

# Building a Secure Environment for Free !

## HP World 2002

James G. McIntyre

*McIntyre & Associates, Inc.*

Radford, VA 24141

[jmcintyr@i-plus.net](mailto:jmcintyr@i-plus.net)

540-633-6379



## McIntyre & Associates, Inc.

At McIntyre & Associates, we use our 30+ years of computer and network experience to deliver comprehensive and cost effective security measures. In fact, we are a SANS GCIA expert based company – a distinction awarded to only approximately 500 individuals worldwide.

Based in Virginia, the company serves businesses ranging from startups to Fortune 1000 companies across the country. The security services provided by us include: firewalls, intrusion detection systems, risk analysis, security scans, and security audits. We also provide all aspects of system administration services for HP-UX and Linux. For more information, check out our website at [www.mcintyresecurity.com](http://www.mcintyresecurity.com)



## 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
  - PortSentry
- System Firewalls
  - ipfilters, iptables, ipchains
- Personal Firewalls
  - ZoneAlarm, BlackIce, Tiny



## The Tools

- Syslog Scanners
  - LogSentry
  - 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, process-explorer/inzider/fport (NT)
  - Sudo (unix/NT)
- **Remote Control Tools**
  - VNCviewer
- **System Security Analyzers**
  - CIS Benchmarks
  - HP-UX Bastille
  - HP-UX Security Patch Check



## 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://www.insecure.org) &
  - [hpux.cs.utah.edu/](http://hpux.cs.utah.edu/)
- Nessus, Saint, Sara, Satan



```
root@biggy:~# nmap -v 10.2.2.2

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
No tcp,udp, or ICMP scantype specified, assuming vanilla tcp connect() scan. Use
-sP if you really don't want to see what hosts are up).
Host skywalker (10.2.2.2) appears to be up ... good.
Initiating Connect() Scan against skywalker (10.2.2.2)
Adding TCP port 5000 (state open).
Adding TCP port 80 (state open).
Adding TCP port 139 (state open).
Adding TCP port 22 (state open).
The Connect() Scan took 139 seconds to scan 1342 ports.
Interesting ports on skywalker (10.2.2.2):
(The 1529 ports scanned but not shown below are in state: filtered)
Port      State      Service
21/tcp    closed    ftp
22/tcp    open      ssh
80/tcp    open      http
113/tcp   closed    auth
115/tcp   closed    sftp
139/tcp   open      netbios-ssn
515/tcp   closed    printer
5800/tcp  closed    vnc
5801/tcp  closed    vnc
5900/tcp  closed    vnc
5901/tcp  closed    vnc-1
6000/tcp  open      X11
6001/tcp  closed    x11:1

Nmap run completed -- 1 IP address (1 host up) scanned in 139 seconds
You have new mail in /var/spool/mail/root
root@biggy:~#
```



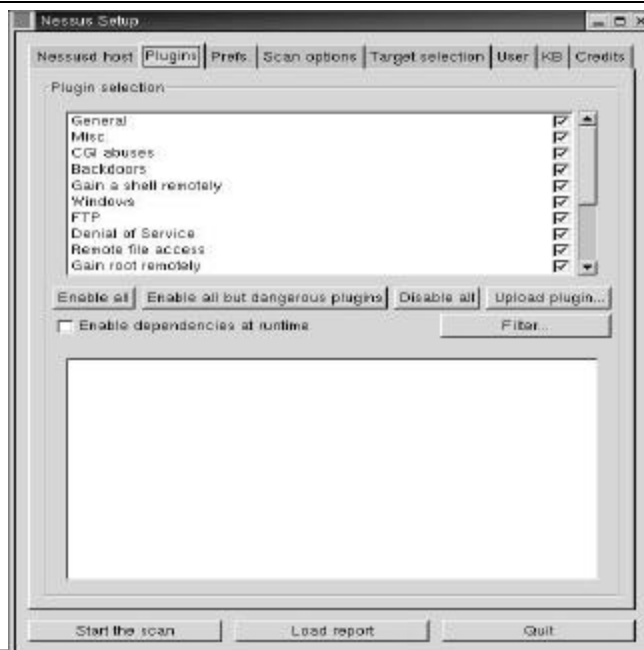
## Nessus

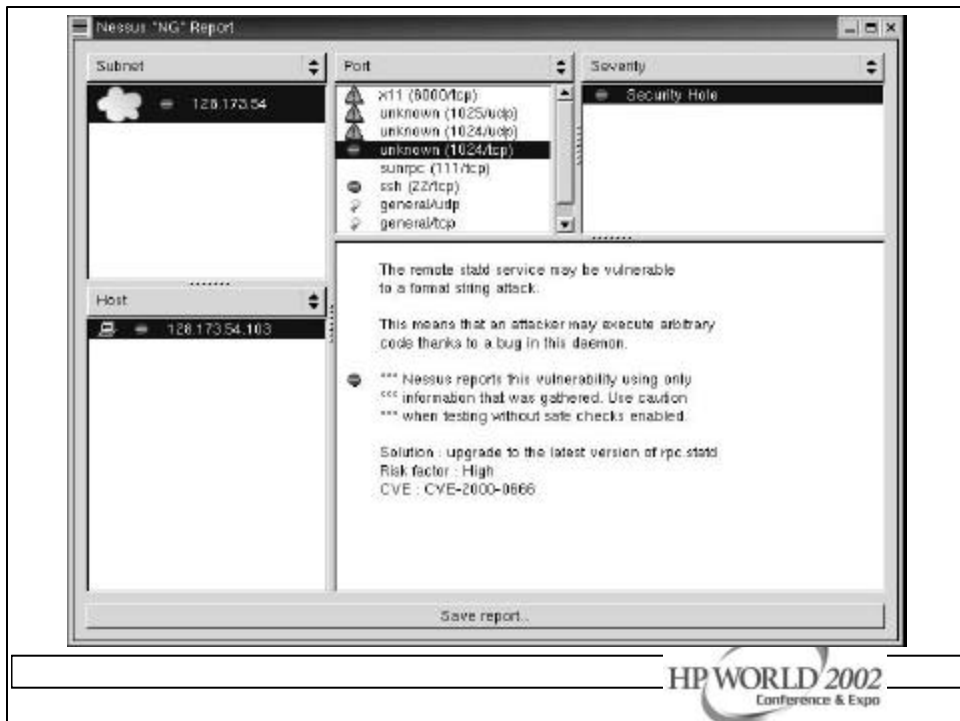
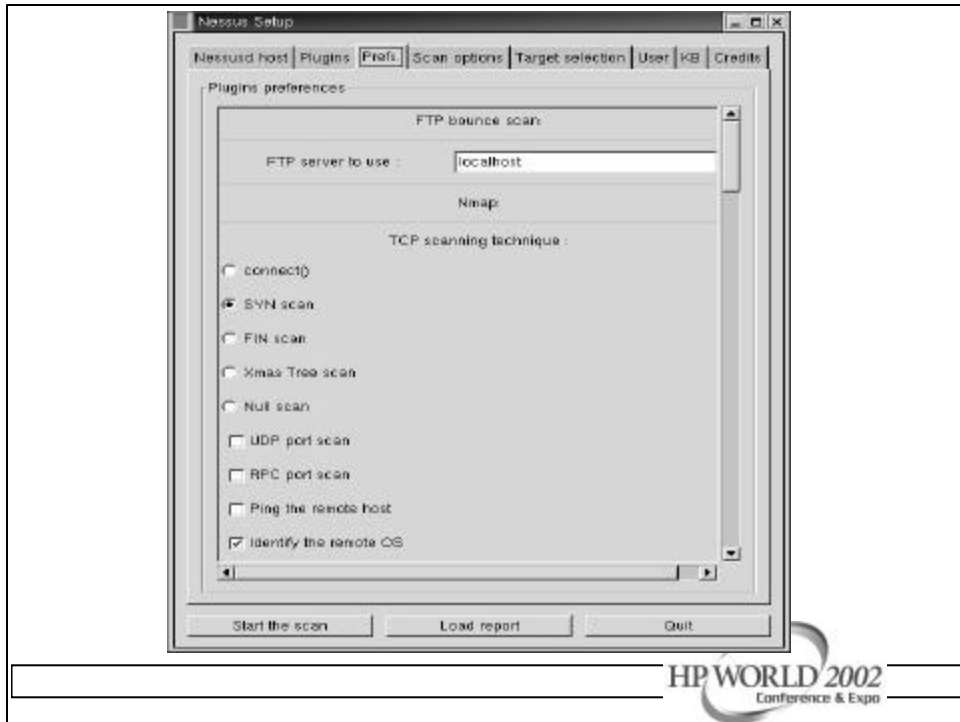
- Best of the scanning tools
- Easy to build for Linux, harder for Solaris & HPUX, need to work on other OS.
- Requires GNU tools
- Provides HTML based reports
- Has distributed architecture: clients (Windows, Unix) & engines (Unix only)



# Nessus – 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

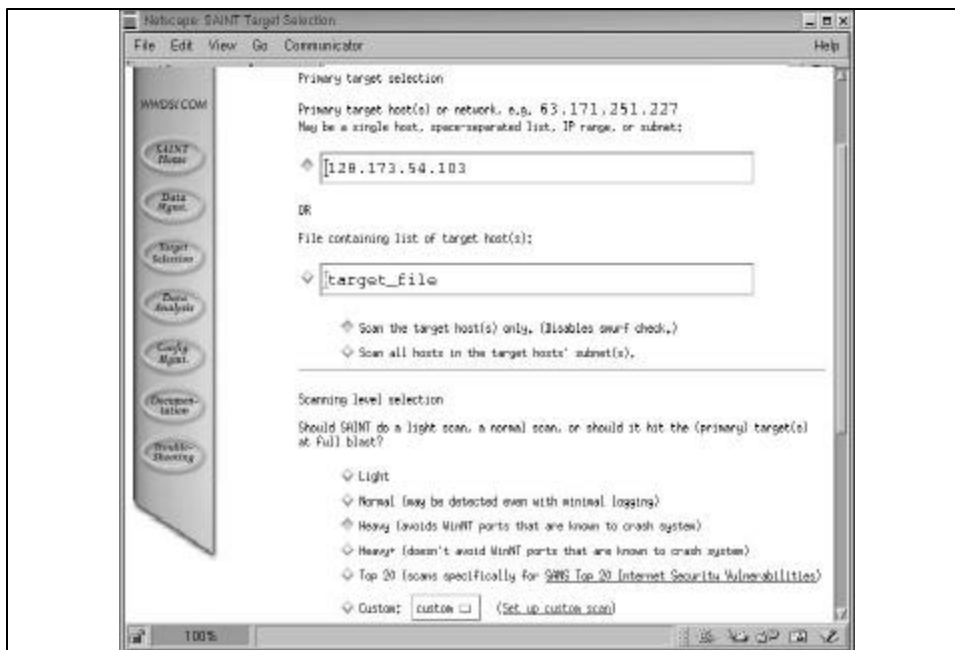




# SAINT

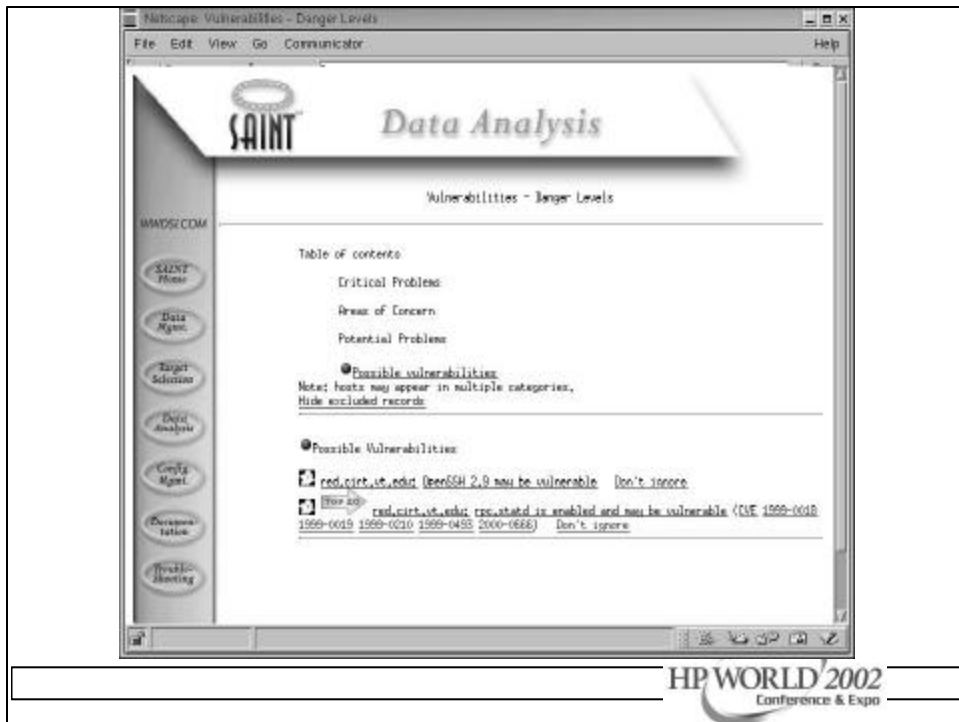
- Based on SATAN
- Security Administrator's Integrated Network Tool
  - Gathers info on remote hosts/nets
  - Looks at finger, NFS, NIS, ftp, tftp, rexd, statd
  - Can run heavy, moderate or light probes on targets.
- Will check for the SANS Top 20 Threats

HP WORLD 2002  
Conference & Expo



HP WORLD 2002  
Conference & Expo

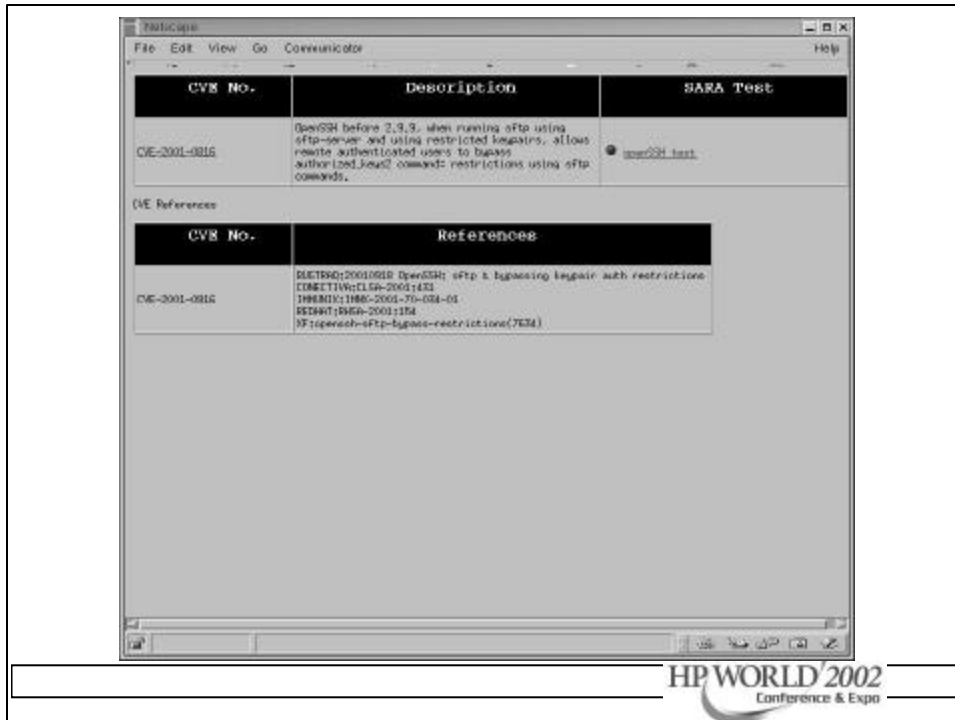




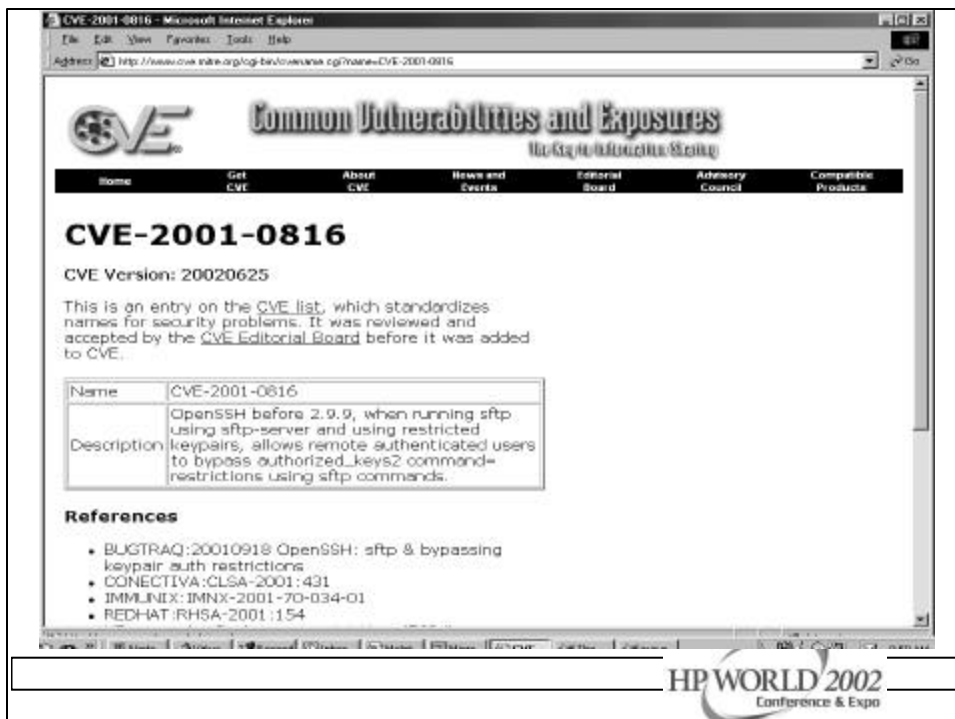
## SARA

- Security Auditor's Research Assistant
- Checks for SANS Top 20 Threats
- Does Unix/Windows vulnerability tests
- Has CVE dictionary support
  - Common Vulnerabilities & Exposure
- 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 \$\$\$



```
Window Edit Options Help
Tripwire(C:\) 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(C:\) 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/tripwire: /etc/hosts: No such file or directory
/usr/local/bin/tw/tripwire: /usr/profile: No such file or directory
/usr/local/bin/tw/tripwire: /usr/logout: No such file or directory
/usr/local/bin/tw/tripwire: /usr/utmp: No such file or directory
/usr/local/bin/tw/tripwire: /kernel/unix: No such file or directory
/usr/local/bin/tw/tripwire: /etc/hosts-equivalent: No such file or directory
/usr/local/bin/tw/tripwire: /hsfsboot: No such file or directory
/usr/local/bin/tw/tripwire: /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/inetd.pid
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----- root 512 Aug 16 17:58:36 2000 /etc/ssh_random_seed
changed: prw----- root 0 Aug 18 11:38:50 2000 /etc/utmp.pid
### Phase 5: Generating observed/expected pairs for changed files
###
### Attr Observed (what it is) Expected (what it should be)
### -----
/etc/.mrttab.lock
st_mtime: Fri Aug 16 14:56:41 2000 Wed Aug 9 15:07:47 2000
st_ino: Fri Aug 18 14:56:41 2000 Wed Aug 9 15:07:47 2000
/etc/inet/inetd.conf
st_size: 5702 S699
st_mtime: Wed Aug 16 15:14:26 2000 Mon Feb 21 10:11:29 2000
Morton Silver
```



# PortSentry

- 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



```
File Edit Settings Help
/etc/port Sentry/port Sentry.conf
# On-comment these if you are really anal:
#TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001,4000,4001,5742,6000,6001,6667,12345,12346,20034,27665,30301,32771,32772,32773,32774,31337,40421,40423,49724,54320"
#UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,31335,27444,34555,32770,32771,32772,32773,32774,31337,54321"
#
# Use these for just bare-bones
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337,32771,32772,32773,32774,40421,49724,54320"
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774,31337,54321"
#
#####
# 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 1024.
#
# On many Linux systems you cannot bind above port 61000. This is because
# these ports are used as part of IP masquerading. I don't recommend you
# bind over this number of ports. Realistically: I DON'T RECOMMEND YOU MONITOR
:|
```



## TCP Wrappers

- Purpose
  - Log network connections to a system
  - Allow you to filter who connects to the system
  - Trigger actions based on access attempts
  - Set banners for un-authorized access
- Needs an inetd-like program to act as the dispatcher of network services
  - FTP, Telnet, TFTP, Finger, R-Commands
- Everyone should buy Wietse Venema dinner for writing this tool. 😊



## 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
    - FTPD: badguy.domain.com, baddomain.com, baduser@badguy.domain.com
- Reverse lookup is done. Paranoid selection terminates the connection immediately if there's a mismatch.
- 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



# 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 – HP Product # B9901-90001



File Edit View Go Communicator

Members WebMail Connections BioJournal SmartUpdate Marketplace

Bookmarks & Location: http://eoccebs.snu.edu.au/~savalon/rules.html

Back Forward Reload Home Search Netscape Print Security Shop Stop

What's Related

```
# block all incoming TCP packets on 1e0 from host 'foo' to any destination.
Block in on 1e0 proto tcp from foo/32 to any

#
#
# block all outgoing TCP packets on 1e0 from any host to port 23 of host bar.
Block out on 1e0 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 10.1.2.1 to any
pass in from 10.1.3.2 to any
pass in from 10.1.3.3 to any
pass in from 10.1.3.4 to any
pass in from 10.1.3.5 to any
pass in from 10.1.0.10/32 to any
pass in from 10.1.1/32 to any
pass in from 10.1.1/32 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 10.1.2.1/32
pass out from any to 10.1.3.1/32
pass out from any to 10.1.3.2/32
pass out from any to 10.1.3.3/32
pass out from any to 10.1.3.4/32
pass out from any to 10.1.0.1/32
pass out from any to 10.1.1/32
pass out from any to 10.1.2.1/32
```

HP WORLD 2002  
Conference & Expo

# 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
```

HP WORLD 2002  
Conference & Expo

# Linux - Iptable Firewall

```
root@bigguy:~#
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 $LANSUBNET --dport sftp -j ACCEPT
# printer - (515/TCP-UDP) printer talk
$IPTABLES -A input-lan-if -p tcp -s $LANSUBNET --dport printer -j ACCEPT
#
# SYSLOG - (514/UDP) System and kernel logging to central logging host.
#
$IPTABLES -A lan-if -p udp -s $LAN_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
:~#
```

HP WORLD 2002  
Conference & Expo

# LogSentry

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

```
root@bigguy-Aus:/local/etc
File Edit Settings Help
|=
-ERR Password
ATTACK
BAD
CID etc
DEBUG
EXPN
FAILURE
ILLEGAL
LOGIN FAILURE
LOGIN REFUSED
PERMITTED
REFUSED
RETR group
RETR passed
RETR pud_db
ROOT LOGIN
SITE ENEC
VRFY
*VIZ*
admin
alias database
debug
denied
deny
deny host
exon
failed
illegal
kernel: Oversized packet received from
nested
permitted
reject
revec
rshd
logcheck.violations
```

**Logcheck violations**

**logcheck.violations**

**These keywords denote a problem and are flagged by logcheck.**

root@bigguy:/usr/local/etc

```

File Edit Settings Help
authserv.*AUTHENTICATE
cron.*CMD
cron.*RELOAD
cron.*STARTUP
ftpd-gw.*: exit host
ftpd-gw.*: permit host
ftpd.*ANONYMOUS FTP LOGIN
ftpd.*FTP LOGIN FROM
ftpd.*not-logged
ftpd.*started
http-gw.*: exit host
http-gw.*: permit host
mail.local
named.*Lawe delegation
named.*Response from
named.*transfer queries
named.*points to a CNAME
named.*reloading
named.*starting
nfsacl.*: exit host
nfsacl.*: permit host
popper.*Unshale
popper: -ERR POP server at
popper: -ERR Unknown command: "uidl".
qmail.*New msg
qmail.*Info msg
qmail.*starting delivery
qmail.*delivery
qmail.*end msg
rlogin-gw.*: exit host
rlogin-gw.*: permit host
logcheck.logname

```

**Logcheck ignores**

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

HP WORLD 2002  
Conference & Expo

root@bigguy:/usr/local/etc

```

File Edit Settings Help
*WIZ*
*WIZ*
"debug"
"DEBUG"
ATTACK
nested
MRFV bls
MRFV decode
MRFV uudecode
MRFV lp
MRFV demo
MRFV guest
MRFV root
MRFV uucp
MRFV oracle
MRFV subase
MRFV games
wrfu bls
wrfu decode
wrfu uudecode
wrfu lp
wrfu demo
wrfu guest
wrfu root
wrfu uucp
wrfu oracle
wrfu subase
wrfu games
exon decode
exon uudecode
exon wheel
exon root
EXPN decode
EXPN uudecode
EXPN wheel
logcheck.hack.log

```

**Logcheck – hacking terms**

**logcheck.hacking**

**Keywords in this file indicate an attack is taking place**

HP WORLD 2002  
Conference & Expo

# Network Traffic Sniffers

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



root@bigguy:~

File Edit Settings Help

**TCPDUMP**

```
14:47:37.676401 NAT-062.NRWDC.ORG.1622 > mail.i-plus.net.pop3: S 19684468:19684468(0) win 8192 <msg
1460,ncp,ncp,sackOK> (DF)
0x0000 4500 0c30 2d7c 4000 8006 7e05 ca01 013e      E..0-|@...?....>
0x0010 d836 6bd1 0656 006e 012f 68b4 0000 0000      .6k..V.n./i.....
0x0020 7002 2000 e231 0000 0204 06b4 0101 0402      p....i.....
14:47:37.733859 mail.i-plus.net.pop3 > NAT-062.NRWDC.ORG.1622: S 1568726878:1568726878(0) ack 196844
68 win 17520 <msg 1460,ncp,ncp,sackOK> (DF)
0x0000 4500 0c30 7541 4000 7106 4540 c836 6bd1      E..0uF@.q.E@.Ek.
0x0010 0a01 013e 006e 0656 5e80 e72e 012f 68b5      ...>.n.V]..../i.
0x0020 7012 4470 3801 0000 0204 06b4 0101 0402      p.Dp@.....
14:47:37.733999 NAT-062.NRWDC.ORG.1622 > mail.i-plus.net.pop3: . ack 1 win 8760 (DF)
0x0000 4500 0c28 2e7c 4000 8006 7d08 ca01 013e      E..(.|@...|....>
0x0010 d836 6bd1 0656 006e 012f 68b5 5e80 e72f      .6k..V.n./i.]../
0x0020 5010 2238 67fd 0000 0000 0000 0000          P..8.....
14:47:37.810084 mail.i-plus.net.pop3 > NAT-062.NRWDC.ORG.1622: P 1:56(55) ack 1 win 17520 (DF)
0x0000 4500 0c5f 7543 4000 7106 450f c836 6bd1      E.._u@.q.E..Ek.
0x0010 0a01 013e 006e 0656 5e80 e72f 012f 68b5      ...>.n.V].../i.
0x0020 5018 4470 ab5f 0000 2b4f 4e20 5831 204e      P.Dp...>@K.X1.N
0x0030 942d 9c4f 5033 20c3 6572 7e60 7220 682d      T-P@P3,Server,i-
0x0040 706c 7573 2e6e 6574 2028 494d 6168 6c20      plus.net.(IMail.
0x0050 362e 3c36 2034 3239 3538 2d36 280d 0a      6.06.42968-6)...
14:47:37.811447 NAT-062.NRWDC.ORG.1622 > mail.i-plus.net.pop3: P 1:16(15) ack 56 win 8705 (DF)
0x0000 4500 0c37 2f7c 4000 8006 7e0e ca01 013e      E..7/|@...|....>
0x0010 d836 6bd1 0656 006e 012f 68b5 5e80 e766      .6k..V.n./i.]...f
0x0020 5018 2201 057e 0000 5553 4552 206e 6d63      P..'....USER..jnc
0x0030 686e 7478 720d 0a      intgr...
14:47:38.012796 mail.i-plus.net.pop3 > NAT-062.NRWDC.ORG.1622: . ack 16 win 17505 (DF)
0x0000 4500 0c28 7559 4000 7106 4530 c836 6bd1      E..(uY@.q.E@.Ek.
0x0010 0a01 013e 006e 0656 5e80 e766 012f 68c4      ...>.n.V]...f./i.
0x0020 5010 4461 858e 0000 1401 0000 ca00      P.Dae.....
```

HP WORLD 2002  
Conference & Expo

### Ethereal

No.	Time	Source	Destination	Protocol	Info
1	0.00000	10.2.2.2	63.171.251.2	DNS	Standard query A www.sans.org
2	0.00884	63.171.251.2	10.2.2.2	DNS	Standard query response A 63.100.47.48
3	0.01883	10.2.2.2	63.171.251.2	DNS	Standard query A www.paknet.net
4	0.02613	63.171.251.2	10.2.2.2	DNS	Standard query response, No such name
5	0.02647	10.2.2.2	63.171.251.2	DNS	Standard query A www
6	0.07112	63.171.251.2	10.2.2.2	DNS	Standard query response, No such name
7	0.10516	10.2.2.2	63.100.47.46	TCP	37521 > 80 [SYN] Seq=2195408848 Ack=0 Win=0 Len=0
8	0.16414	63.100.47.46	10.2.2.2	TCP	80 > 37521 [SYN, ACK] Seq=2182925377 Ack=37521 Win=0 Len=0
9	117610.732099	10.2.2.2	63.100.47.46	TCP	37521 > 80 [ACK] Seq=2195408848 Ack=2182925377 Win=0 Len=0
10	0.16476	10.2.2.2	63.100.47.46	HTTP	GET / HTTP/1.0
11	0.20039	63.100.47.46	10.2.2.2	TCP	80 > 37521 [ACK] Seq=2182925378 Ack=2195408848 Win=0 Len=0
12	0.20127	63.100.47.46	10.2.2.2	TCP	80 > 37521 [FIN, ACK] Seq=2182925378 Ack=2195408848 Win=0 Len=0
13	117610.769116	10.2.2.2	63.100.47.46	TCP	37521 > 80 [ACK] Seq=2195409129 Ack=2182925378 Win=0 Len=0
14	0.21026	63.100.47.46	10.2.2.2	HTTP	HTTP/1.1 301 Moved Permanently
15	117610.778314	10.2.2.2	63.100.47.46	TCP	37521 > 80 [ACK] Seq=2195409129 Ack=2182925378 Win=0 Len=0

Frame 1 (72 on wire, 72 captured)  
 Ethernet II  
 Internet Protocol, Src Addr: 10.2.2.2 (10.2.2.2), Dest Addr: 63.171.251.2 (63.171.251.2)  
 User Datagram Protocol, Src Port: 32699 (32699), Dest Port: domain (53)  
 Source port: 32699 (32699)  
 Destination port: domain (53)  
 Length: 38

```

0000 0d 48 54 5f 6d 52 0d 48 54 63 12 f8 08 0d 45 0d  .Htoah.H Tc...E.
0010 0d 3a bd 07 40 0d 40 11 36 f6 0a 02 02 02 3f ab  ...9.B.6....7.
0020 fb 02 80 83 0d 36 0d 26 34 c5 e8 29 01 00 00 01  ....5.4.4....
0030 00 00 00 00 00 00 03 77 77 77 04 73 61 6e 73 03  ....WWW.sans:
0040 6f 72 67 00 00 01 00 01                               org....
  
```

HP WORLD 2002  
Conference & Expo

### Analyzer

Num	Capture Time	Dest. MAC	Src. MAC	Len
1	08h:48m:34s:715500us	0000AD-070EAB	000000-00-1080	10
2	08h:48m:34s:723162us	000000-00-1080	0000AD-070EAB	10
3	08h:48m:34s:730705us	0000AD-070EAB	000000-00-1080	10
4	08h:48m:34s:738359us	000000-00-1080	000000-00-1080	10
5	08h:48m:34s:746013us	000000-00-1080	0000AD-070EAB	10
6	08h:48m:34s:753667us	000000-00-1080	0000AD-070EAB	10
7	08h:48m:34s:820705us	0000AD-070EAB	000000-00-1080	10
8	08h:48m:34s:820707us	000000-00-1080	000000-00-1080	10
9	08h:48m:34s:830104us	000000-00-1080	0000AD-070EAB	10
10	08h:48m:34s:845415us	0000AD-070EAB	000000-00-1080	10

General  
 Name: DHCP Discover  
 Time Information: 08h:48m:34s:738359us  
 Description: DHCP Discover  
 MAC Header: 000000-00-1080 (10.1.1.125) to 0000AD-070EAB (192.178.10.180)  
 IP Header: Version=4, Header length=20, Type of service=0, Total length=372 bytes, Identification=2498, Flags=0, Fragment offset=0, Time to live=128 seconds/ hops, Protocol=6 (TCP), Header checksum=130F8, Source address=10.1.1.125, Destination address=192.178.10.180

```

00 00 C0 0B 1 2D 00 00 00 1 AB 87 8E 85 1 68 00 05 00
[.....]
01 78 03 81 1 50 00 00 00 1 23 00 00 05 1 83 70 C4 02
[.....]
00 34 06 34 1 00 50 00 5E 1 B3 28 35 83 1 34 F2 50 18
[.....]
* 22 20 06 61 1 00 00 47 45 1 54 20 2F 32 1 68 69 6E 72
[* a..GET /www.sans.org]
* 2F 61 74 74 1 62 62 2E 69 1 69 67 2F 66 1 6E 6E 74 65
[/http://www.sans.org]
* 72 5E 72 69 1 67 69 74 63 1 6E 72 6E 65 1 72 2B 47 69
[...sightcorner.org]
* 6C 20 44 74 1 54 99 2E 31 1 2E 31 00 0A 1 31 63 63 69
[...HTTP/1.1...]
* 70 74 3A 20 1 2A 2B 2A 00 1 0A 52 65 66 1 65 72 65 72
[...Referer:]
* 2A 20 62 74 1 74 70 2A 2F 1 2F 68 65 6C 1 70 20 62 72
[...http://www.sans.org]
* 6E 61 64 62 1 61 68 64 2E 1 61 74 74 2E 1 63 6E 60 2E
[...hand.att.com/]
* 6C 6E 65 65 1 2B 2E 6A 74 1 2B 2F 6F 1 65 69 6A 6B
  
```

HP WORLD 2002  
Conference & Expo

# Intrusion Detection Systems - IDS

- Snort
- Shadow
- HP IDS/9000



Webpage: SnortSnarf: Snort signatures in /var/log/snort/alert et al

File Edit View Go Communicator Help

**SILICON DEFENSE** SnortSnarf start page  
All Snort signatures  
SnortSnarf v020316.1

[Signature section C3581](#) [Top 20 source IPs](#) [Top 20 dest IPs](#)

358 alerts found using input module SnortFileInput, with sources:  
• /var/log/snort/alert

Earliest alert at 14:25:40.981126 on 07/19/2002  
Latest alert at 14:02:06.418891 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-MISC /doc/ access [sig]	1	1	1	<a href="#">Summary</a>
2	NETBIOS SMB IPCAccess [sig]	2	2	1	<a href="#">Summary</a>
2	NETBIOS NT NULL session [sig]	2	1	1	<a href="#">Summary</a>
2	MEB-IDS scripts access [sig]	2	1	1	<a href="#">Summary</a>
2	MEB-MISC search.dll access [sig]	6	1	2	<a href="#">Summary</a>
2	SNMP public access udp [sig]	10	1	1	<a href="#">Summary</a>
2	ICMP PING WMP [sig]	330	3	2	<a href="#">Summary</a>
1	SMTP RCPT TO overflow [sig]	1	1	1	<a href="#">Summary</a>
1	FTP USER overflow attempt [sig]	4	1	1	<a href="#">Summary</a>

100%



Message: 001 alerts going to 63.171.251.15 in /var/log/snort/alert

File Edit View Go Communicate Help

**SILICON DEFENSE** SnortSnarf alert page  
 Destination: 63.171.251.15  
 SnortSnarf v000516.1

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

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

- /var/log/snort/alert

Earliest: 14:49:07.09045 on 07/19/2002  
 Latest: 14:49:07.09045 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:	HEIN	RIPE	NETIC	Geektools
63.171.251.15	Whois lookup at:	omninet	IRIDM	Business	
	Raw lookup link:	Whois	Sam.Snoops		

```
07/19-14:49:07.09045 [**] [1:554:5] SMTP_RCPT_TO_overflow [**]
[Classification: Attempted Administrator Privilege Gain] [Priority:
1] (TCP) 10.1.1.41-2380 -> 63.171.251.15:25
```

SnortSnarf brought to you courtesy of Silicon\_Defense  
 Authors: Jim Hoasland and Stuart Staniford  
 See also the [Snort Page](#) by Marty Roesch  
 Page generated at Fri Jul 19 14:53:00 2002

HP WORLD 2002  
 Conference & Expo

Message: List of top 10 destination IPs in /var/log/snort/alert

File Edit View Go Communicate Help

**SILICON DEFENSE** SnortSnarf summary page  
 Top 10 destination IPs  
 SnortSnarf v000516.1

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

This page provides summary information about alerts acquired using input module SnortFileInput, with sources:

- /var/log/snort/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	329 alerts	207.26.131.177	1 signatures	10.1.1.79
rank #2	10 alerts	10.1.1.2	1 signatures	10.1.1.2
rank #3	6 alerts	216.25.157.20	1 signatures	10.1.1.45
rank #4	4 alerts	10.1.1.2	2 signatures	13 source IPs
		193.60.22.13	1 signatures	63.171.251.227
rank #5	2 alerts	216.25.22.210	1 signatures	10.1.1.106, 10.1.1.108
		216.25.221.57	1 signatures	10.1.1.79
		63.171.251.15	1 signatures	10.1.1.45
rank #6	1 alerts	66.139.134.131	1 signatures	10.1.1.45
		193.246.0.20	1 signatures	63.171.251.227

SnortSnarf brought to you courtesy of Silicon\_Defense  
 Authors: Jim Hoasland and Stuart Staniford  
 See also the [Snort Page](#) by Marty Roesch  
 Page generated at Fri Jul 19 14:53:00 2002

HP WORLD 2002  
 Conference & Expo

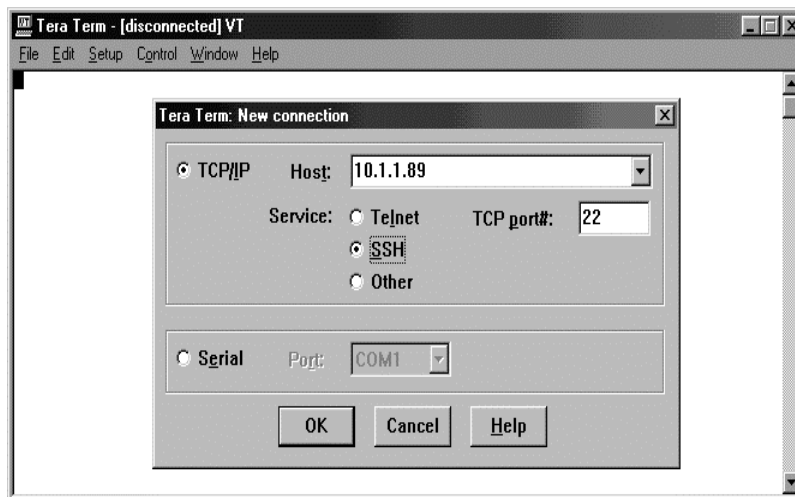


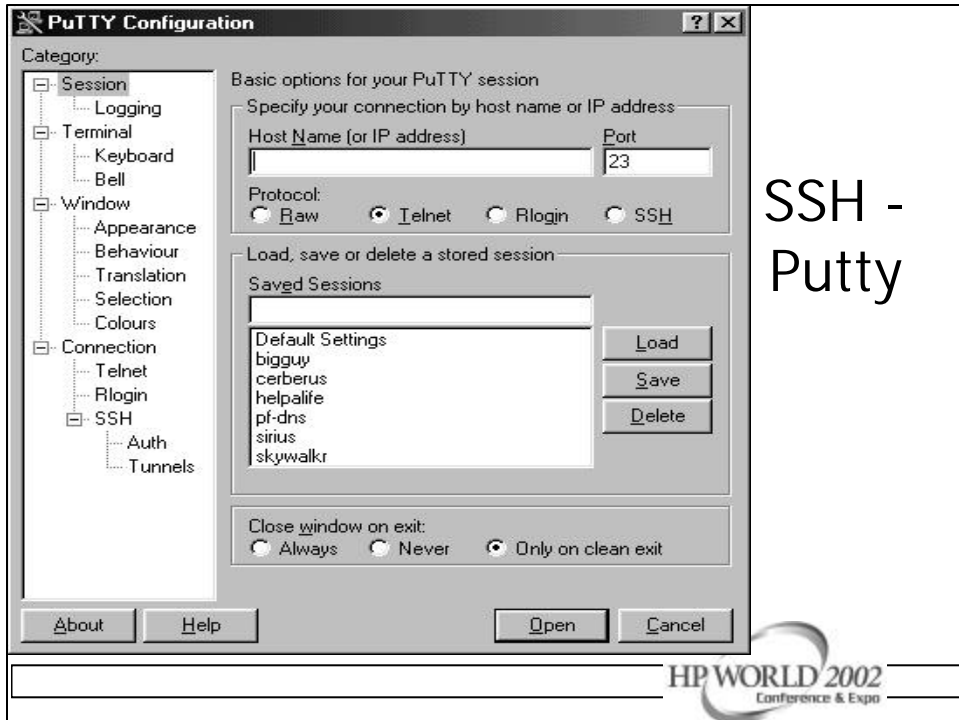
# SSH Connectivity Tool

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



# SSH - TeraTerm





## SSH - Putty

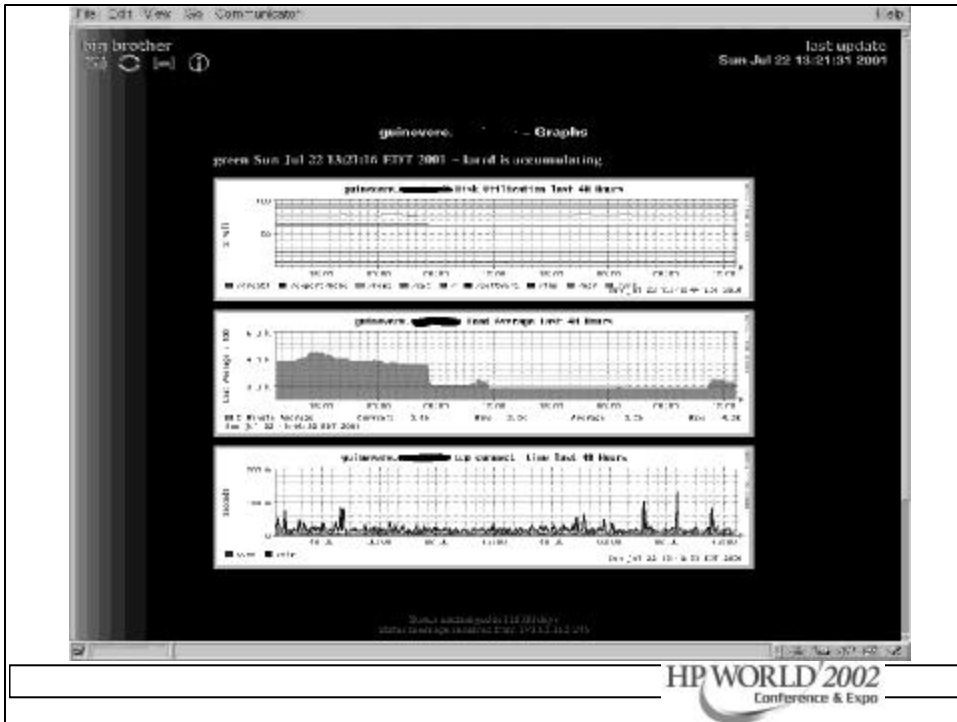
## Big Brother

- 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

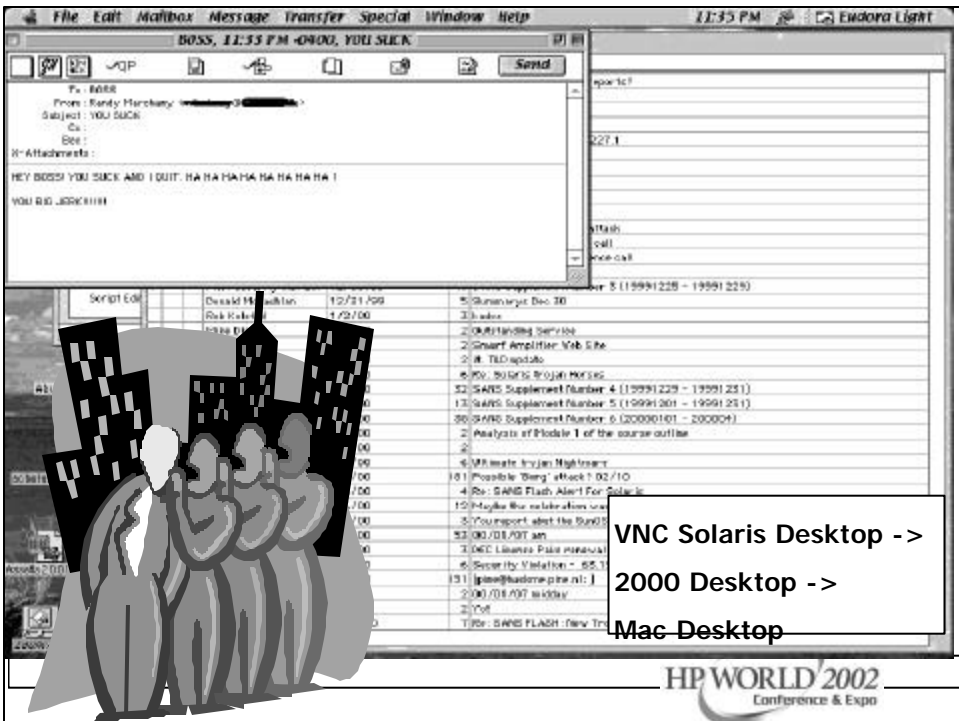
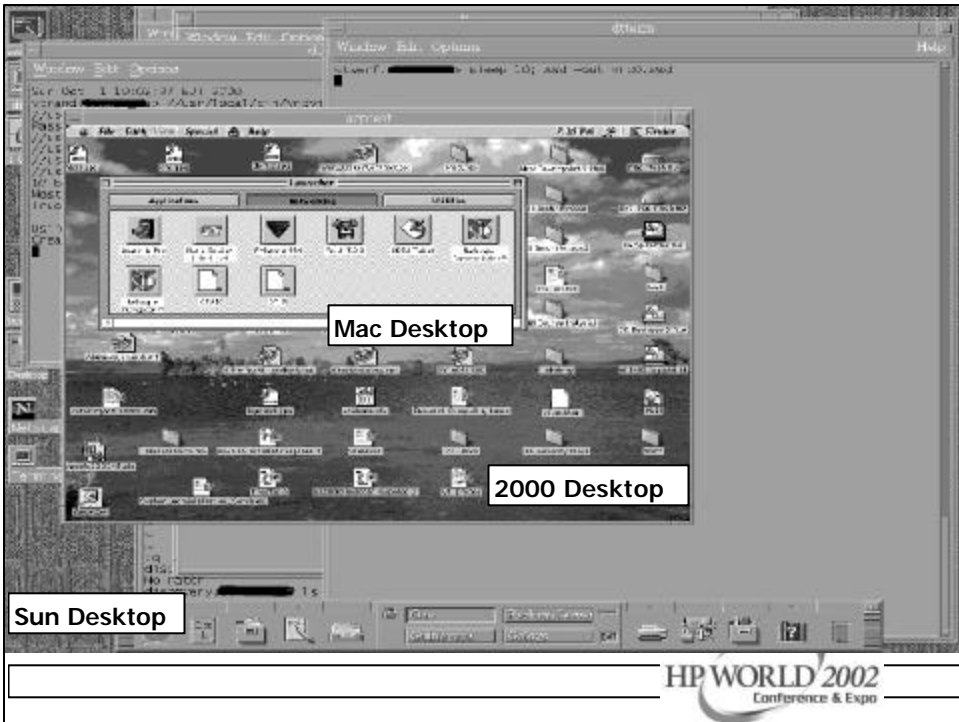
- Color coded WWW page showing a matrix of machines and monitored functions
- Notifies sysadmins by email, pager, SMS.
- System requirements
  - Unix – www server, /bin/sh, C compiler to port BB
  - NT – v4.0 with SP3 minimum, Intel or Alpha platforms.





## 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, process explorer

- 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
root@biggy:~/usr/local/src/logcheck-1.1.1
lsof -p 4009
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
sshd 4009 root cwd DIR 3,5 1024 2 /
sshd 4009 root rtd DIR 3,5 1024 2 /
sshd 4009 root txt REG 3,9 206152 132788 /usr/sbin/sshd
sshd 4009 root ses REG 3,8 494250 61310 /lib/ld-2.2.4.so
sshd 4009 root ses REG 3,8 12020 8187 /lib/security/pam_stack.so
sshd 4009 root ses REG 3,8 6487 8180 /lib/security/pam_nologin.so
sshd 4009 root ses REG 3,8 14717 8174 /lib/security/pam_limits.so
sshd 4009 root ses REG 3,8 4984 8206 /lib/security/pam_deny.so
sshd 4009 root ses REG 3,8 35424 61202 /lib/libc.so.0.75
sshd 4009 root ses REG 3,8 65907 61214 /lib/libdl-2.2.4.so
sshd 4009 root ses REG 3,8 263407 61248 /lib/libresolv-2.2.4.so
sshd 4009 root ses REG 3,8 47522 61294 /lib/libutil-2.2.4.so
sshd 4009 root ses REG 3,9 59775 64677 /usr/lib/libz.so.1.1.3
sshd 4009 root ses REG 3,8 436384 61219 /lib/libnsl-2.2.4.so
sshd 4009 root ses REG 3,8 818752 61276 /lib/libcrypt.so.0.9.6b
sshd 4009 root ses REG 3,9 425483 96830 /usr/kerberos/lib/libkrb5.so.3.0
sshd 4009 root ses REG 3,9 78183 96825 /usr/kerberos/lib/libk5crypto.so.3.0
sshd 4009 root ses REG 3,8 8713 96820 /usr/kerberos/lib/libcom_err.so.3.0
sshd 4009 root ses REG 3,8 5779542 73448 /lib/libnss/libc-2.2.4.so
sshd 4009 root ses REG 3,8 262272 61235 /lib/libnss_files-2.2.4.so
sshd 4009 root ses DWR 1,5 11150 /dev/zoro
sshd 4009 root ses REG 3,8 50891 8165 /lib/security/pam_console.so
sshd 4009 root ses REG 3,8 13025 8207 /lib/security/pam_env.so
sshd 4009 root ses REG 3,8 14636 8205 /lib/security/pam_cracklib.so
sshd 4009 root ses REG 3,9 182363 64462 /usr/lib/libglib-1.2.so.0.0.10
sshd 4009 root ses REG 3,8 325236 61243 /lib/libnss_rndspplus-2.2.4.so
sshd 4009 root ses REG 3,8 71988 61232 /lib/libnss_dns-2.2.4.so
sshd 4009 root ses REG 3,8 48678 8191 /lib/security/pam_unix.so
sshd 4009 root ses REG 3,8 35115 61212 /lib/libcrypt-2.2.4.so
sshd 4009 root ses REG 3,9 69064 64452 /usr/lib/libcrack.so.2.7
sshd 4009 root ses DWR 1,5 11150 /dev/zoro
sshd 4009 root cu D-R 1,3 5203 /dev/null
sshd 4009 root lu D-R 1,3 5203 /dev/null
sshd 4009 root zu D-R 1,3 5203 /dev/null
sshd 4009 root 4u IPv4 1258537 TCP biggy:ssh->HNT-062.NRVC.ORG:1028 (ESTABLISHED)
sshd 4009 root 5u unix (/var/sock) 1258560 socket
root@biggy:~/usr/local/src/logcheck-1.1.1
```





## 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



## 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 !!!





Center for Internet Security - Microsoft Internet Explorer

# THE CENTER FOR INTERNET SECURITY

HOME  
WHAT IS CIS?  
STANDARDS  
FAQ - CIS  
MEMBERSHIP  
CONTACT US

Join Us  
\* Register of Members  
\* Membership Information  
CIS Benchmarks & Security Tools  
\* NEW! Windows XP 2002  
\* Windows 2000  
\* Windows XP  
\* Windows NT  
\* Linux  
\* Solaris

**CIS Security Benchmarks and Scoring Tools for:**  
New Available - FREE of Charge  
(Click on the Name to Download)

JUST ADDED (July 17, 2002)  
- Windows 2000 - Workstation Benchmark - Consensus Baseline  
- Solaris - Level 1  
- Linux - Level 1  
- HP-UX - Level 1  
- Cisco IOS Router - Levels 1 & 2  
- Windows 2000 - Level 1  
- Windows NT - Level 1

- NEW: CIS Provides Recognition for Developers of the Consensus Benchmarks and Scoring Tools

What's New on This Site? Click Here

CIS FEATURES:

- Free 1-hour Webinars - "Pass or Fail? How Does Your Security Measure Up?"
- Case Study - ISP Secures Its Servers to CIS Benchmark Standards

CIS featured in USA TODAY Click Here

CIS Certifies Commercial Software Click Here for information

CIS Designates Information Security Pacesetters Click Here for information

Become a Member of the Center for Internet Security Click Here for More Information

The Center for Internet Security (CIS) is a not-for-profit cooperative enterprise that helps organizations reduce the risk of business and e-commerce disruptions resulting from inadequate security configurations.

CIS members are developing and propagating the widespread application of Security Benchmarks

HP WORLD 2002  
Conference & Expo

root@biggy:/var/local/in05net5/nan-020116.1

## CIS Ruler Report

```

*** CIS Ruler Run ***
Starting at time 20000415-10:44:06

Positive: 1.1 System appears to have been patched within the last month.
Positive: 2.2 Authorized usage banners are configured well in /etc/issue.
Positive: 2.3 telnet is deactivated.
Positive: 2.4 ftp is deactivated.
Positive: 2.5 rsh, rcp and rlogin are deactivated.
Positive: 2.6 rftn is deactivated.
Negative: 2.7 xinetd either requires global 'only-from' statement or one for each service.
Positive: 3.1 Miscellaneous scripts are all turned off.
Positive: 3.2 NFS Server script nfs is deactivated.
Positive: 3.3 This machine isn't being used as an NFS client.
Positive: 3.4 NIS Client processes are deactivated.
Positive: 3.5 NIS Server processes are deactivated.
Positive: 3.6 portmap has been deactivated.
Positive: 3.7 samba windows filesharing daemons are deactivated.
Positive: 3.8 net/rpc script is deactivated.
Negative: 3.9 cups (printing daemon) not deactivated.
Positive: 3.10 Graphical login is deactivated.
Positive: 3.11 Mail daemon is not listening on TCP 25.
Positive: 3.12 Web server is deactivated.
Positive: 3.13 snmp daemon is deactivated.
Positive: 3.14 DNS server is deactivated.
Positive: 3.15 postgresql (SQL) database server is deactivated.
Positive: 3.16 routing daemons are deactivated.
Positive: 3.17 Webmin GUI-based system administration daemon deactivated.
Positive: 3.18 Squid web cache daemon deactivated.
Positive: 3.19 /etc/xinetd not activated.
Positive: 3.20 Found a good daemon weak.
Positive: 4.1 Bonded up are deactivated.
Positive: 4.2 /etc/exports is empty or doesn't exist, so it doesn't need to be tuned for privacy.
Negative: 4.3 IP forwarding is activated.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth1/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth0/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/lo/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/default/send_redirects should be 0 to disable outgoing redirect messages.
Positive: 5.1 syslog captures auth and authpriv messages.
Positive: 6.1 /etc/fstab mounts all removable file systems noauto.
:~

```

HP WORLD 2002  
Conference & Expo

## 2.7 Set TCP Wrappers/xinetd Access Control

### Action (if you have an `/etc/inetd.conf` file):

1. Create a simple `/etc/hosts.allow` file containing a single line of the form:  
ALL: <net>/<mask>, <net>/<mask>, .. : banners /etc/banners  
where each <net>/<mask> combination (for example,  
"192.168.1.0/255.255.255.0") represents one network block in use by your organization.

2. Create `/etc/hosts.deny`:

```
echo 'ALL: ALL: /bin/mail \\  
-s "%s: connection attempt from %s" \  
root@localdomain.com' >/etc/hosts.deny
```

Replace the address `root@localdomain.com` with an appropriate email address for your site.

### Action (if you have an `/etc/xinetd.conf` file):

Insert the following line into the "default" block in `/etc/xinetd.conf`,  
`only_from=<net>/<mask_bits> <net>/<mask_bits> -`  
where each <net>/<mask\_bits> combination (for example,  
"192.168.1.0/24") represents one network block in use by your organization.

### Discussion:

Linux distributions do access control services in two different ways. On older or more conservative systems where `inetd` is used, TCP Wrappers provide access control via `/etc/hosts.allow` and `/etc/hosts.deny`. TCP Wrappers also provides logging information via Syslog about both successful and unsuccessful connections.

Newer systems generally use `xinetd`, which allows for access control natively, without requiring any wrapping programs.

Though the `xinetd` program usually doesn't take advantage of TCP Wrappers,

# Summary

- Port Scanning
- Audit Tools
- Firewalls
- Log Scanners
- Sniffers
- IDS's
- Encryption Tools
- Password Crackers
- System Security Analyzers

## 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 ?



## Many Thanks to:

Randy Marchany – Director Security Testing  
Lab, Virginia Tech



## Where to Get the Tools

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



## Where to Get the Tools

- [www.psonic.com](http://www.psonic.com)
  - LogSentry, portsentry
- [www.uk.research.att.com/vnc](http://www.uk.research.att.com/vnc)
  - VNCViewer
- [www.insecure.org](http://www.insecure.org)
  - Nmap
- [www.openssh.org](http://www.openssh.org) or [hpux.cs.utah.edu/](http://hpux.cs.utah.edu/)
  - SSH



## Where to Get the Tools

- [www.nessus.org](http://www.nessus.org)
  - Nessus
- [www.packetstormsecurity.org](http://www.packetstormsecurity.org)
  - Hacker tools
- [bb4.com](http://bb4.com)
  - Big Brother
- [www.ethereal.com](http://www.ethereal.com)
  - Ethereal
- [analyzer.polito.it](http://analyzer.polito.it)
  - analyzer



## Where to Get the Tools

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

