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

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

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

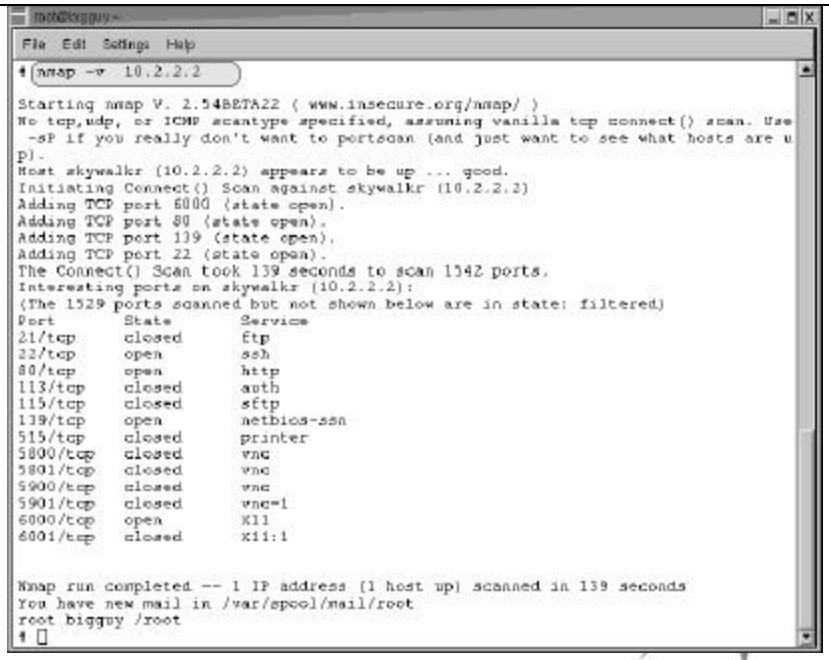
- **Sysadmin Tools**
  - Big Brother
  - Password Checkers -
    - Crack, l0phtcrack, John the Ripper
  - Lsof, process-explorer/inzider/fport (NT)
  - Sudo (unix/NT)
- **Remote Control Tools**
  - VNCviewer
- **System Security Analyzers**
  - CIS Benchmarks
  - HP-UX Bastille
  - HP-UX Security Patch 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 &
  - hpux.cs.utah.edu/
- Nessus, Saint, Sara, Satan



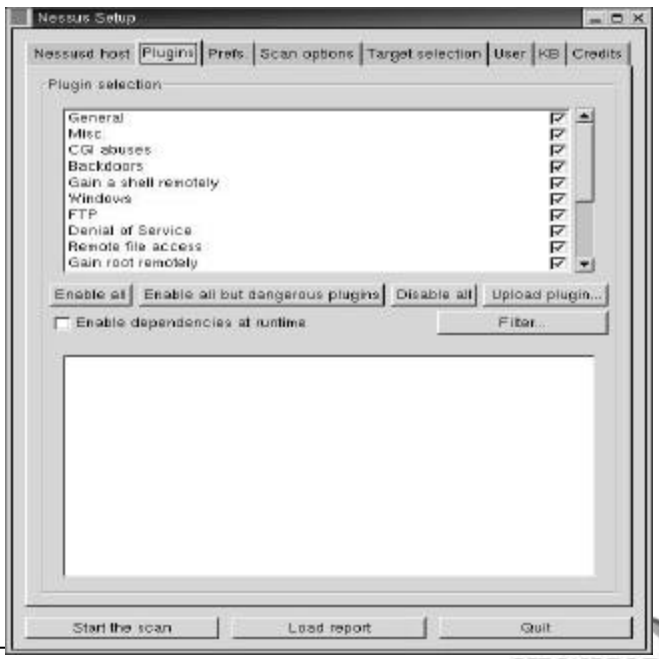
Nessus

- 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)

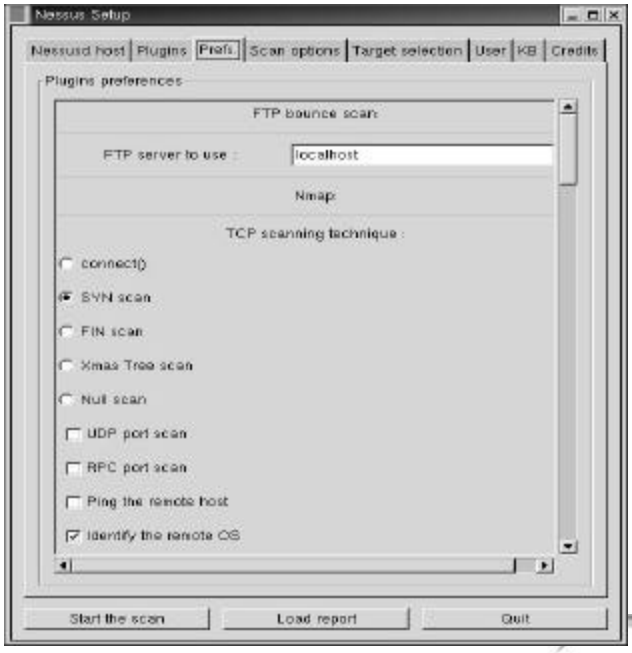
HP WORLD 2002 Conference & Expo

Nessus – Pros/Cons

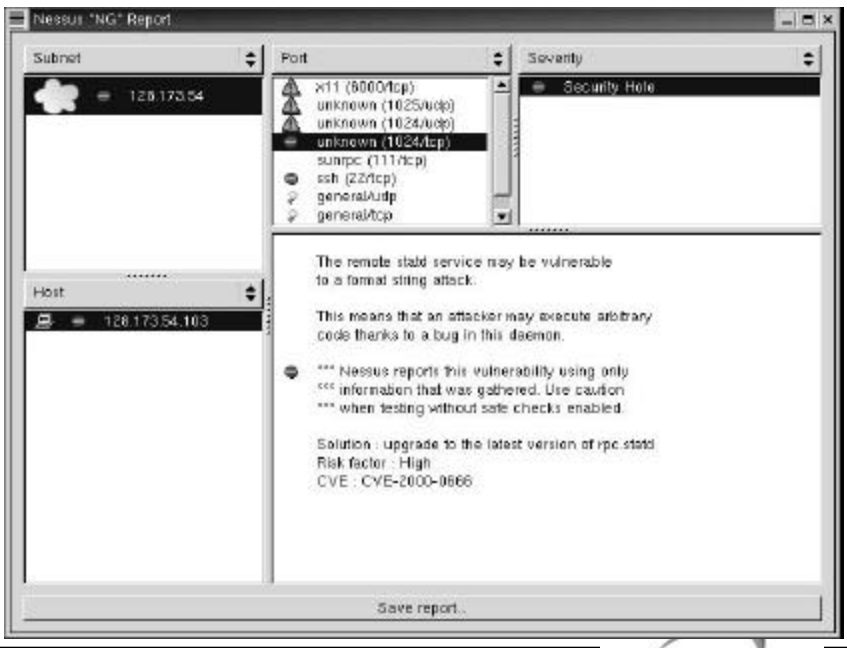
- Pros
  - Easy to install if you have linux
  - Most comprehensive tests for your money
- Cons
  - Not that easy to understand at first
  - Non-linux builds require GNU software
  - Some inconsistency in quality of checks
  - Must use Unix server for specific user accounts



HP WORLD 2002 Conference & Expo



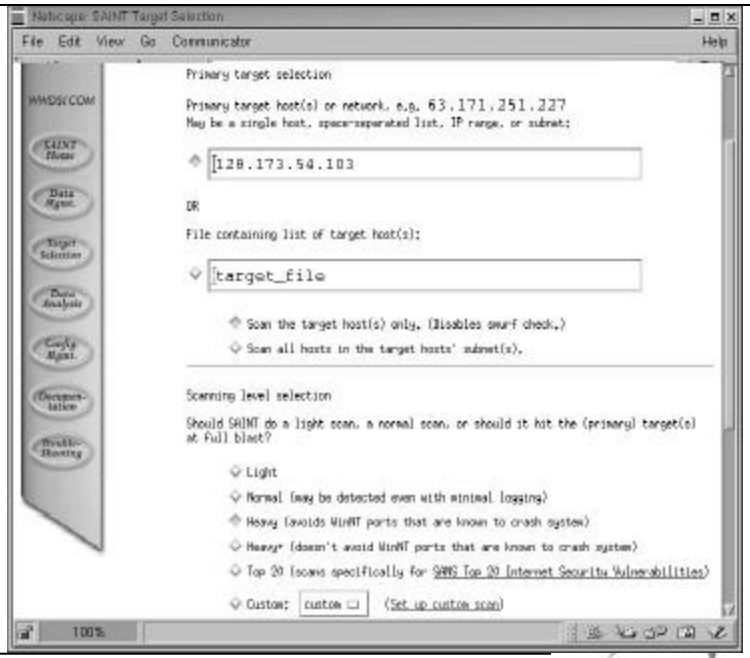
HP WORLD 2002 Conference & Expo



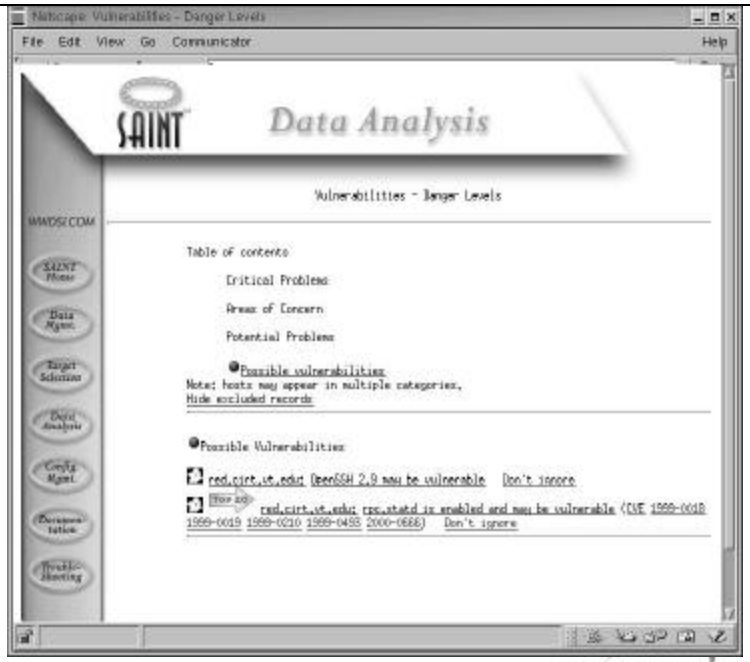
HP WORLD 2002 Conference & Expo

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

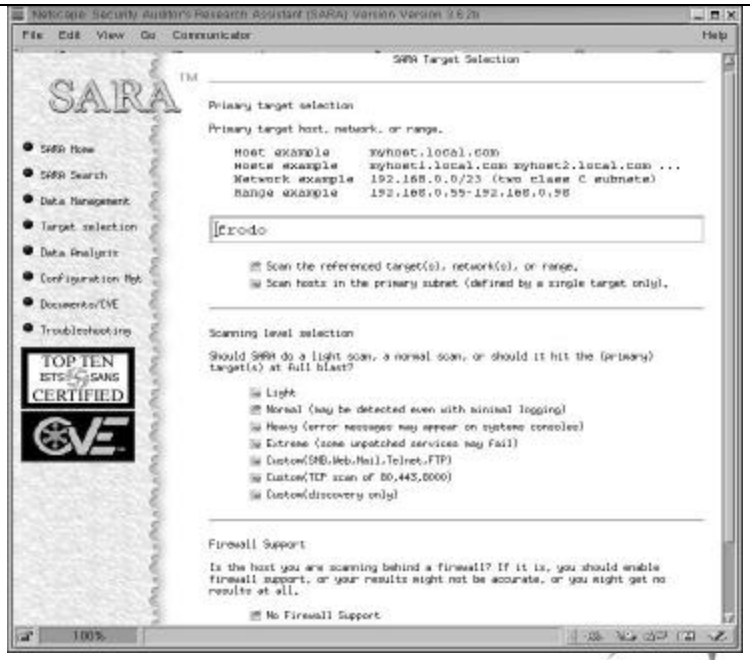


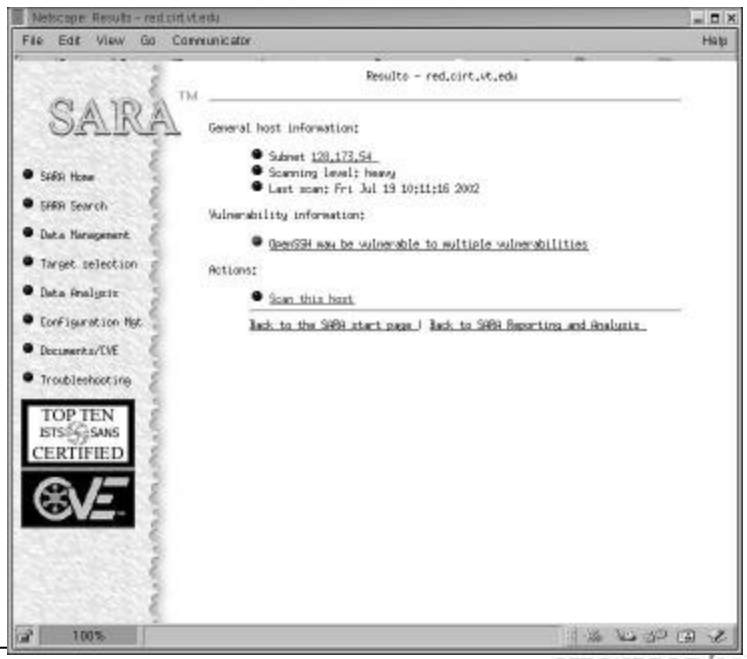
HP WORLD 2002 Conference & Expo

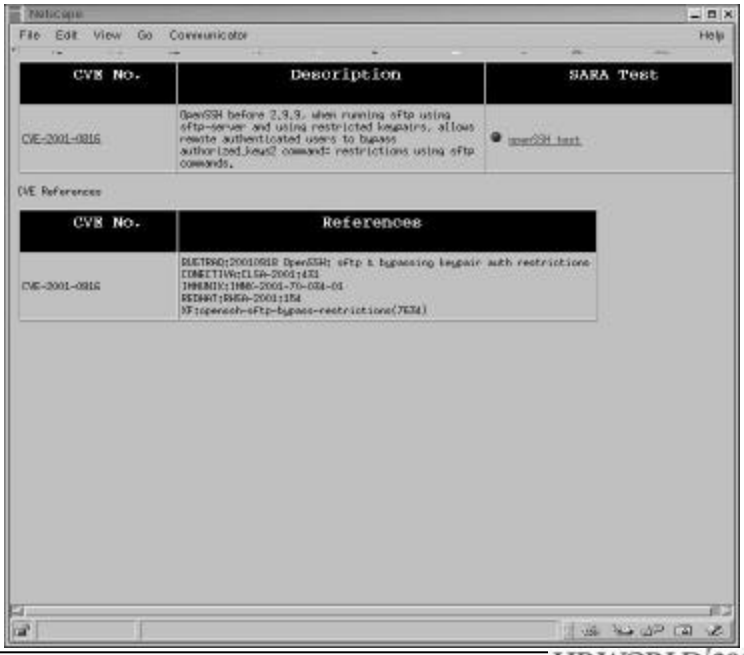
SARA

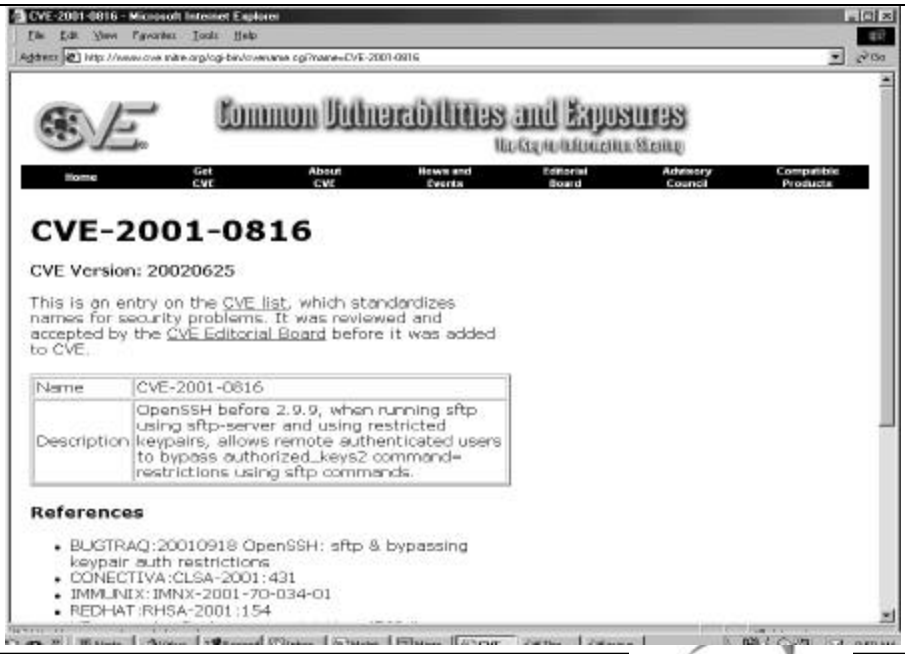
- Security Auditor's Research Assistant
- Checks for SANS Top 20 Threats
- Does Unix/Windows vulnerability tests
- Has CVE dictionary support
  - Common Vulnerabilities & Exposure
- Search engine for post audit analysis
- Uses CIS Benchmarks
- Has a Report Writer

HP WORLD 2002 Conference & Expo


File Edit View Go Communicator Help
SARA
SARA Target Selection
Primary target selection
Primary target host, network, or range.
Host example myhost.local.com
Hosts example myhost1.local.com myhost2.local.com ...
Network example 192.168.0.0/23 (two class C subnets)
Range example 192.168.0.55-192.168.0.98
frodo
Scan the referenced target(s), network(s), or range.
Scan hosts in the primary subnet (defined by a single target only).
Scanning level selection
Should SARA do a light scan, a normal scan, or should it hit the (primary) target(s) at full blast?
Light
Normal (may be detected even with minimal logging)
Heavy (error messages may appear on systems consoles)
Extreme (some unpatched services may fail)
Custom(SMB,Web,Mail,Telnet,FTP)
Custom(TCP scan of 80,443,8000)
Custom(discovery only)
Firewall Support
Is the host you are scanning behind a firewall? If it is, you should enable firewall support, or your results might not be accurate, or you might get no results at all.
No Firewall Support
SARA Home
SARA Search
Data Management
Target selection
Data Analysis
Configuration Mgt
Documents/CVE
Troubleshooting
TOP TEN
ISTS SANS
CERTIFIED
CVE
100%


File Edit View Go Communicator Help
SARA
Results - red.cirt.vt.edu
General host information:
Subnet 128.173.54
Scanning level: heavy
Last scan: Fri Jul 19 10:11:16 2002
Vulnerability information:
OpenSSH may be vulnerable to multiple vulnerabilities
Actions:
Scan this host
Back to the SARA start page | Back to SARA Reporting and Analysis
SARA Home
SARA Search
Data Management
Target selection
Data Analysis
Configuration Mgt
Documents/CVE
Troubleshooting
TOP TEN
ISTS SANS
CERTIFIED
CVE
100%


File Edit View Go Communicator Help
CVE No.
Description
SARA Test
CVE-2001-0816
OpenSSH before 2.9.9, when running sftp using sftp-server and using restricted keypairs, allows remote authenticated users to bypass authorized_keys2 command= restrictions using sftp commands.
openSSH test
CVE References
CVE No.
References
CVE-2001-0816
BUGTRAQ:20010918 OpenSSH: sftp & bypassing keypair auth restrictions
CONECTIVA:CLSA-2001:431
IMMUNIX:IMNX-2001-70-034-01
REDHAT:RHSA-2001:154
XF:openssh-sftp-bypass-restrictions(7634)


CVE-2001-0816 - Microsoft Internet Explorer
Common Vulnerabilities and Exposures
Home
Get CVE
About CVE
News and Events
Editorial Board
Advisory Council
Compatible Products
CVE-2001-0816
CVE Version: 20020625
This is an entry on the CVE list, which standardizes names for security problems. It was reviewed and accepted by the CVE Editorial Board before it was added to CVE.
Name
CVE-2001-0816
Description
OpenSSH before 2.9.9, when running sftp using sftp-server and using restricted keypairs, allows remote authenticated users to bypass authorized_keys2 command= restrictions using sftp commands.
References
BUGTRAQ:20010918 OpenSSH: sftp & bypassing keypair auth restrictions
CONECTIVA:CLSA-2001:431
IMMUNIX:IMNX-2001-70-034-01
REDHAT:RHSA-2001:154

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.

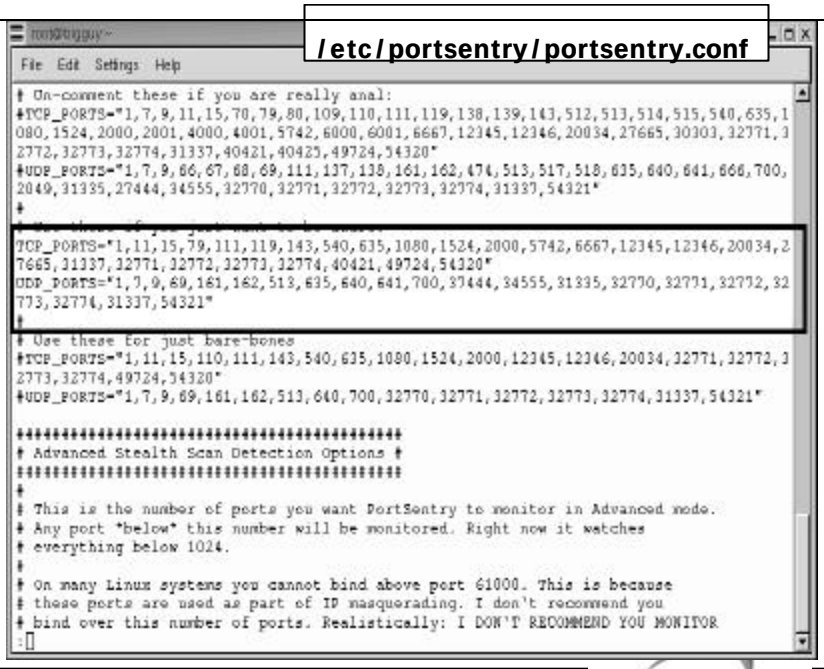
Tripwire

- 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 $$$

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

/etc/portsentry/portsentry.conf



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

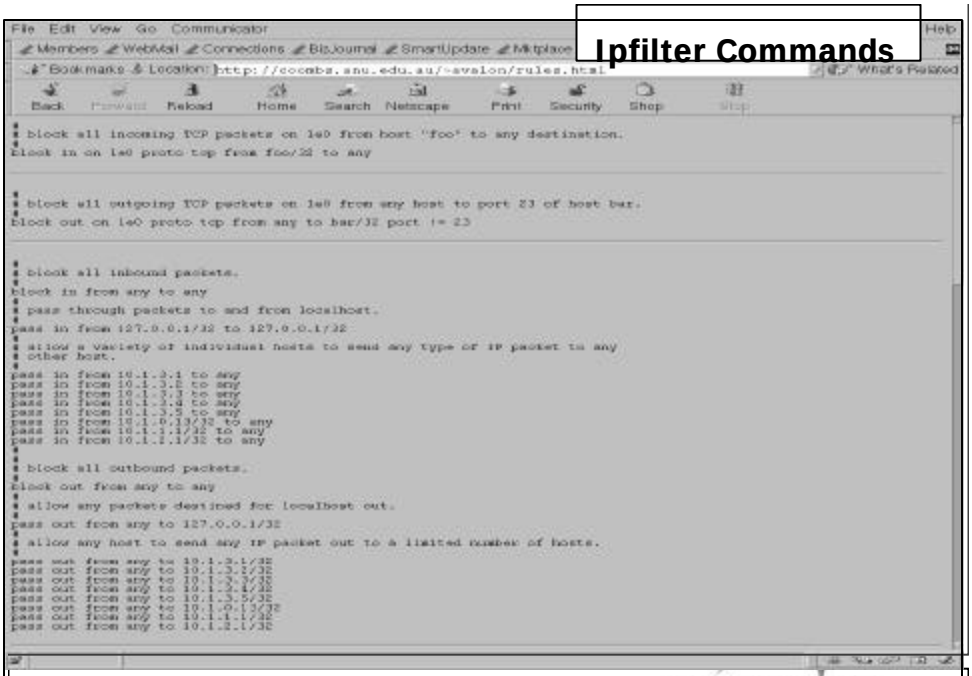
Personal Firewall Tools

- 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

Ipfilter Commands



Ipfilter 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
```


Linux - Iptable Firewall

root@bigguy:~

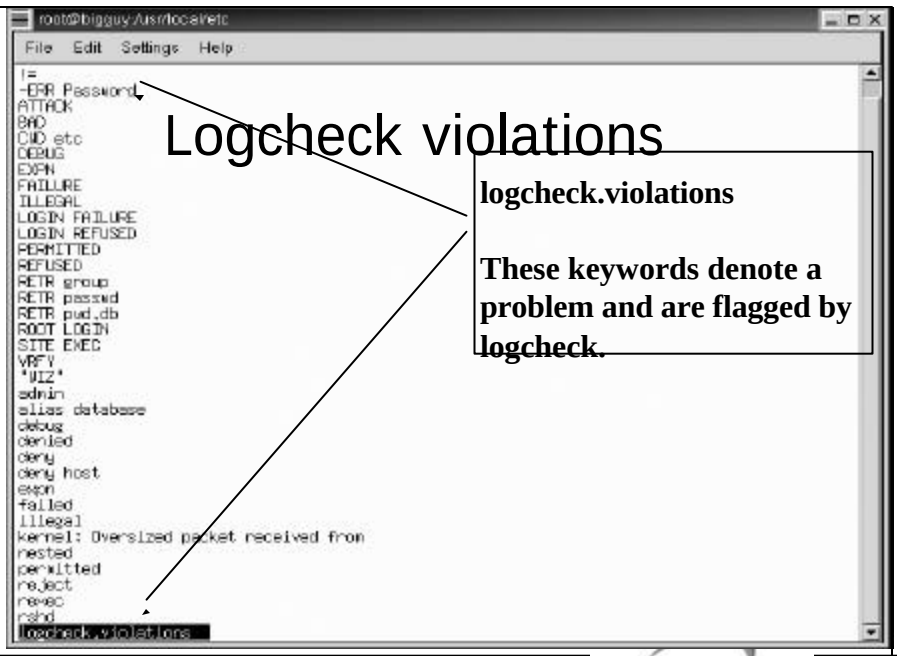
File Edit Settings Help

```
################################################################################
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 PCKT: "
        $IPTABLES -A input-lan-if -j DROP

:
```

LogSentry

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

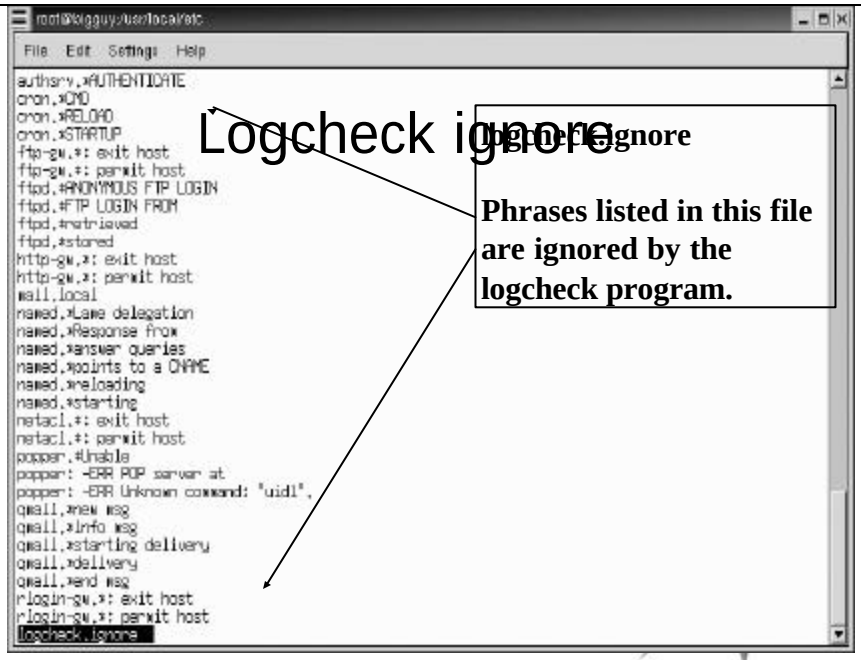
Logcheck violations



logcheck.violations

These keywords denote a problem and are flagged by logcheck.

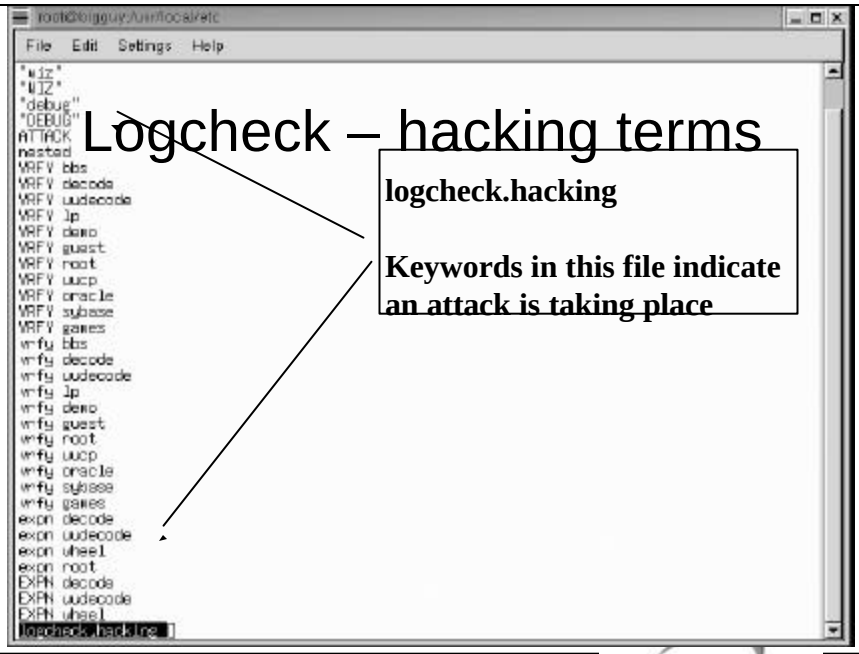
Logcheck ignore



logcheck.ignore

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

Logcheck – hacking terms



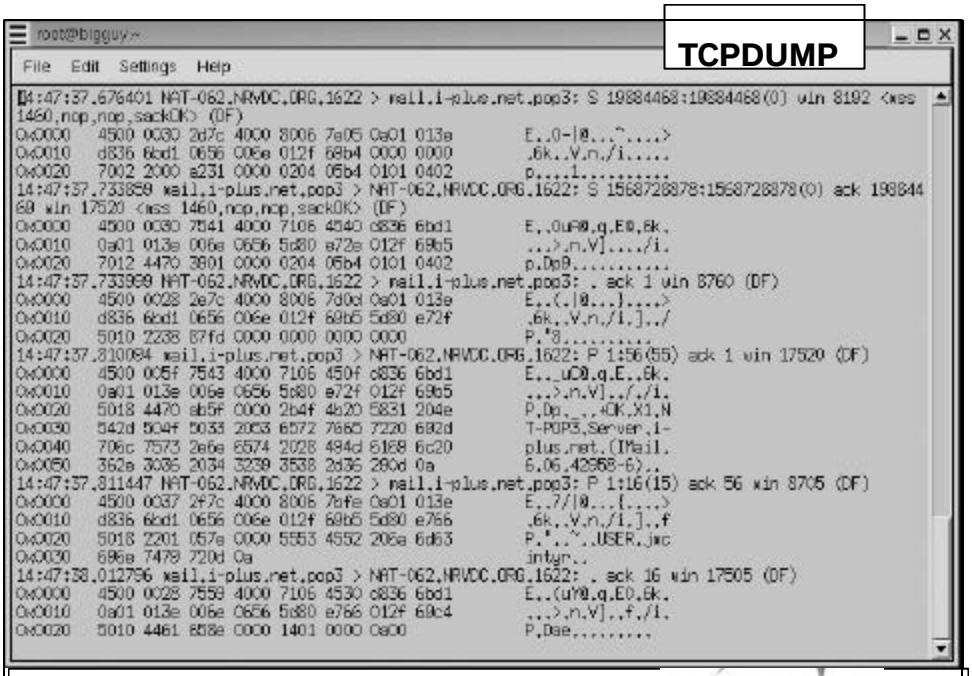
logcheck.hacking

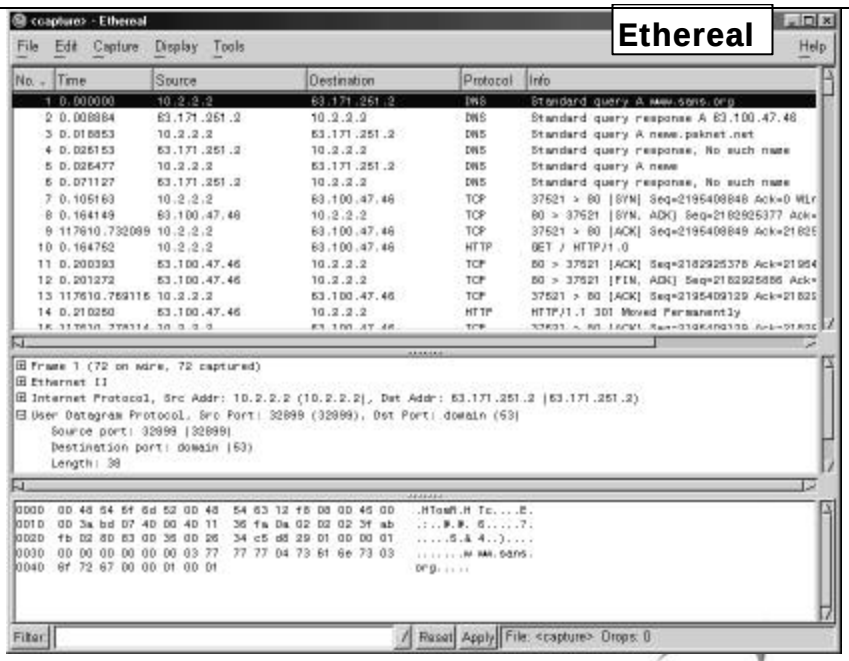
Keywords in this file indicate an attack is taking place

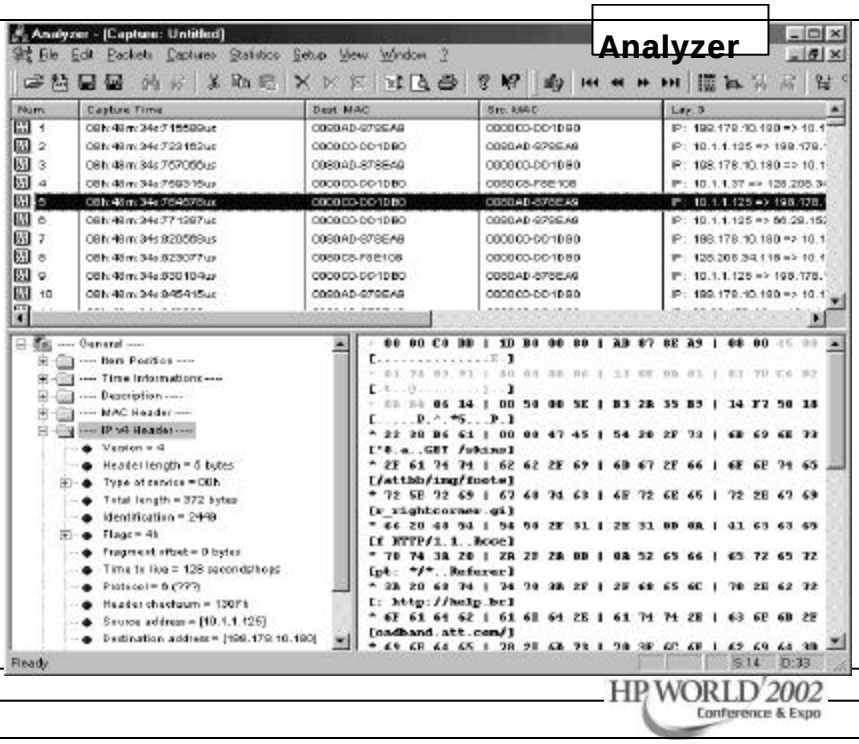
Network Traffic Sniffers

- 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

TCPDUMP

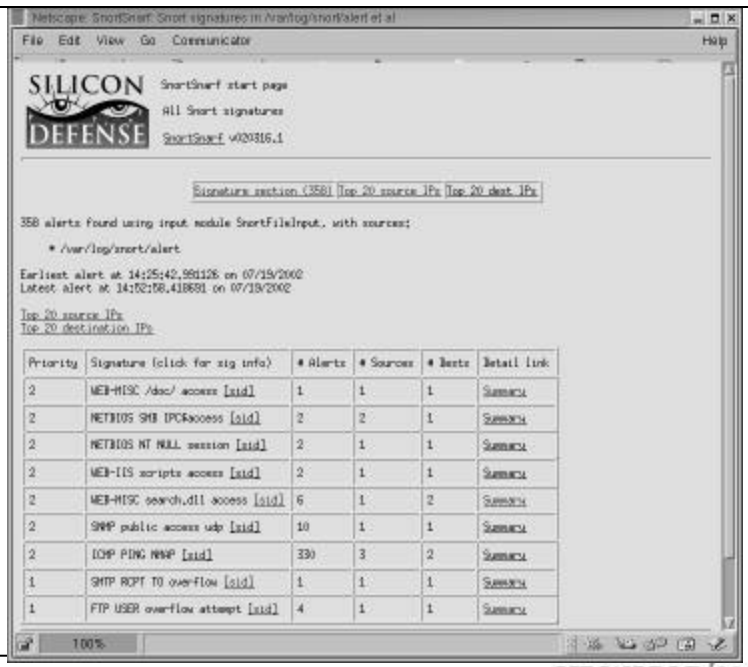


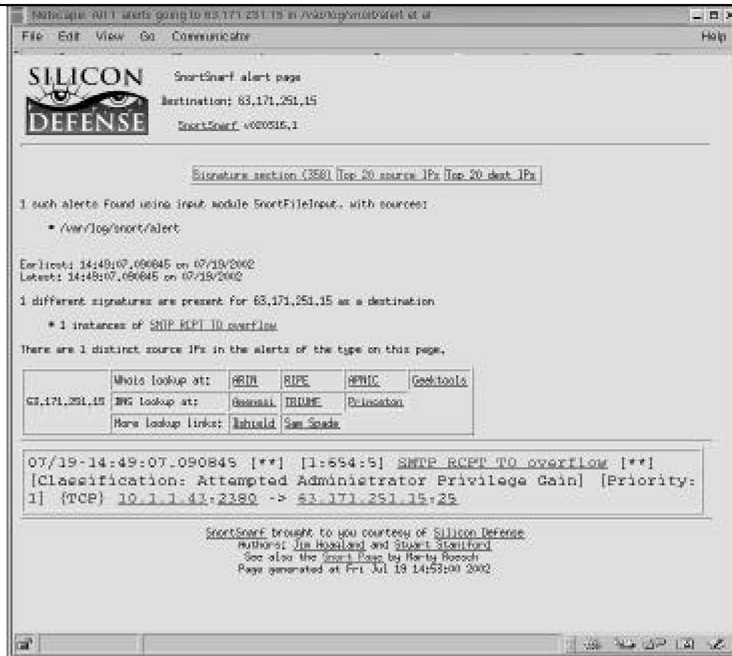




Intrusion Detection Systems - IDS

- Snort
- Shadow
- HP IDS/9000





Netscape: All 1 alerts going to 63.171.251.15 in /var/log/snort/alert et al

File Edit View Go Communicator Help

SILICON DEFENSE

SnortSnarf alert page

Destination: 63.171.251.15

SnortSnarf v020516.1

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: 14:49:07.090845 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

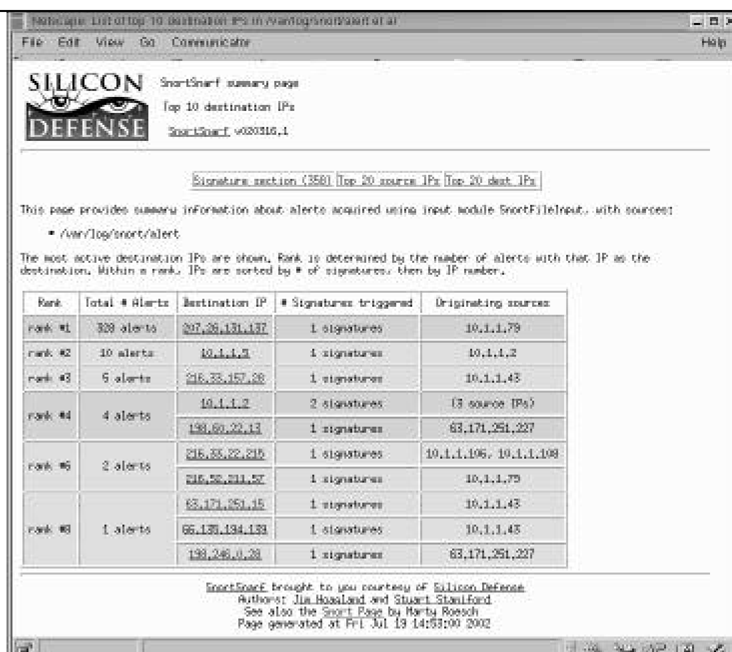
There are 1 distinct source IPs in the alerts of the type on this page.

63.171.251.15	Whois lookup at:	ARIN	RIPE	APNIC	Geektools
	DNS lookup at:	Amenesi	TRIUMF	Princeton	
	More lookup links:	Dshield	Sam Spade		

07/19-14:49:07.090845 [**] [1:654:5] SMTP RCPT TO overflow [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 10.1.1.43:2380 -> 63.171.251.15:25

SnortSnarf brought to you courtesy of Silicon Defense
Authors: Jim Hoagland 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



Netscape: List of top 10 destination IPs in /var/log/snort/alert et al

File Edit View Go Communicator Help

SILICON DEFENSE

SnortSnarf summary page

Top 10 destination IPs

SnortSnarf v020516.1

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	328 alerts	207.26.131.137	1 signatures	10.1.1.79
rank #2	10 alerts	10.1.1.5	1 signatures	10.1.1.2
rank #3	5 alerts	216.33.157.28	1 signatures	10.1.1.43
rank #4	4 alerts	10.1.1.2	2 signatures	(3 source IPs)
		198.60.22.13	1 signatures	63.171.251.227
rank #6	2 alerts	216.33.22.215	1 signatures	10.1.1.106, 10.1.1.108
		216.52.211.57	1 signatures	10.1.1.79
rank #8	1 alerts	63.171.251.15	1 signatures	10.1.1.43
		66.135.194.139	1 signatures	10.1.1.43
		198.246.0.28	1 signatures	63.171.251.227

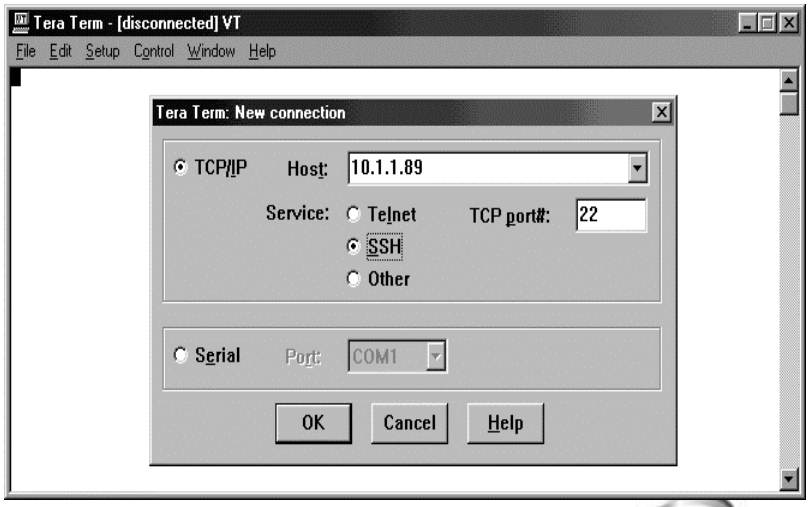
SnortSnarf brought to you courtesy of Silicon Defense
Authors: Jim Hoagland and Stuart Staniford
See also the Snort Page by Marty Roesch
Page generated at Fri Jul 19 14:53:00 2002

HP WORLD 2002 Conference & Expo

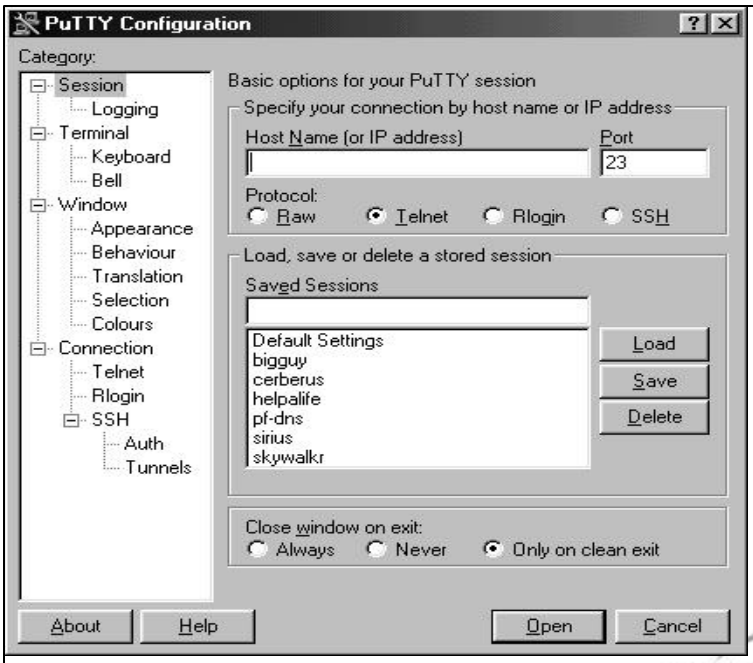
SSH Connectivity Tool

- 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



HP WORLD 2002
Conference & Expo



SSH - Putty

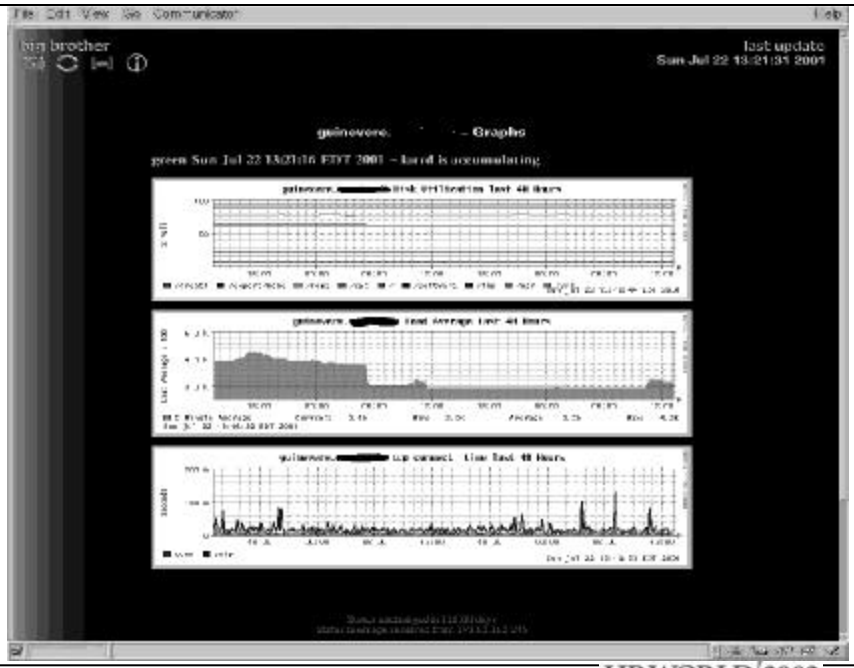
Big Brother

- 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.

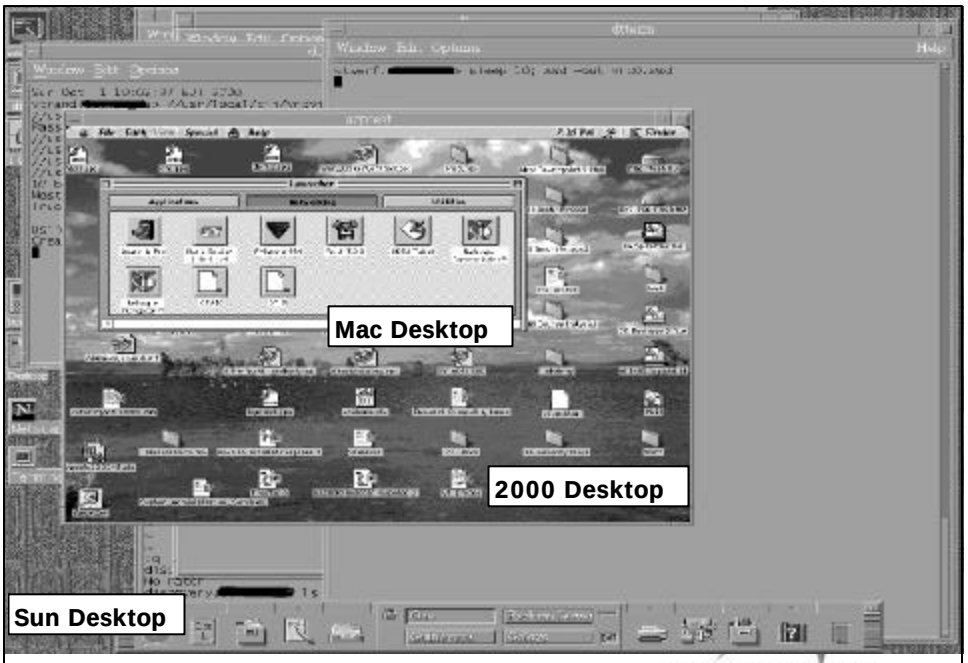
HP WORLD 2002 Conference & Expo



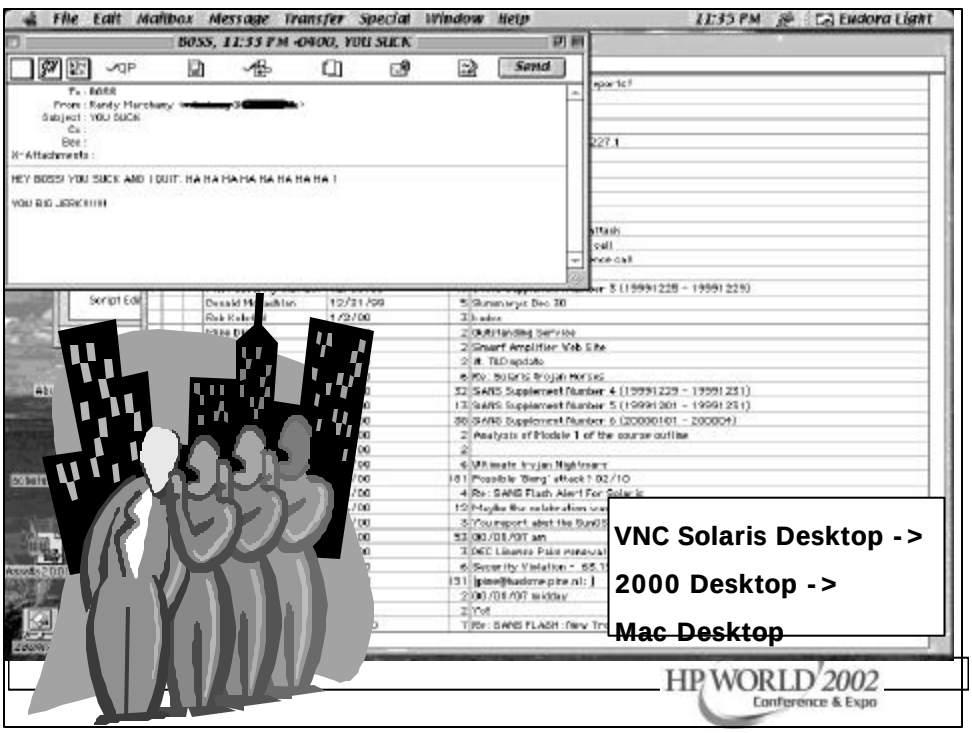
VNCViewer

- 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

HP WORLD 2002 Conference & Expo



HP WORLD 2002 Conference & Expo

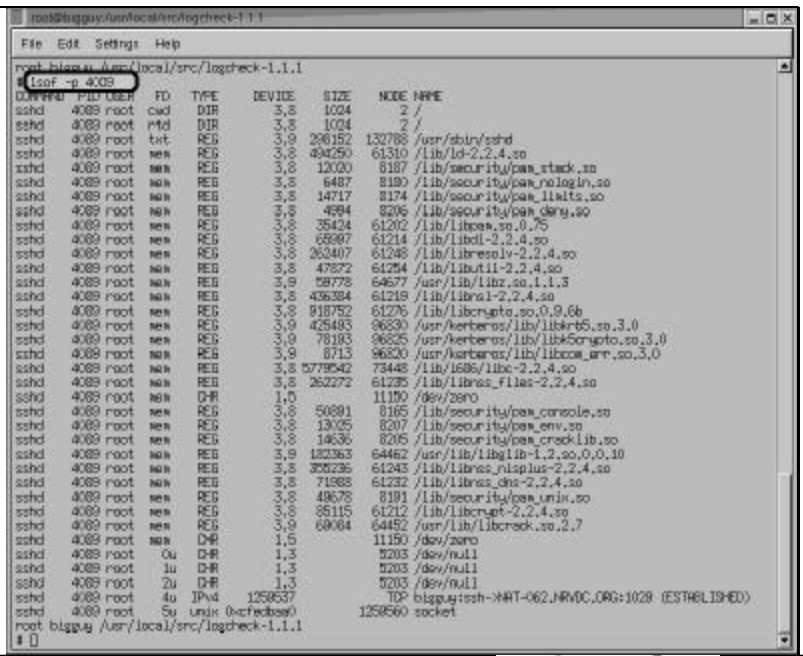


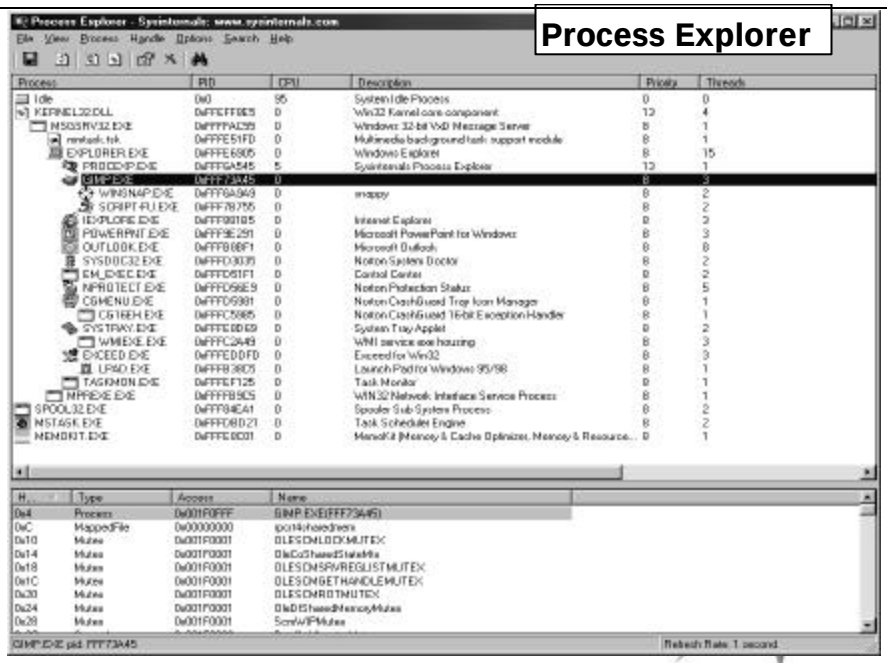
HP WORLD 2002 Conference & Expo

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





Sysadmin Tools

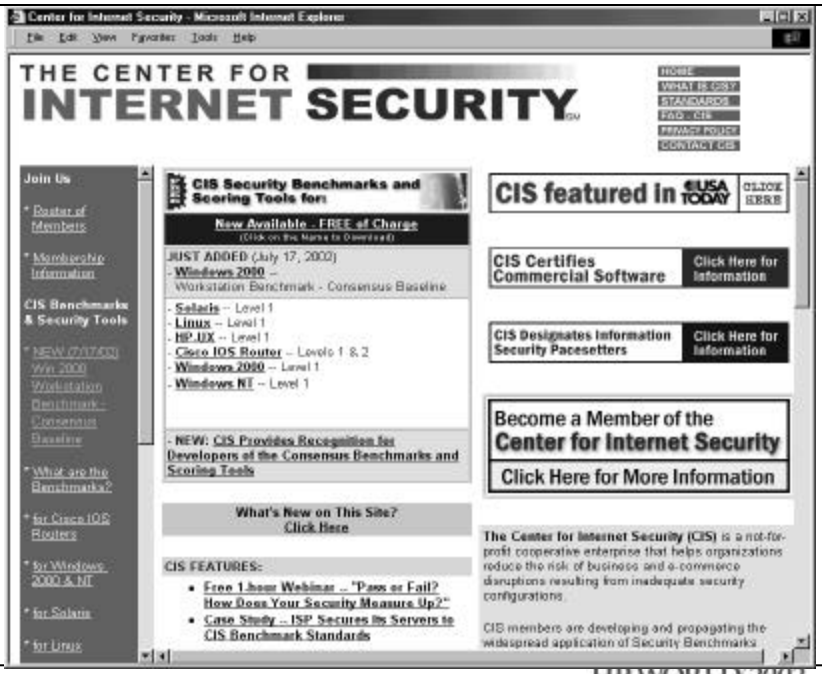
- **Sudo**
  - Unix access control is all (root) or nothing (user).
  - Some commands (backup, restore) are restricted to root but are really an OPER class command. You don't want an operator to have root access but you want them to do backups.
  - Sudo lets you set up this "pseudo" privilege scheme.

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

Crack - l0phtcrack

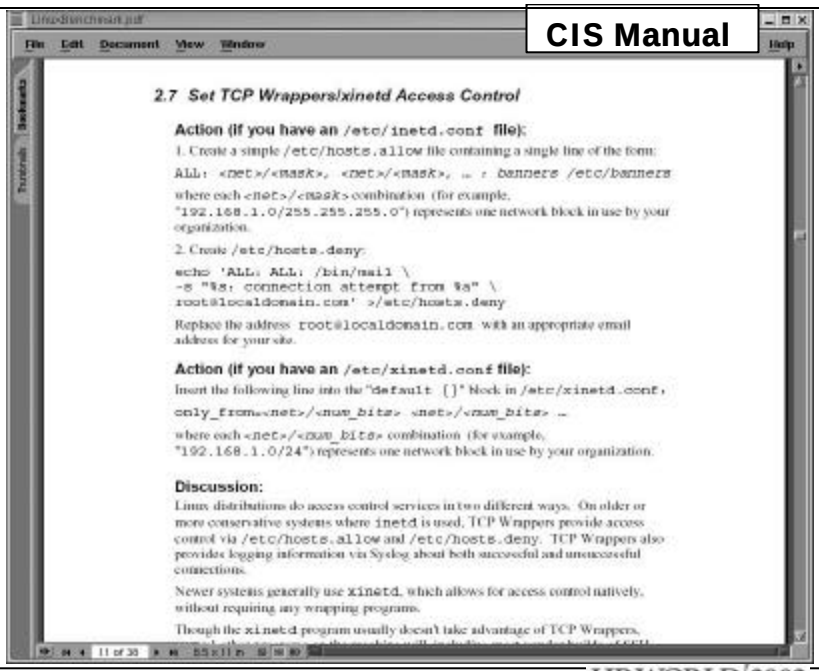
- The first of the really good password crackers. Available on the net for the past 10 years.
- Easy to customize. Works on non-shadow password files.
- Use a preprocessor to rebuild in old format or use NIS, NIS+ ☺
- Can be distributed among systems
- Have AUTHORIZATION to RUN !!!



CIS Ruler Report

```
File  Edit  Settings  Help
*** CIS Ruler Run ***
Starting at time 20020415-10:44:06

Positive: 1.1 System appears to have been patched within the last month.
Positive: 2.2 Authorized usage banners are configured well in inetd/xinetd.
Positive: 2.3 telnet is deactivated.
Positive: 2.4 ftp is deactivated.
Positive: 2.5 rsh, rcp and rlogin are deactivated.
Positive: 2.6 tftp 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 portmapper has been deactivated.
Positive: 3.7 samba windows filesharing daemons are deactivated.
Positive: 3.8 netfs rc 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 inetd/xinetd not activated.
Positive: 3.20 Found a good daemon umask.
Positive: 4.1 Coredumps are deactivated.
Positive: 4.2 /etc/exports is empty or doesn't exist, so it doesn't need to be tuned for privports.
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 nosuid.
:
```

CIS Manual



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 "%d: connection attempt from %a" \
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>/<num_bits> <net>/<num_bits> …`

where each `<net>/<num_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,

HP WORLD 2002 Conference & Expo

Summary

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

HP WORLD 2002 Conference & Expo

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/
  - 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
  - LogSentry, portsentry
- 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
  - Ipfilter or HP Ipfilter/9000
- www.snort.org
  - Snort, SnortSnarf, SnortSort
- devresource.hp.com
- hpux.cs.utah.edu
- thewrittenword.com
- www.interex.org
- www.software.hp.com