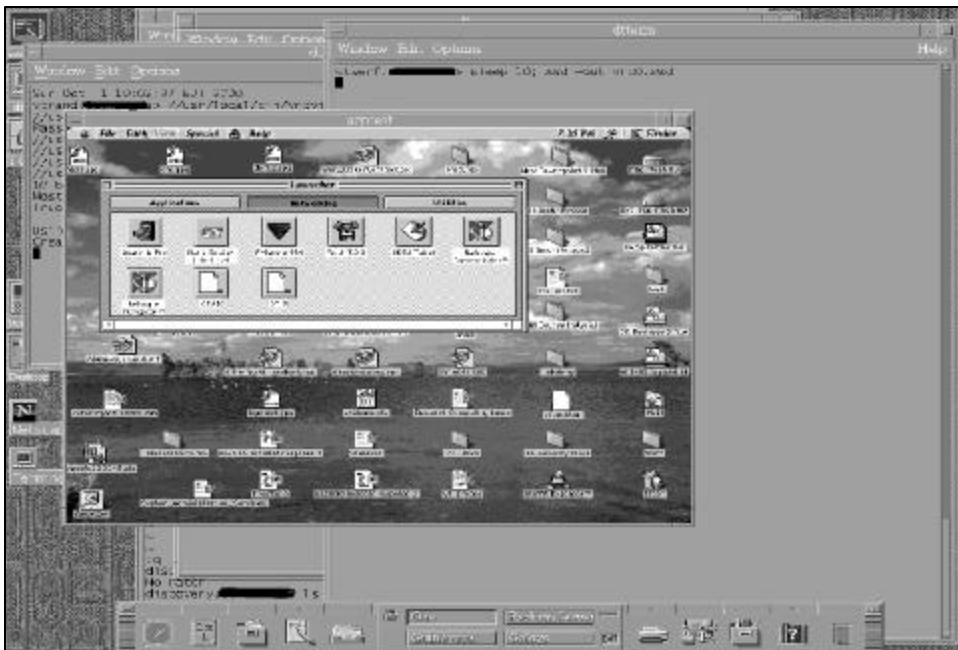


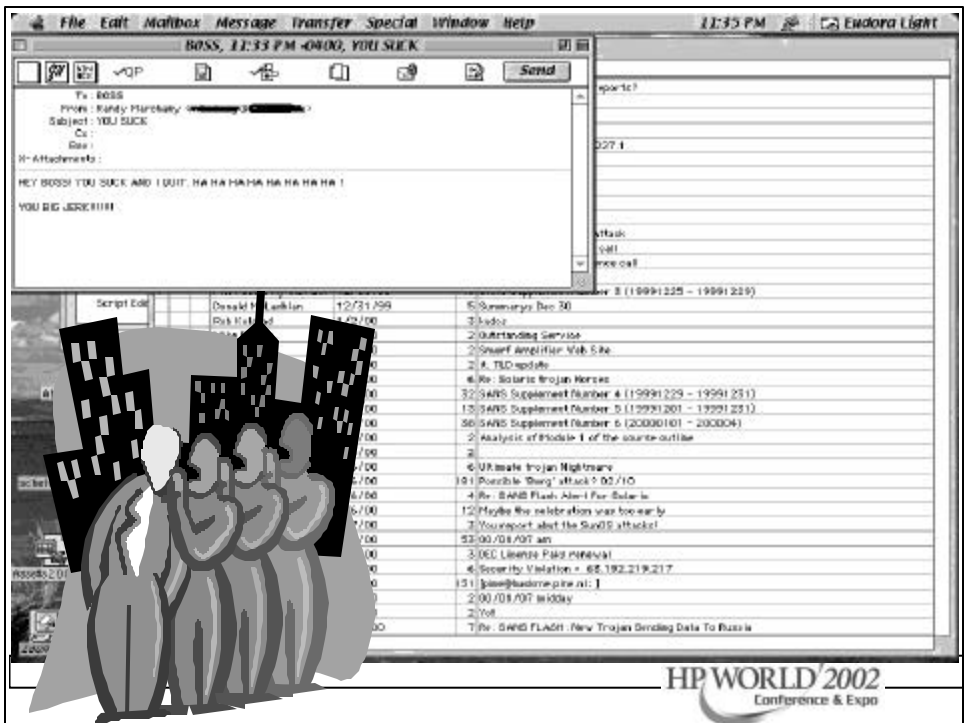
Big Brother

- Can monitor more service by modifying `bb-network.sh`
- BB shows historical data. Drilling down a host page and clicking on the history buttons shows the last 24 hr stats.
- Doesn't need to run as root. Run as 'bb'.
- Restricts incoming connections by ACL.

VNCViewer

- Great remote control tool for Windows 95/98, NT, 2000, XP, Macintosh, Unix clients
- Nice help desk tool
- It displays the remote desktop on your system.
- A better version of BackOrifice, BO2K tool
- Brought to you by your friends at AT&T





Lsof, inzider, filemon

- These programs list the processes running on a system.
- They also list the files opened by those processes.
- Useful in finding where a sniffer log file is located



Lsof
Utility
Output

```

root@biggy:/usr/local/src/logcheck-1.1.1
# lsof -p 4089
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
sshd 4089 root cwd DIR 3,8 1024 2 /
sshd 4089 root rld DIR 3,8 1024 2 /
sshd 4089 root txt REG 3,9 238152 132788 /usr/sbin/sshd
sshd 4089 root mem REG 3,8 494250 61310 /lib/ld-2.2.4.so
sshd 4089 root mem REG 3,8 12000 8187 /lib/security/pam_stack.so
sshd 4089 root mem REG 3,8 6487 8180 /lib/security/pam_nologin.so
sshd 4089 root mem REG 3,8 14717 8174 /lib/security/pam_limits.so
sshd 4089 root mem REG 3,8 4894 8206 /lib/security/pam_deny.so
sshd 4089 root mem REG 3,8 35424 61202 /lib/libc.so.0.75
sshd 4089 root mem REG 3,8 65887 61214 /lib/libc-2.2.4.so
sshd 4089 root mem REG 3,8 263407 61246 /lib/libresolv-2.2.4.so
sshd 4089 root mem REG 3,8 47822 61254 /lib/libutil-2.2.4.so
sshd 4089 root mem REG 3,9 59778 64677 /usr/lib/libz.so.1.1.3
sshd 4089 root mem REG 3,8 436384 61219 /lib/libnsl-2.2.4.so
sshd 4089 root mem REG 3,8 818752 61276 /lib/libcrypto.so.0.9.6b
sshd 4089 root mem REG 3,9 425483 96830 /usr/karberos/lib/libkrb5.so.3.0
sshd 4089 root mem REG 3,9 78183 96825 /usr/karberos/lib/libk5crypto.so.3.0
sshd 4089 root mem REG 3,9 8713 96820 /usr/karberos/lib/libk5sasl.so.3.0
sshd 4089 root mem REG 3,8 5779542 73448 /lib/libnsl/libc-2.2.4.so
sshd 4089 root mem REG 3,8 262272 61225 /lib/libnss_files-2.2.4.so
sshd 4089 root mem D#R 1,5 11150 /dev/tty0
sshd 4089 root mem REG 3,8 50891 8185 /lib/security/pam_console.so
sshd 4089 root mem REG 3,8 13025 8207 /lib/security/pam_err.so
sshd 4089 root mem REG 3,8 14636 8205 /lib/security/pam_cracklib.so
sshd 4089 root mem REG 3,9 182363 64462 /usr/lib/libglib-1.2.so.0.0.10
sshd 4089 root mem REG 3,8 305236 61243 /lib/libnss_nisplus-2.2.4.so
sshd 4089 root mem REG 3,8 71888 61232 /lib/libnss_dns-2.2.4.so
sshd 4089 root mem REG 3,8 48678 8191 /lib/security/pam_unix.so
sshd 4089 root mem REG 3,8 55115 61212 /lib/libcrypt-2.2.4.so
sshd 4089 root mem REG 3,9 69084 64452 /usr/lib/libcrack.so.2.7
sshd 4089 root mem D#R 1,5 11150 /dev/tty0
sshd 4089 root Ou D#R 1,3 5203 /dev/null
sshd 4089 root lu D#R 1,3 5203 /dev/null
sshd 4089 root 2u D#R 1,3 5203 /dev/null
sshd 4089 root 4u IPv4 1258537 TCP biggy:ssh->NAT-062.NVDC.ORG:1029 (ESTABLISHED)
sshd 4089 root 5u unix (/var/empty) 1258560 socket
root@biggy:/usr/local/src/logcheck-1.1.1
#
    
```



Document - WordPad

File Edit View Insert Format Help

(c) 1999, Arne Vidstrom - <http://www.ntsecurity.nu/toolbox/inzider/>

Checked C:\LOGITECH\MOUSE\SYSTEM\EM_EXEC.EXE (PID=429477753)
Checked C:\WINDOWS\SYSTEM\DDHELP.EXE (PID=4294187141)
Checked C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\POWERPNT.EXE (PID=4294511325)
Checked C:\WINDOWS\EXPLORER.EXE (PID=4294891201)
Checked C:\PROGRAM FILES\INTERNET EXPLORER\EXPLORE.EXE (PID=4294268533)
Found UDP port 1344 bound at 127.0.0.1 by C:\PROGRAM FILES\INTERNET EXPLORER\EXPLORE.EXE (PID=4294268533) [UDP client]
Checked C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\OUTLOOK.EXE (PID=4294452161)
Checked C:\PROGRAM FILES\ADOBE\ACROBAT 5.0\READER\ACRODRD32.EXE (PID=4294517333)
Checked C:\WINDOWS\SYSTEM\KERNEL32.DLL (PID=4294948741)

inzider

HP WORLD 2002
Conference & Expo

Sysadmin Tools

- **Sudo**
 - Unix access control is all (root) or nothing (user).
 - Some commands (backup, restore) are restricted to root but are really an OPER class command. You don't want an operator to have root access but you want them to do backups.
 - Sudo lets you set up this "pseudo" privilege scheme.

Sudo

- The sudoers files lists the commands, shells, hosts that a user can execute commands
- Should always specify the full path name for the commands
- Notifies sysadmins if illegal uses of sudo is attempted.
- Notifies sysadmins if user in sudoers tries to run a restricted command



Sudo

- Advantages
 - Good warning if someone tries to use it incorrectly.
 - Easy to configure for multiple machines
 - Adequate internal security checks
 - Check for "." in PATH
 - Removes LD* variables before execution
- Disadvantages
 - Works with root userid only. Can't use with other userids.
 - Doesn't handle commands that use a subshell to spawn other commands



Proactive Password Tools

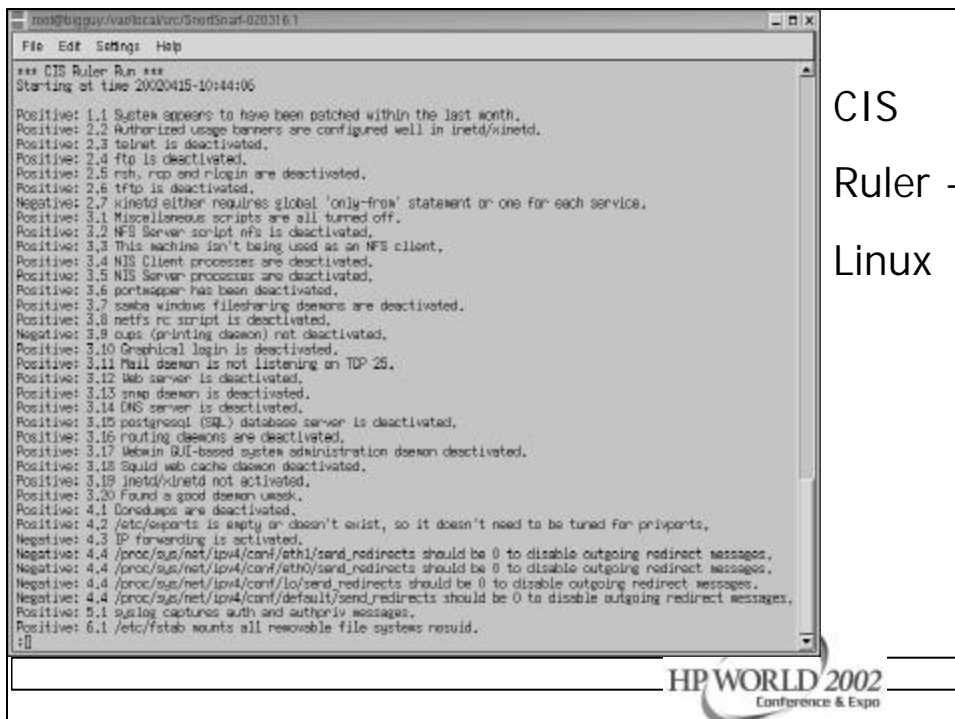
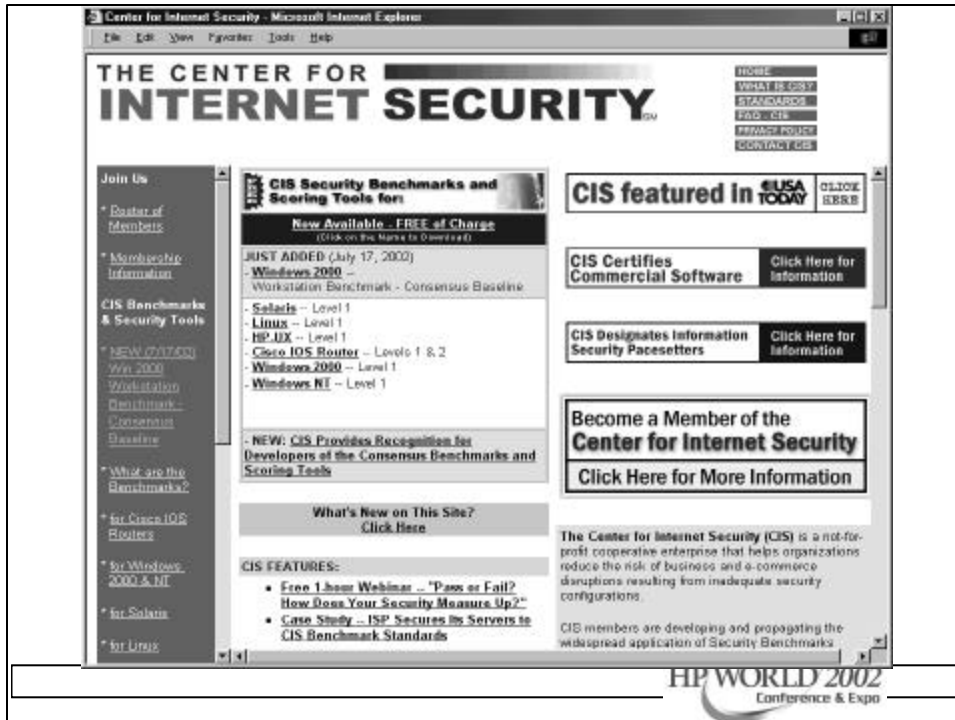
- Most newer OS allow you to set password rules in config files.
- Npasswd and passwd+ are two older but still effective tools.
- Npasswd is a good tool for those who don't want to spend a lot of time configuring a password checker
- Passwd+ requires more configuration time.



Crack - l0phtcrack

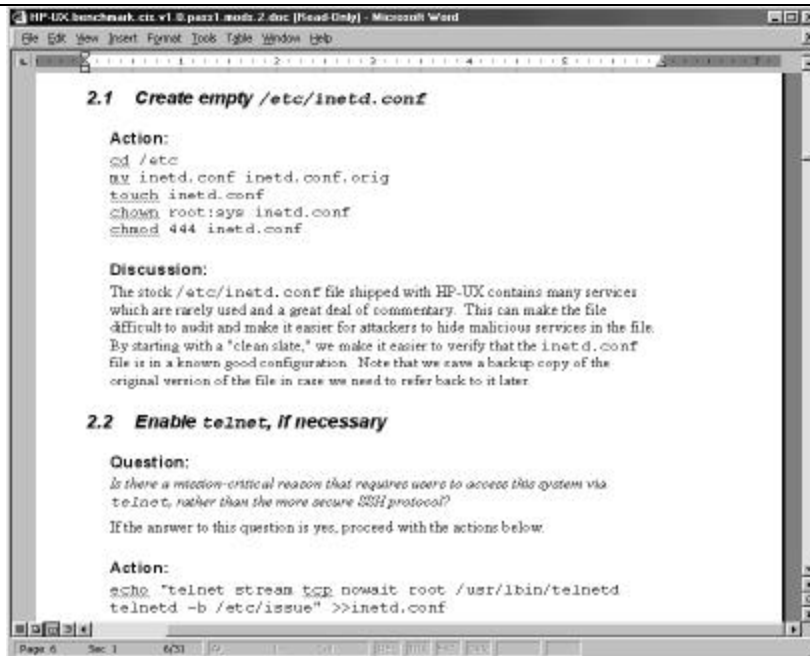
- The first of the really good password crackers. Available on the net for the past 10 years.
- Easy to customize. Works on non-shadow password files.
- Use a preprocessor to rebuild in old format or use NIS, NIS+ ☺
- Can be distributed among systems
- Have AUTHORIZATION to RUN !!!





CIS
Ruler -
Linux

CIS
Manual
- HPUX



Summary

- There are some excellent freeware tools that will help you with sysadmin and security issues at your site.
- Use these tools to gain experience in evaluating vendor tools.
- A combination of vendor and freeware tools is desired
- There are MORE tools out there!

Questions ?



Co-author

Randy Marchany – Director Security Testing
Lab, Virginia Tech



Where to Get the Tools

- www.ciac.org/ciac/
 - TCP Wrappers, crack, tcpdump, lsof, windump
- www.networkingfiles.com/SecurityApps/saint.htm
 - SAINT
- www.www-arc.com/sara
 - SARA
- www.tripwire.com or www.tripwire.org
 - tripwire



Where to Get the Tools

- www.psionic.com
 - Logcheck, portentry
- www.uk.research.att.com/vnc
 - VNCViewer
- www.insecure.org
 - Nmap
- www.openssh.org or hpux.cs.utah.edu/
 - SSH



Where to Get the Tools

- www.nessus.org
 - Nessus
- www.packetstormsecurity.org
 - Hacker tools
- bb4.com
 - Big Brother
- www.ethereal.com
 - Ethereal
- analyzer.polito.it
 - analyzer



Where to Get the Tools

- coombs.anu.edu.au/~avalon/ip-filter.html
 - Ipfiler or HP Ipfiler/9000
- www.snort.org
 - Snort, SnortSnarf, SnortSort
- devresource.hp.com
- hpux.cs.utah.edu
- thewrittenword.com
- www.interex.org
- www.software.hp.com

