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
  - Portsentry
- 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/

HP WORLD 2002 Conference & Expo

Nessus

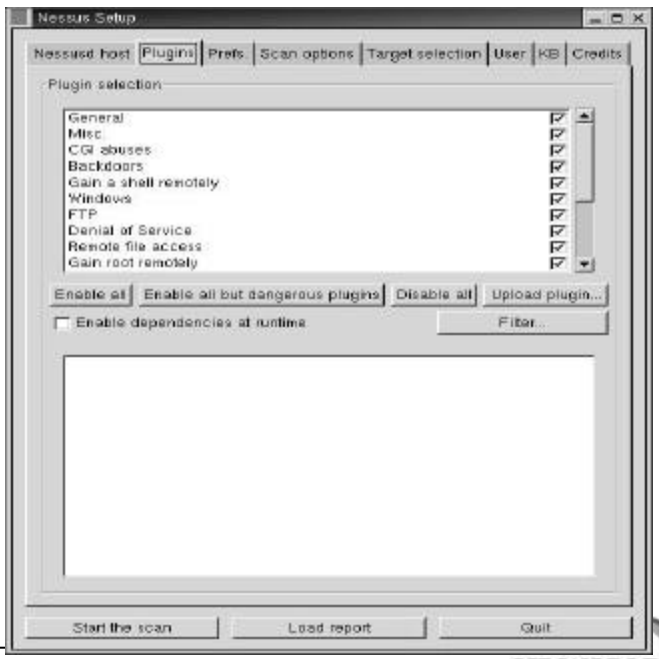
- Best of the scanning tools
- Easy to build for Linux, harder for Solaris & HPUX, need to work on other OS.
- Requires GNU tools
- Provides HTML based reports
- Has distributed architecture: clients (Windows, Unix) & engines (Unix only)

Nessus – Building It

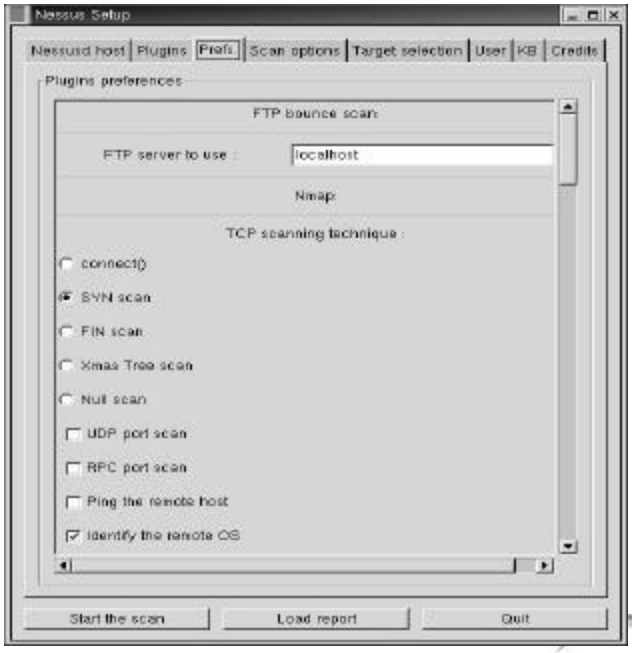
- Linux
  - Download the RPMs
  - Add nessus user
  - Start up nessusd daemon
  - Start up nessus client
  - Start testing
- Windows Client
  - Download executable & run

Nessus – Pros/Cons

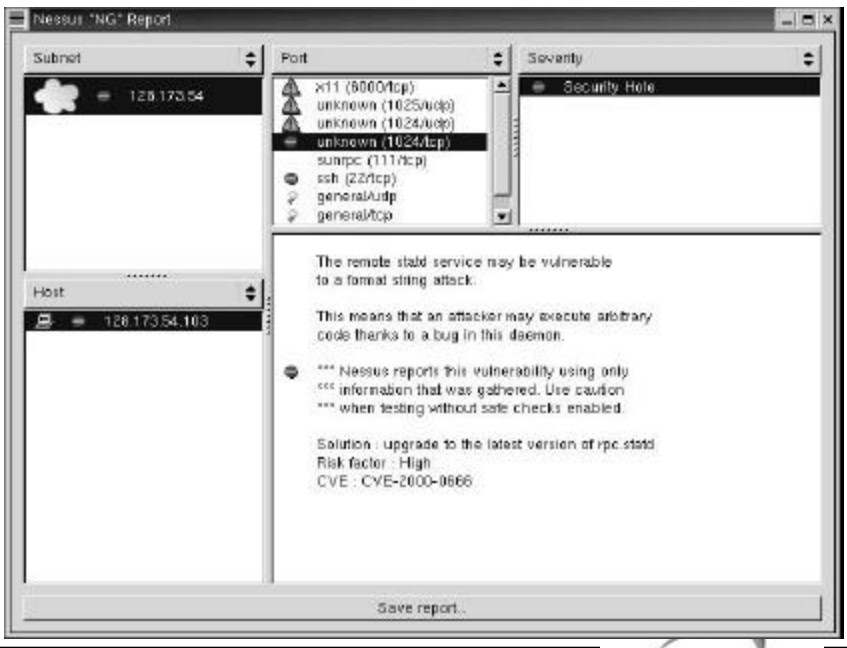
- Pros
  - Easy to install if you have linux
  - Most comprehensive tests for your money
- Cons
  - Not that easy to understand at first
  - Non-linux builds require GNU software
  - Some inconsistency in quality of checks
  - Must use Unix server for specific user accounts



HP WORLD 2002 Conference & Expo



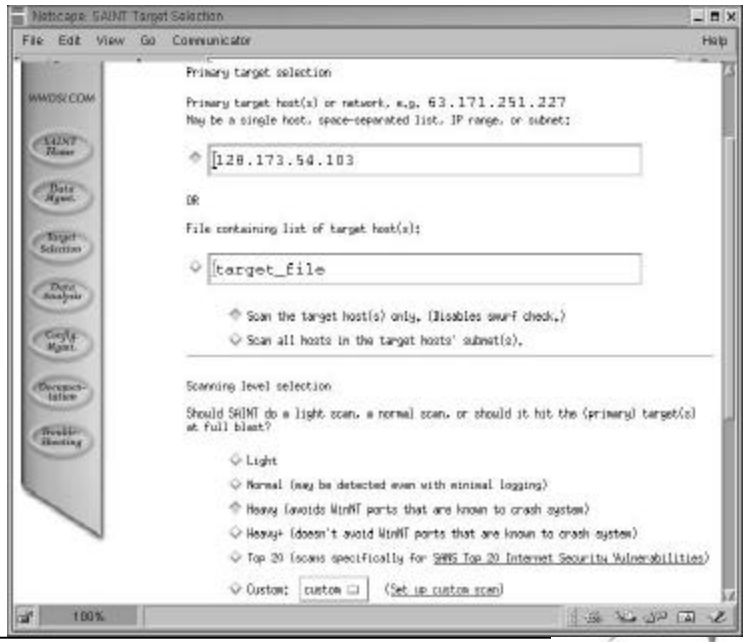
HP WORLD 2002 Conference & Expo



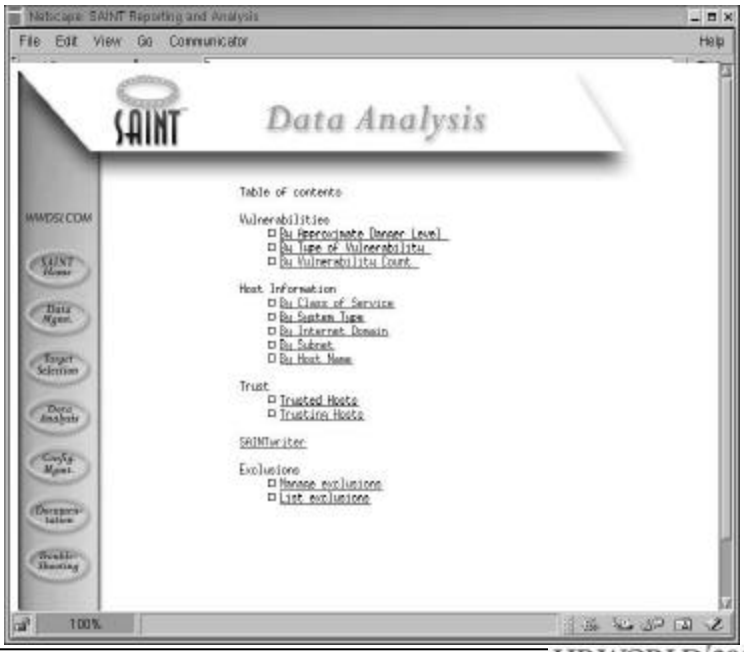
HP WORLD 2002 Conference & Expo

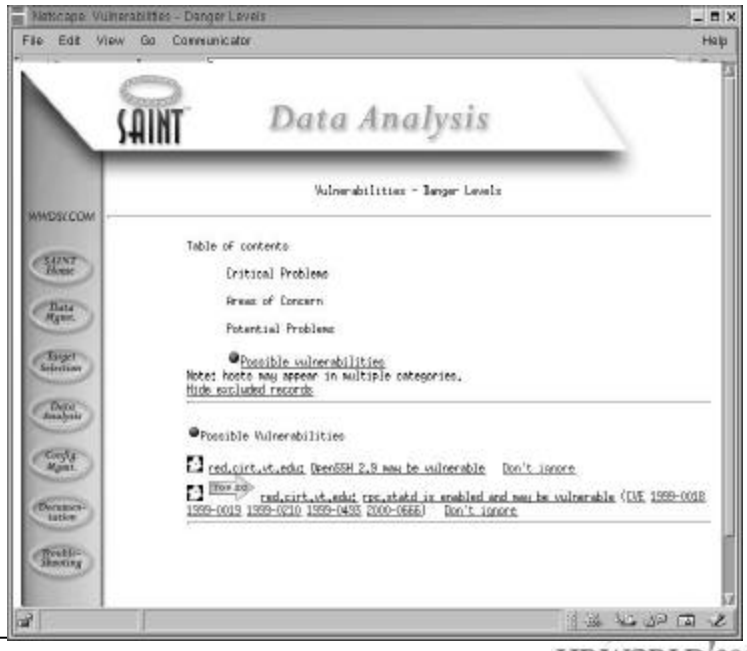
SAINT

- 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



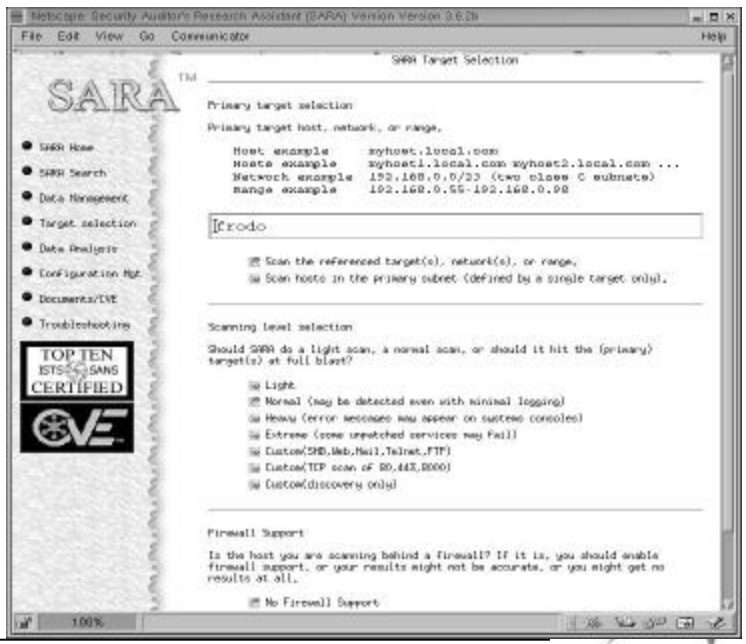
HP WORLD 2002 Conference & Expo

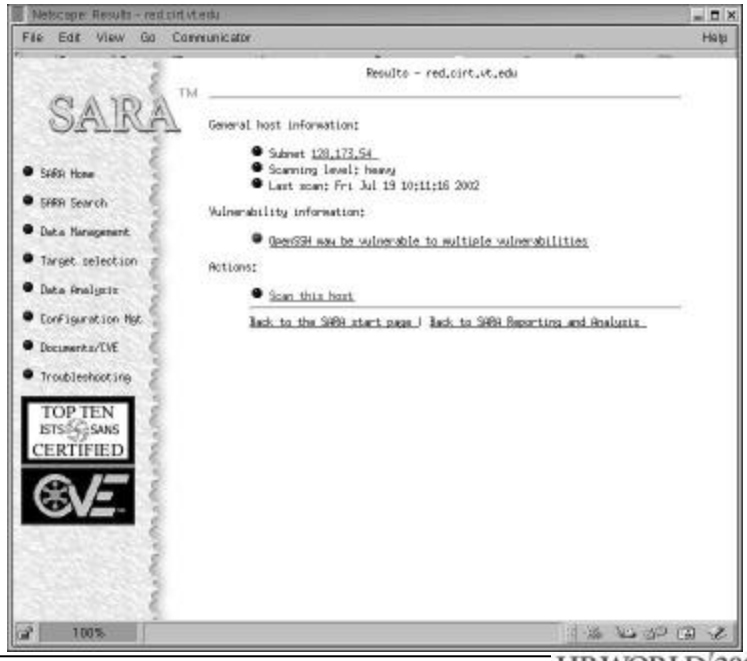

Netscape: SAINT Reporting and Analysis
File Edit View Go Communicator Help
SAINT
Data Analysis
WWDSI.COM
Table of contents
Vulnerabilities
By Appropriate Danger Level
By Type of Vulnerability
By Vulnerability Count
Host Information
By Class of Service
By System Type
By Internet Domain
By Subnet
By Host Name
Trust
Trusted Hosts
Trusting Hosts
SAINTwriter
Exclusions
Manage exclusions
List exclusions
100%

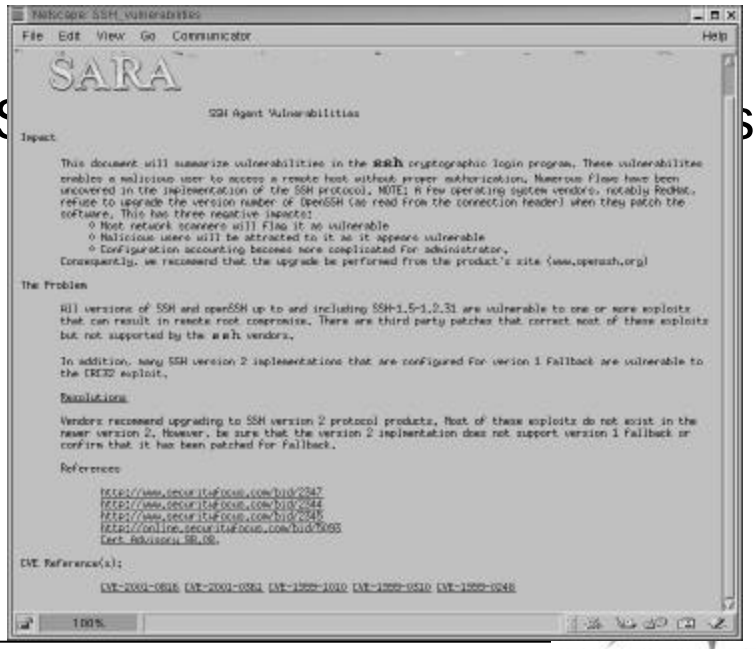

Netscape: Vulnerabilities - Danger Levels
File Edit View Go Communicator Help
SAINT
Data Analysis
WWDSI.COM
Vulnerabilities - Danger Levels
Table of contents
Critical Problems
Areas of Concern
Potential Problems
Possible vulnerabilities
Notes: hosts may appear in multiple categories.
Hide excluded records
Possible Vulnerabilities
red.cirt.vt.edu OpenSSH 2.9 may be vulnerable Don't ignore
Top
red.cirt.vt.edu rpc.statd is enabled and may be vulnerable (CVE 1999-0018 1999-0019 1999-0210 1999-0493 0000-0666) Don't ignore

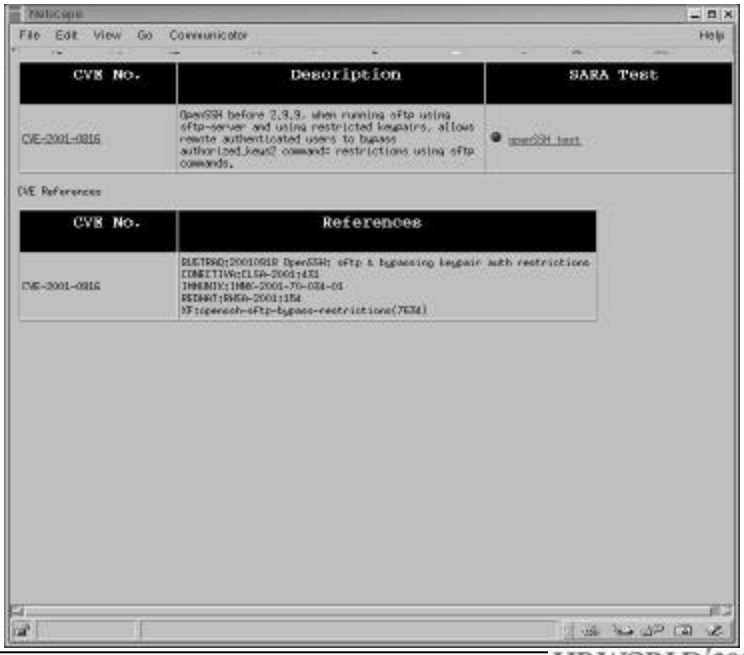
SARA

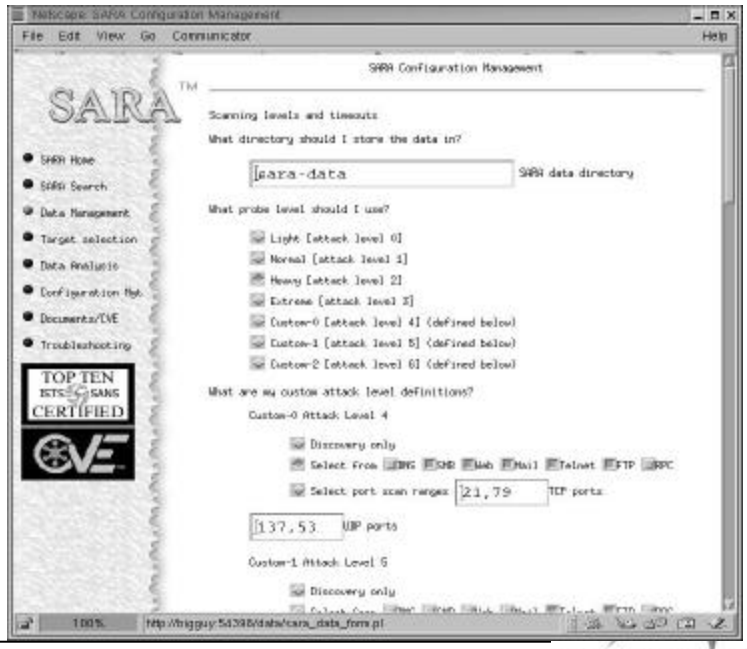
- Security Auditor's Research Assistant
- Checks for SANS Top 20 Threats
- Does Unix/Windows vulnerability tests
- Has CVE dictionary support
- Search engine for post audit analysis
- Uses CIS Benchmarks
- Has a Report Writer




Netscape: Results - red.cirt.vt.edu
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
SANS
CERTIFIED
100%


Netscape: SSH vulnerabilities
File Edit View Go Communicator Help
SARA
SSH Agent Vulnerabilities
Impact
This document will summarize vulnerabilities in the ssh cryptographic login program. These vulnerabilities enables a malicious user to access a remote host without proper authorization. Numerous flaws have been uncovered in the implementation of the SSH protocol. NOTE: A few operating system vendors, notably RedHat, refuse to upgrade the version number of OpenSSH (as read from the connection header) when they patch the software. This has three negative impacts:
Most network scanners will flag it as vulnerable
Malicious users will be attracted to it as it appears vulnerable
Configuration accounting becomes more complicated for administrator.
Consequently, we recommend that the upgrade be performed from the product's site (www.openssh.org)
The Problem
All versions of SSH and openSSH up to and including SSH-1.5-1.2.31 are vulnerable to one or more exploits that can result in remote root compromise. There are third party patches that correct most of these exploits but not supported by the ssh vendors.
In addition, many SSH version 2 implementations that are configured for version 1 Fallback are vulnerable to the CRC32 exploit.
Resolutions
Vendors recommend upgrading to SSH version 2 protocol products. Most of these exploits do not exist in the newer version 2. However, be sure that the version 2 implementation does not support version 1 fallback or confirm that it has been patched for Fallback.
References
http://www.securityfocus.com/bid/2347
http://www.securityfocus.com/bid/2344
http://www.securityfocus.com/bid/2343
http://online.securityfocus.com/bid/5093
Cert Advisory CA-98.
CVE Reference(s):
CVE-2001-0816 CVE-2001-0361 CVE-1999-1010 CVE-1999-0510 CVE-1999-0348
100%


Netscape
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:CLA-2001:431
IMMUNIX:IMNX-2001-70-034-01
REDHAT:RHSA-2001:154
XF:openssh-sftp-bypass-restrictions(7634)


Netscape: SARA Configuration Management
File Edit View Go Communicator Help
SARA
SARA Configuration Management
SARA Home
SARA Search
Data Management
Target selection
Data Analysis
Configuration Mgt.
Documents/CVE
Troubleshooting
TOP TEN
ISTS SANS
CERTIFIED
Scanning levels and timeouts
What directory should I store the data in?
sara-data
SARA data directory
What probe level should I use?
Light [attack level 0]
Normal [attack level 1]
Heavy [attack level 2]
Extreme [attack level 3]
Custom-0 [attack level 4] (defined below)
Custom-1 [attack level 5] (defined below)
Custom-2 [attack level 6] (defined below)
What are my custom attack level definitions?
Custom-0 Attack Level 4
Discovery only
Select From DNS SMB Web Mail Telnet FTP RPC
Select port scan range: 21,79 TCP ports
137,53 UDP ports
Custom-1 Attack Level 5
Discovery only

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

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
  - Tcpwrappers 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

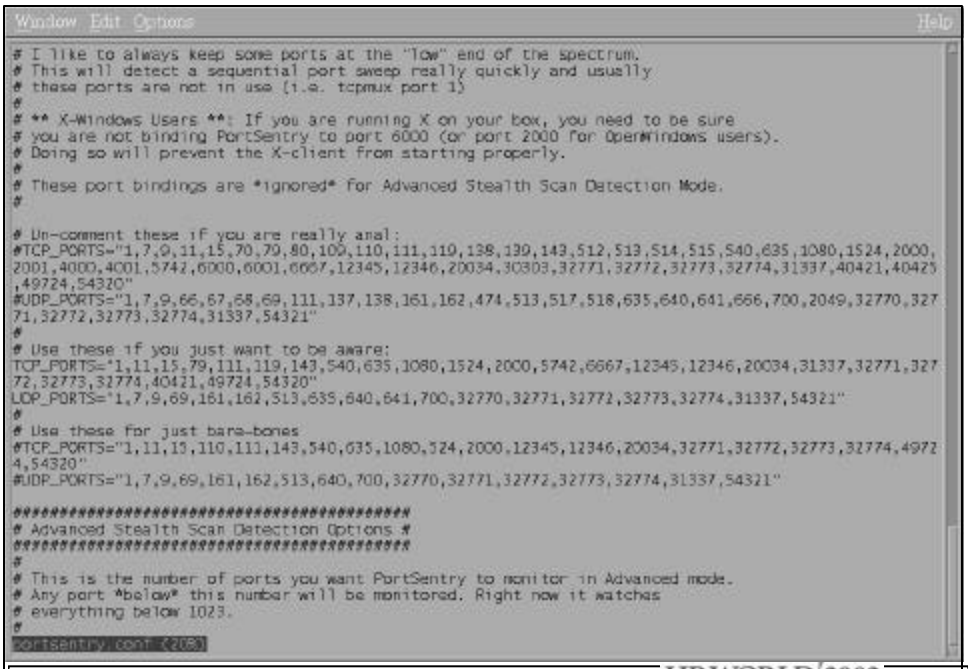
- Access Control is enabled by default.
- 2 files
  - /etc/hosts.deny – restrict access if IP addr here
  - /etc/hosts.allow – allow access if IP addr here
    - Can restrict to username@host if services are enabled
- Reverse lookup is done. Paranoid selection terminates the connection immediately if 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

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



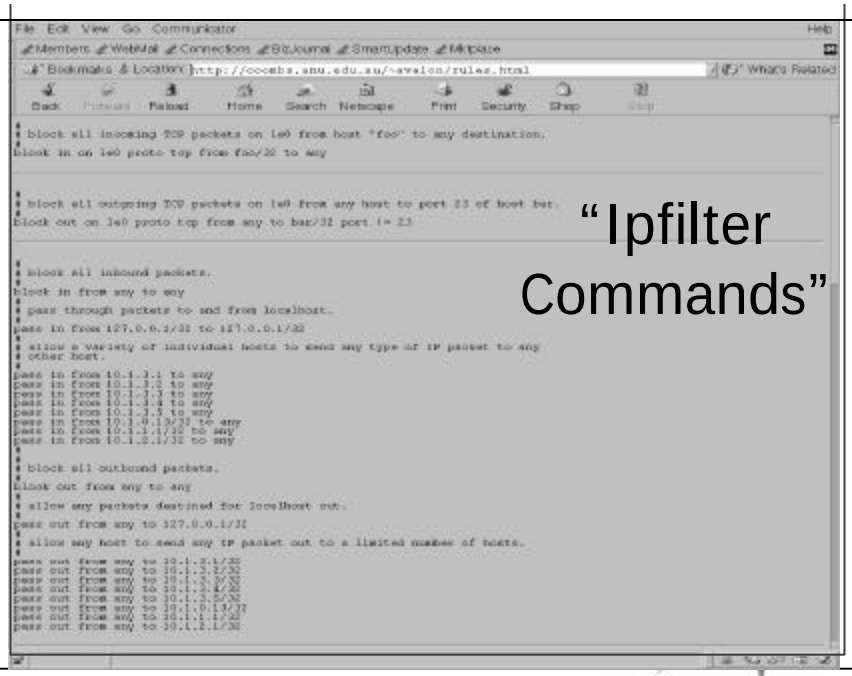
Personal Firewall Tools

- 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.

HP WORLD 2002 Conference & Expo

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



"Ipfilter Commands"

Ipfilter output

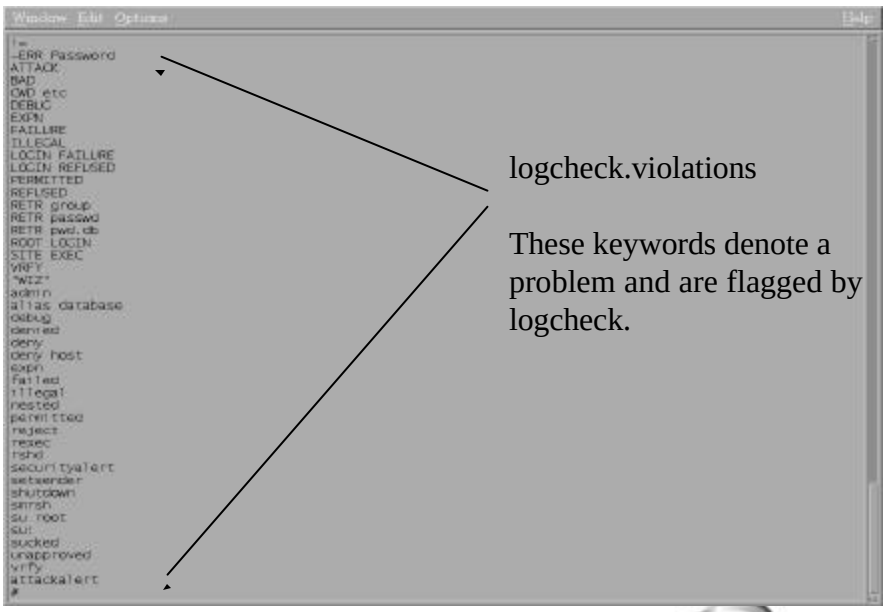
```
Jul 30 01:46:52 myhost. ipmon[147]: [ID
702911local0.warning] 01:46:52.196772 hme0 @0:5 b
194.143.66.126,21 ->198.82.255.255,21 PR tcp len 20 40 -S IN

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
```

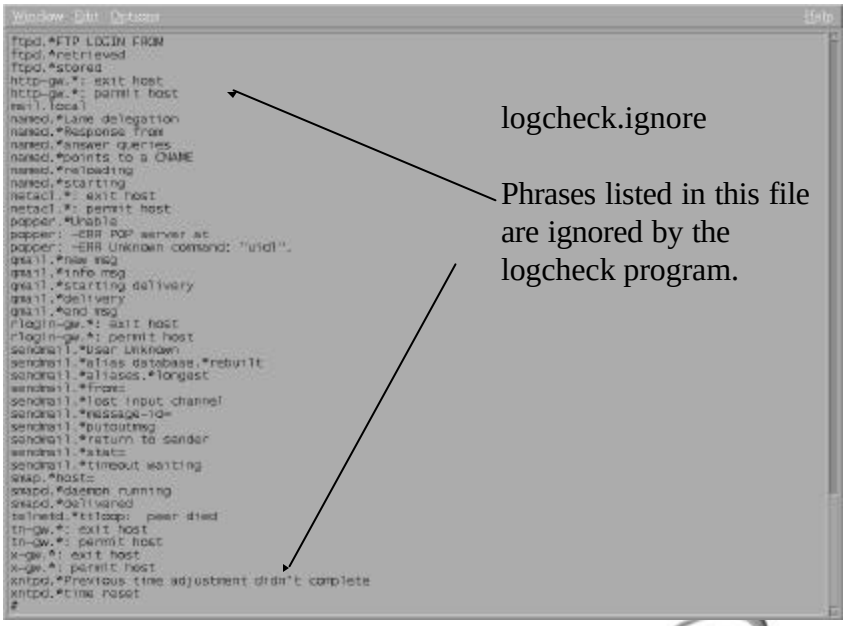

Iptable Commands

```
root@blgguy:~
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/TDP) NTP  connections from local to External
        echo "  NTP (123/TDP) 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/TDP-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

:
```

Logcheck

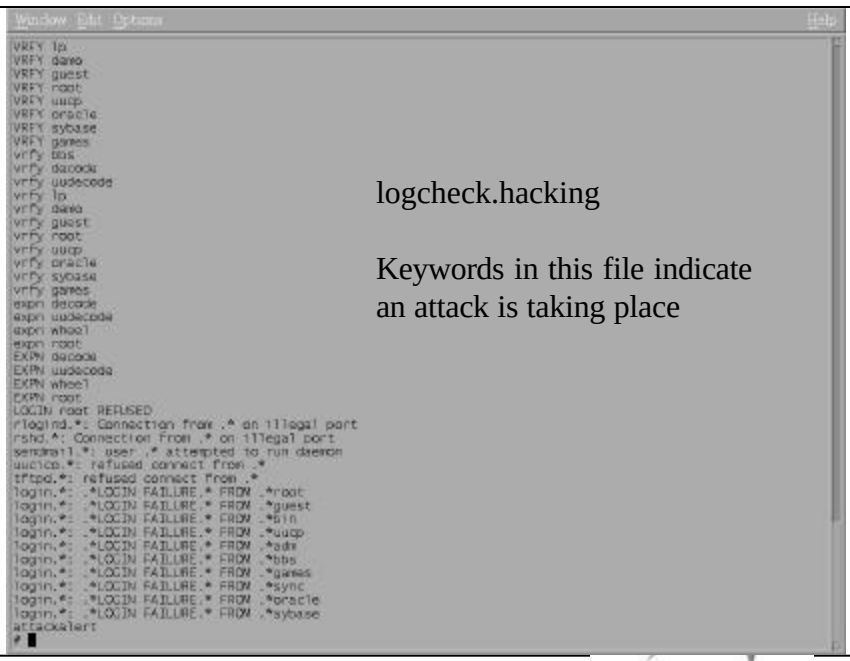
- Syslog keyword scanner
- When it matches something, it does something
  - Send email
  - Page someone
  - Run a command





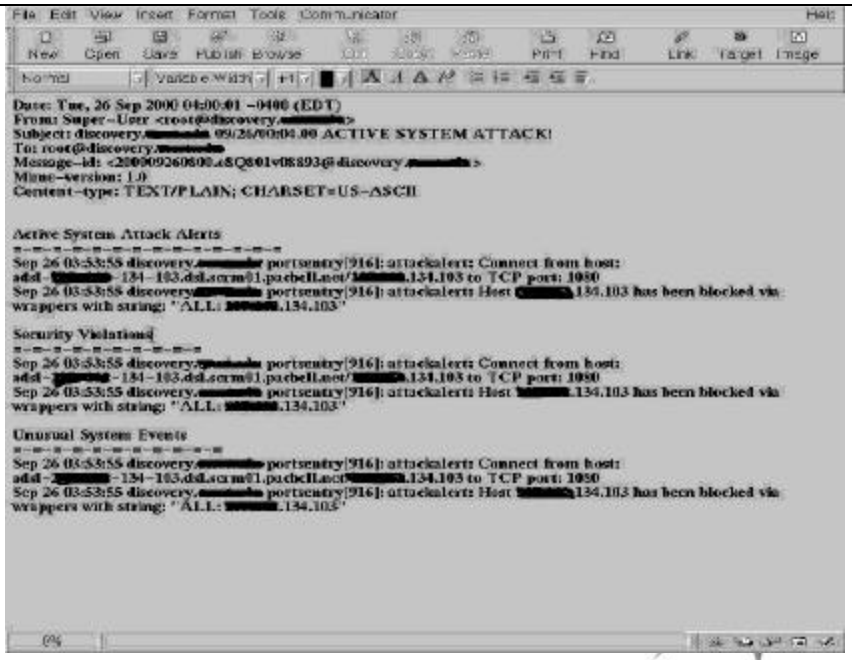
logcheck.ignore

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



logcheck.hacking

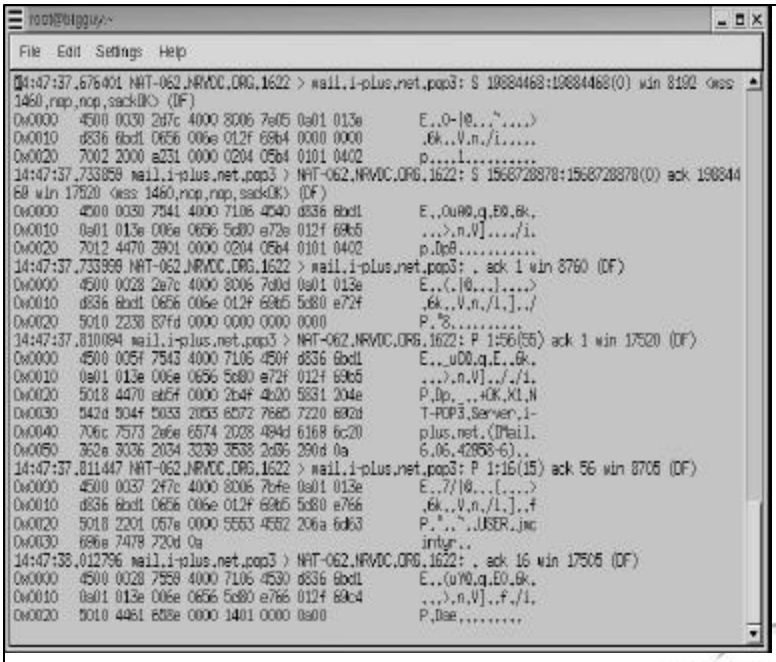
Keywords in this file indicate an attack is taking place



Sniffers: snoop, iptrace, tcpdump, snort, windump

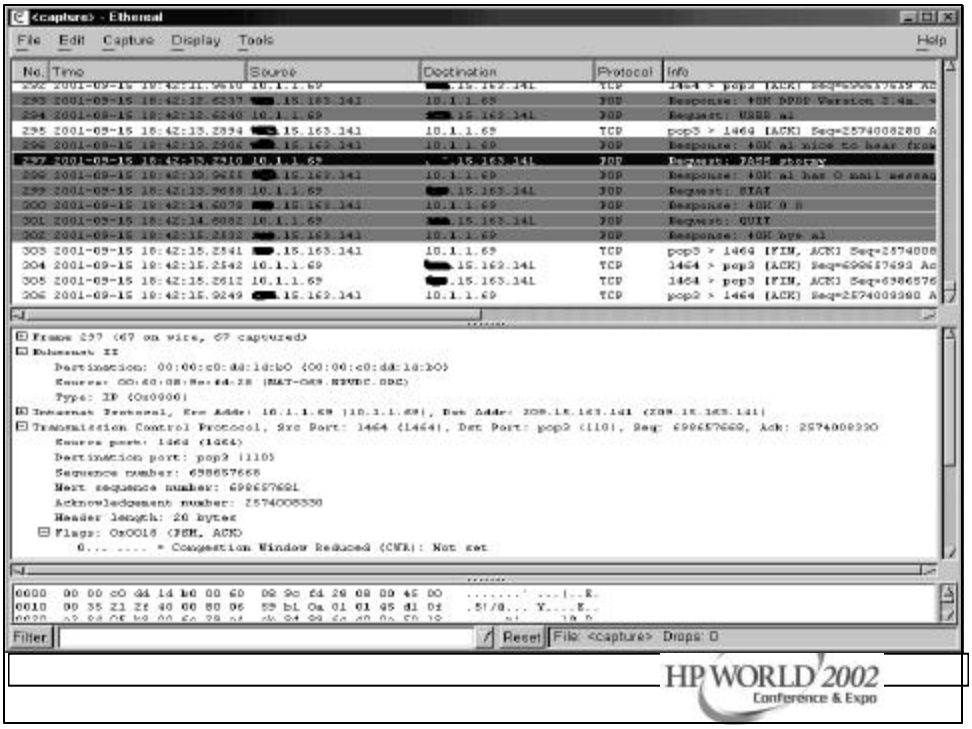
- Some systems have builtin sniffers
  - Solaris - snoop
  - AIX - iptrace
  - Linux/HP-UX – tcpdump, ethereal
  - 98/NT/2000 – netwatch, windump
- Tcpdump is the generic sniffer for those systems with no builtin sniffer

HP WORLD 2002 Conference & Expo

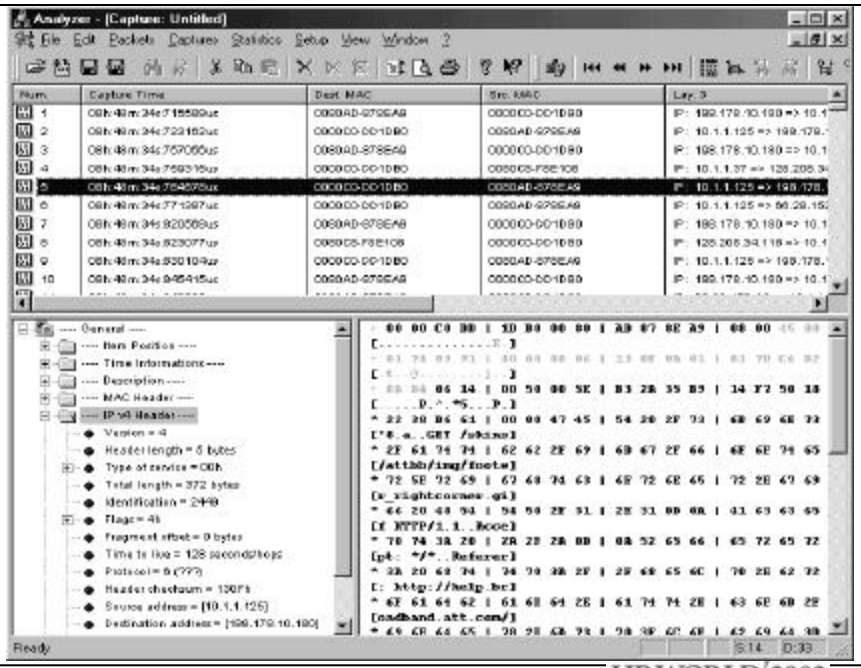


TCPDUMP Command

HP WORLD 2002 Conference & Expo



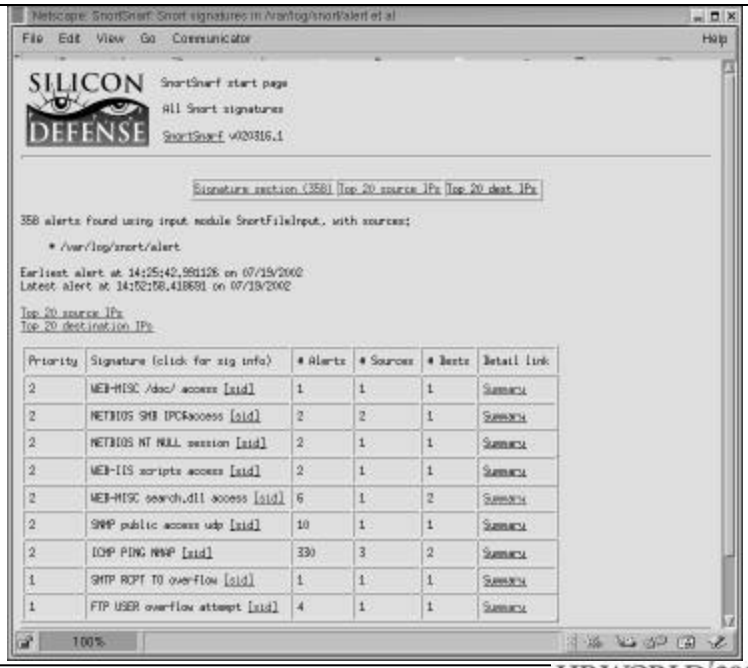
HP WORLD 2002 Conference & Expo

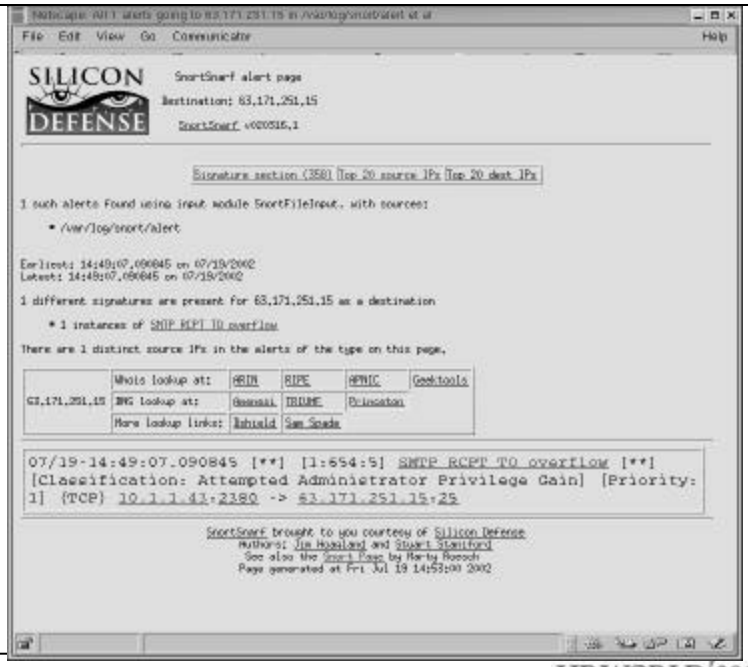


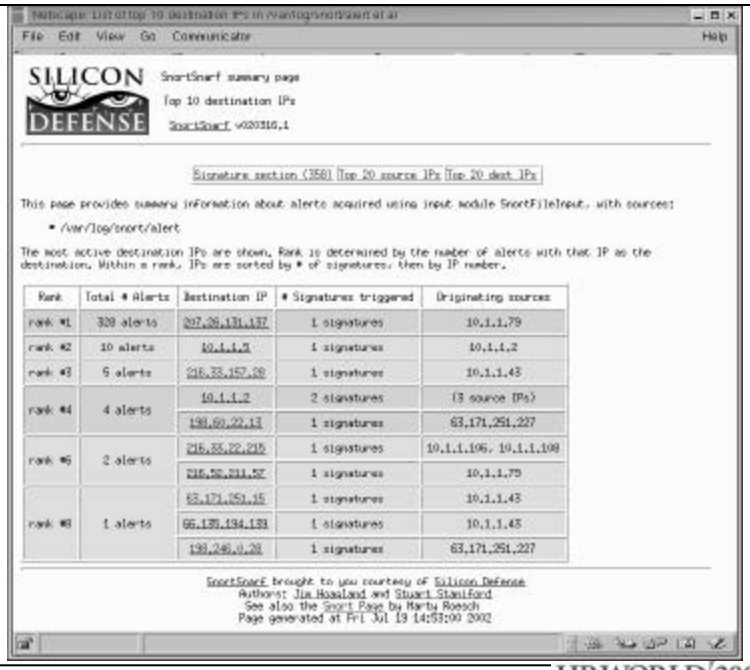
Intrusion Detection Systems - IDS

- Snort
- Shadow
- HP IDS/9000

HP WORLD 2002
Conference & Expo



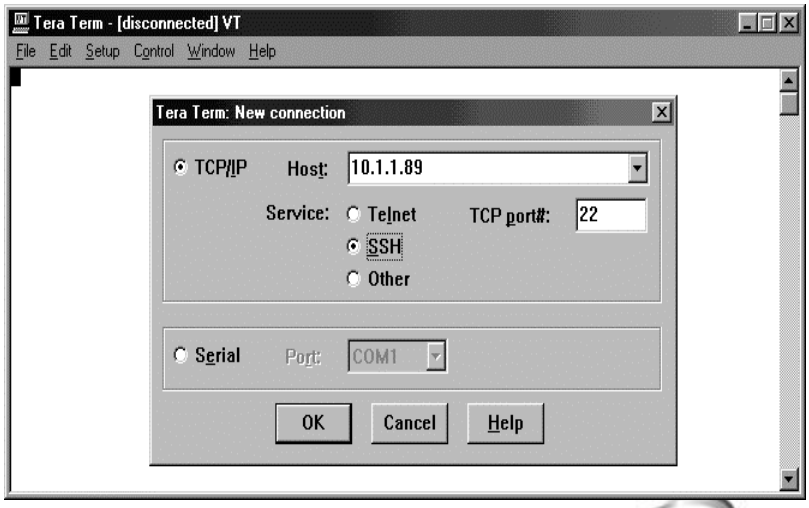




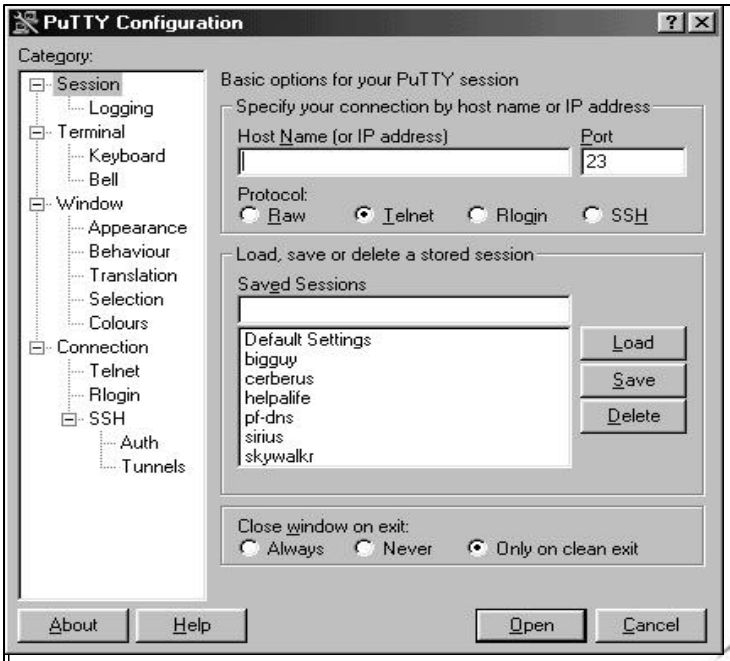
SSH Connectivity Tool

- 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



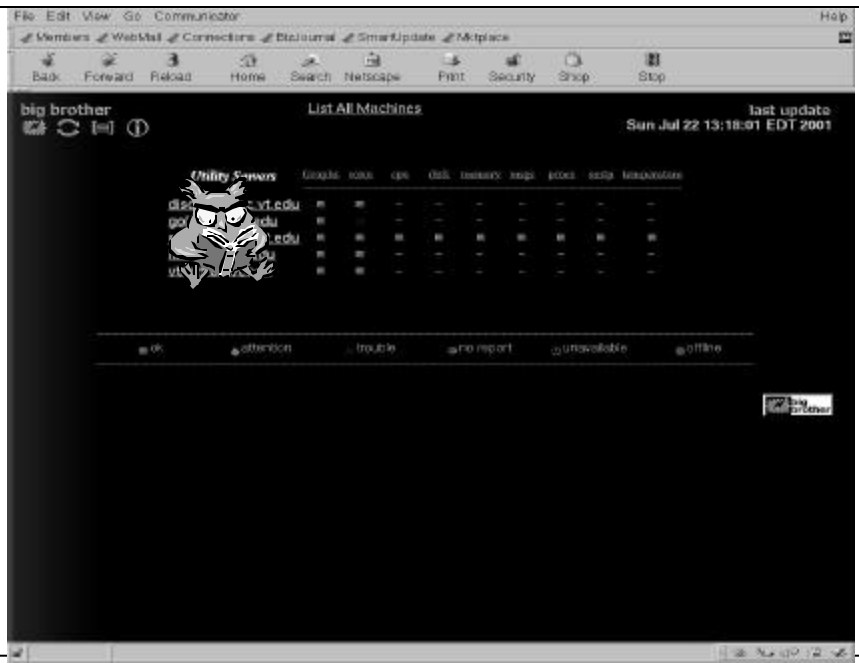
Big Brother

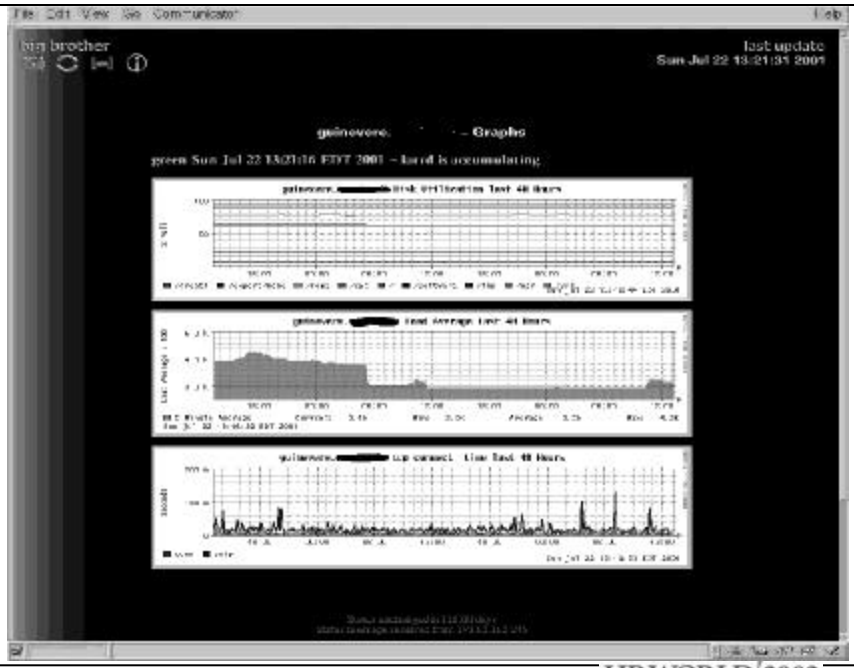
- Web based system and network monitor
- Client server model
  - Clients run on the systems you want to monitor
  - Simple shell scripts that monitor different aspects of your system and network
- What can it check?
  - Disk space, CPU Utilization, critical processes, weather parameters, building monitors

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.


File Edit View Go Communicator Help
Members WebMail Connections BizJournal SmartUpdate Mktplace
Back Forward Reload Home Search Netscape Print Security Shop Stop
big brother
List All Machines
last update
Sat Jul 21 06:02:15 EDT 2001
Tape Mounts
TapeMounts
Pages Hosted Locally
4Help Servers
Big Brother Monitoring Systems
Blacksburg Electronic Village
Building Facilities
Communications Network Services
Computing Center
DBServers
Educational Technologies
Engineering
IWAServers
Legacy Tape Servers
Mail, News, and Directory Servers
Network Backup Servers
Print Servers
Registration Servers
Utility Servers
Video Conferencing
Ward Group


File Edit View Go Communicator Help
Members WebMail Connections BizJournal SmartUpdate Mktplace
Back Forward Reload Home Search Netscape Print Security Shop Stop
big brother
List All Machines
last update
Sun Jul 22 13:18:01 EDT 2001
Utility Servers
ok
attention
trouble
no report
unavailable
offline



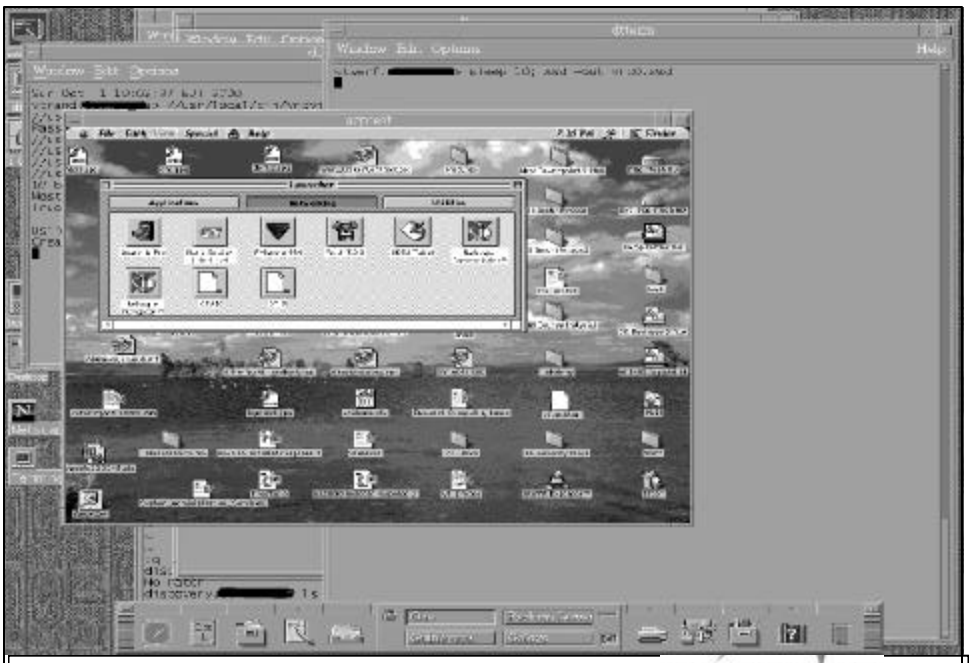
Big Brother

- 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.

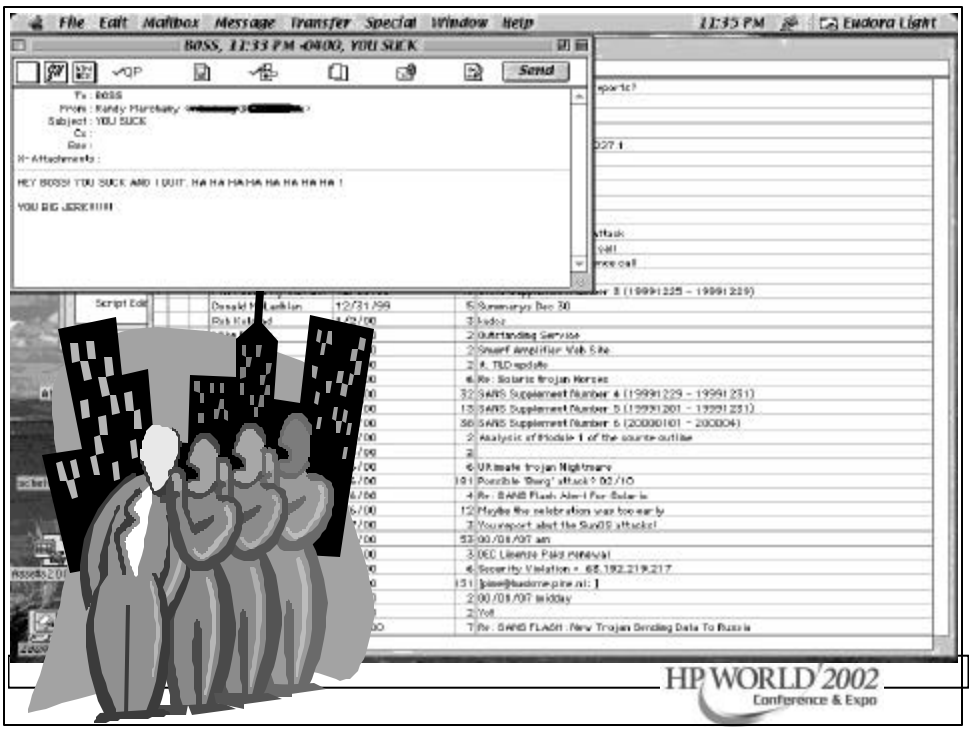
HP WORLD 2002
Conference & Expo

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

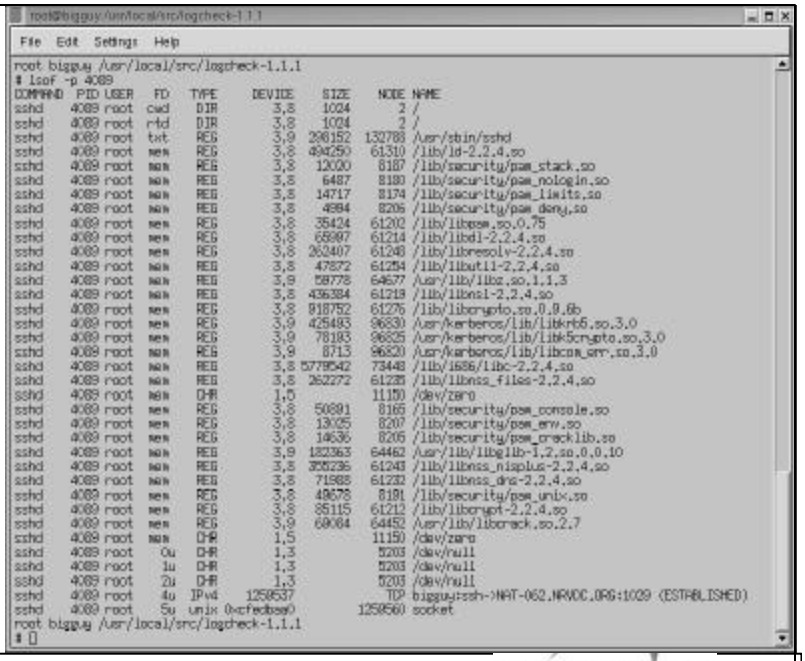


HP WORLD 2002
Conference & Expo

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



inzider

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

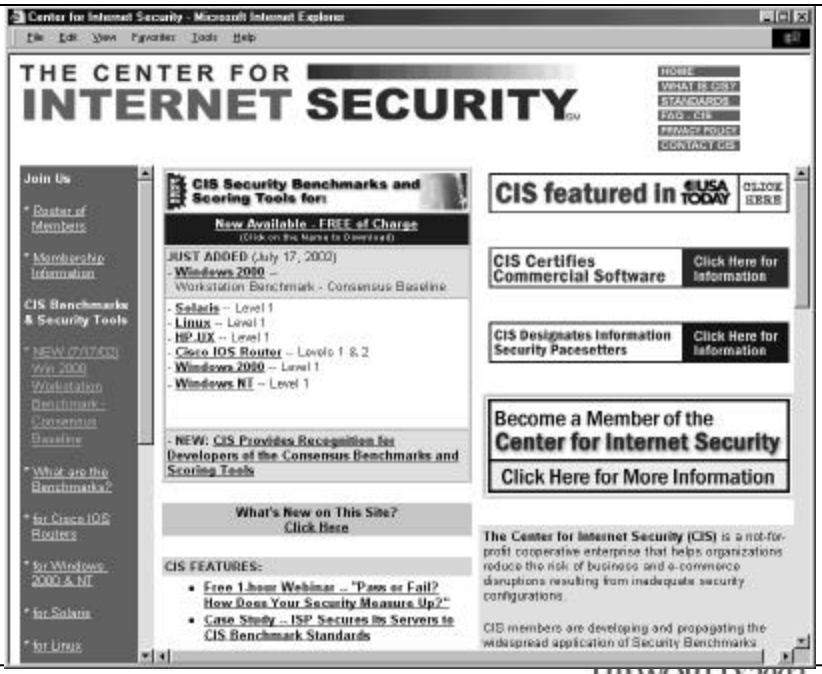
- Advantages
  - Good warning if someone tries to use it incorrectly.
  - Easy to configure for multiple machines
  - Adequate internal security checks
    - Check for "." in PATH
    - Removes LD* variables before execution
- Disadvantages
  - Works with root userid only. Can't use with other userids.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

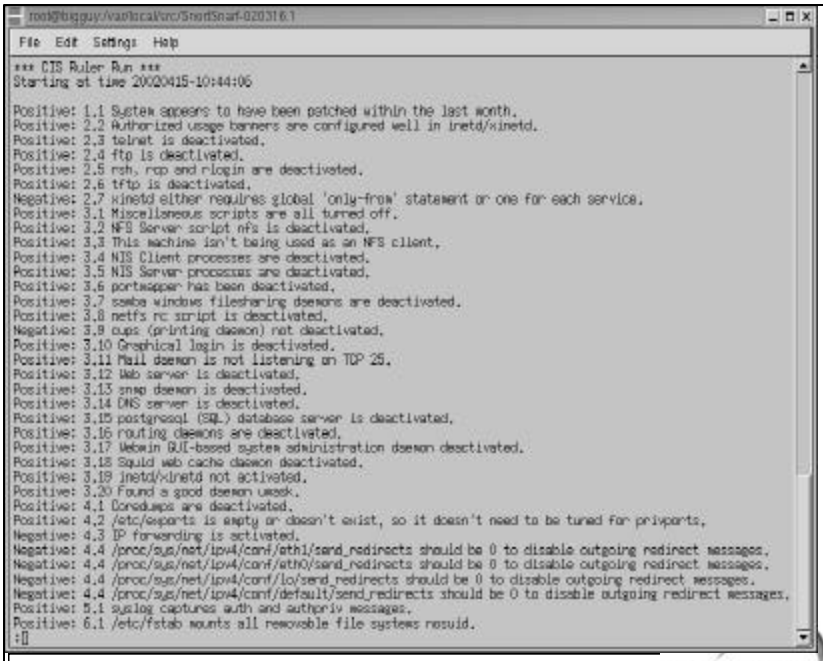
Proactive Password Tools

- 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

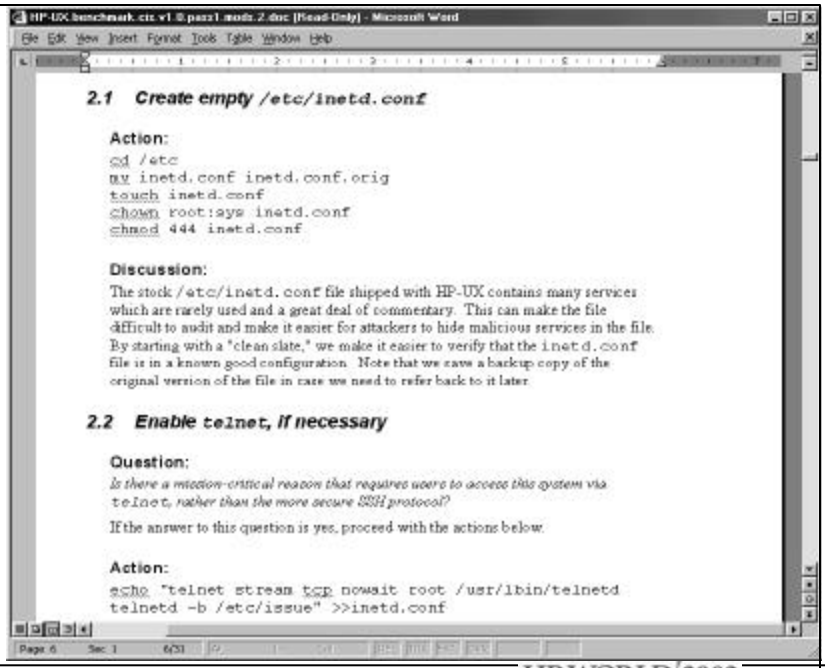
- The first of the really good password crackers. Available on the net for the past 10 years.
- Easy to customize. Works on non-shadow password files.
- Use a preprocessor to rebuild in old format or use NIS, NIS+ ☺
- Can be distributed among systems
- Have AUTHORIZATION to RUN !!!





CIS Ruler - Linux

CIS Manual - HPUX



2.1 Create empty /etc/inetd.conf

Action:

```
cd /etc
mv inetd.conf inetd.conf.orig
touch inetd.conf
chown root:sys inetd.conf
chmod 444 inetd.conf
```

Discussion:

The stock /etc/inetd.conf file shipped with HP-UX contains many services which are rarely used and a great deal of commentary. This can make the file difficult to audit and make it easier for attackers to hide malicious services in the file. By starting with a "clean slate," we make it easier to verify that the inetd.conf file is in a known good configuration. Note that we save a backup copy of the original version of the file in case we need to refer back to it later.

2.2 Enable telnet, if necessary

Question:

Is there a mission-critical reason that requires users to access this system via telnet, rather than the more secure SSH protocol?

If the answer to this question is yes, proceed with the actions below.

Action:

```
echo "telnet stream tcp nowait root /usr/lbin/telnetd
telnetd -b /etc/issue" >>inetd.conf
```

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!

HP WORLD 2002 Conference & Expo

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, 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