Linux Authentication and Security

Jamie Becker

Wylie Swanson

Linux Security Architects

HP Services

Consulting & Integration

Technology Leadership Group

HP WORLD 2003

Solutions and Technology Conference & Expo

Agenda

- Introduction & Audience Survey
- Overview (Jamie)
  - Authentication
  - Service Hardening
  - Cracking
  - Detecting Intrusion
- Indepth Tutorials:
  - Messaging Security (Wylie)
  - Dynamic NetFilter Firewalls (Wylie)
  - User Mode Linux (Jamie)
- Final Q & A (Opportunity for questions after each tutorial as well.)

"Gartner recommends that enterprises hit by both Code Red and Nimda immediately investigate alternatives to IIS, including moving Web applications to Web server software from other vendors, such as iPlanet and Apache.."

John Pescatore

The Gartner Group

Introductions

Jamieson Becker

Technology Leadership Group, HP Services

Jamieson.Becker@HP.com

Houston, TX

+1 936-648-5654

Wylie Swanson

Technology Leadership Group, HP Services

Wylie.Swanson@HP.com

Los Angeles, CA

+1 888 352 9266

Assumptions & Objectives

- Assumptions
  - Intermediate knowledge of Linux and/ or UNIX from a systems administrative and/ or programming/ scripting perspective
- Objectives
  - Provide a comprehensive overview of security from a Linux perspective
  - Additionally provide in-depth tutorials on several Linux security topics

Audience Survey

- Your Security Background?
  - forensics
  - authentication
  - packet filtering firewalls
  - NAT
  - proxy services
  - mail routing
  - NIDS
  - /etc/services
  - /etc/hosts.allow | /etc/hosts.deny
  - shell scripting
  - Python/PHP/Perl

Agenda – Security Overview

- Authentication Methods
- Service Hardening
- Cracking
- Detecting Intrusion
- Q & A

Authentication: / etc/ passwd

- / etc/ passwd
  - Shadow Passwords
  - MD5
  - 3DES

jamie@jamiemain:~ - Shell - Konsole <3>

Session Edit View Bookmarks Settings Help

```
root:$1$Iwv19np$6Skp2g4yZdZ9w0o5Nc/:12191:0:::::
halt:*:9797:0:::::
operator:*:9797:0:::::
shutdown:*:9797:0:::::
sync:*:9797:0:::::
bin:*:9797:0:::::
ftp:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
mail:*:9797:0:::::
postmaster:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
man:*:9797:0:::::
games:*:9797:0:::::
guest:*:9797:0:::::
nobody:*:9797:0:::::
sshd:!:12188:0:99999:7:::
radvd:!:12191:0:99999:7:::
~
~
~
~
~
~
~
~
~
~
"/etc/shadow" 21L, 503C                    20,1          All
```

New Shell

jamie@jamien

Session Edit View

```
root:x:0:0:root:/r
bin:x:1:1:bin:/bin
daemon:x:2:2:daemo
adm:x:3:4:adm:/var
lp:x:4:7:lp:/var/s
sync:x:5:0:sync:/s
shutdown:x:6:0:shu
halt:x:7:0:halt:/s
mail:x:8:12:mail:/
news:x:9:13:news:/
uucp:x:10:14:uucp:
operator:x:11:0:op
man:x:13:15:man:/u
postmaster:x:14:12
cron:x:16:16:cron:
ftp:x:21:21::/home
at:x:25:25:at:/var
squid:x:31:31:Squi
gdm:x:32:32:GDM:/v
xfs:x:33:33:X Font
games:x:35:35:game
named:x:40:40:bind
mysql:x:60:60:mysq
postgres:x:70:70::
apache:x:81:81:apa
nut:x:84:84:nut:/v
cyrus:x:85:12::/us
vpopmail:x:89:89::
alias:x:200:200::/
qmaild:x:201:200::
"/etc/passwd" 43L, 1830C                   1,1           Top
```

New Shell

Authentication: PAM

- LDAP:
  - OpenLDAP
  - Iplanet
  - Novell NDS
  - MS Active Directory
- SQL:
  - MySQL
  - Oracle
  - PostgreSQL
  - MS SQL
- SASL (Simple Authentication and Security Layer)
- Kerberos 5
- SecureID
- pam_crack

Authentication: NIS

- Network Information Service, aka Yellow Pages (YP)
- Really File Replication, not truly an authentication service
- Often used to replicated information in /etc/passwd files and non-DNS host information.
- NIS+ raised more issues than it corrects, particularly on the server side. NIS+ development on Linux has ceased, probably permanently.
- NIS has had serious security flaws in the past but is still used in some legacy parts of the datacenter. It should not be deployed in new installations.

Authentication: LDAP

- Outgrowth of the original X.500 directory specification.
- Generally an excellent option for heterogeneous authentication information (eg. user accounts)
- Directory Services: a hierarchical database, usually holding user account information and often other times of information.
- Can be replicated across multiple master servers
- Scalable to millions of users
- Access Control Lists (ACLs) control access to user account info
- Active Directory is a modified LDAP implementation.
- NDS is an X.500 implementation that also implements an LDAP interface.
- Common LDAP Servers: OpenLDAP, iPlanet, Active Directory, NDS

Authentication: HTTP Authentication

- HTTP Basic Authentication and Session-based authentication without TLS/ SSL are NOT secure.
- Tunneling either type of authentication through TLS or SSL encrypts the data stream.
- Digest-based authentication is basically the same as Basic Auth but hashes the password – nothing else. This can also be done using Javascript in the login form for session-based auth but it's better to use TLS for the whole connection.
- Session ID's should be UNPREDICTABLE!

Basic Authentication

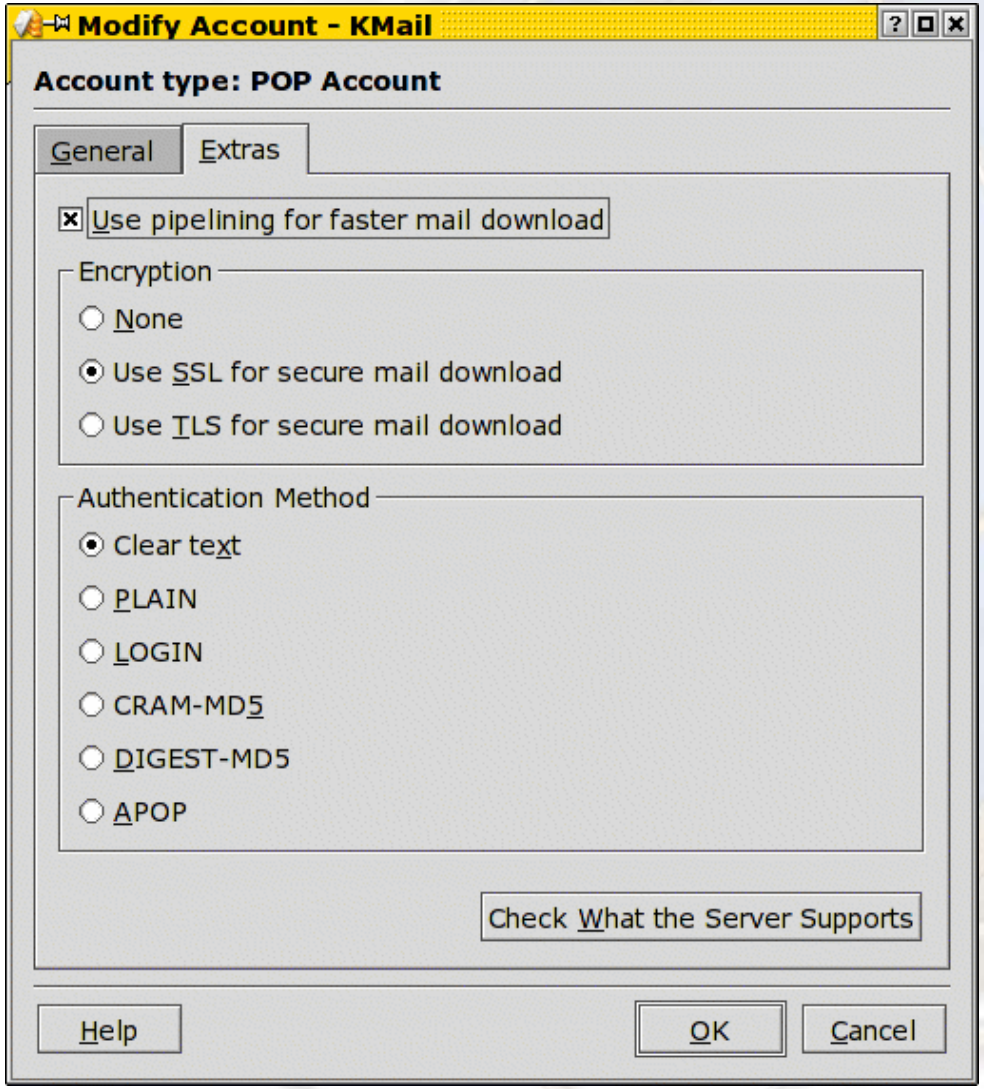
Session Authentication

Authentication: HTTP Authentication Comparison

	Basic Auth	Session Auth	Digest Auth
Manual Logout	No	Yes	No
Time-based logout	No	Yes	No
Encrypts session	TLS/SSL	TLS/SSL	TLS/SSL
Encrypts Password	TLS/SSL	TLS/SSL	Yes
Cross-platform	Yes	Yes	Partly
Session Hijackable	No	Yes	No

Authentication: Mail Authentication

- IMAP and POP3 do NOT encrypt any session data by themselves!
  - Are you sending your systems administrator password in clear text every time you check your mailbox? (Perhaps every minute??)
  - Use IMAP and POP3 over SSL/ TLS to encrypt this session!
  - Or, use DIGEST or CRAM to at least minimally hash (MD5) the password (not necessary with TLS).
- SMTP (SMTP AUTH) does not encrypt the password by itself!
  - If you're not using SMTP AUTH, you might have an open relay!
  - You must use SMTP over SSL to encrypt the password!



Authentication: Database

- ODBC
- JDBC
- Middleware
- Straight Connection

Most connection methods do not hash ANY credentials or encrypt the whole connection!!

How to fix this?

Tunnel using Stunnel

SSL/ TLS driver in the vendor's connection code

Hash passwords using the vendor's credential hashing (data still sniffable)

Service Hardening: Notorious Services and daemons – and replacements!

- Sendmail (.org)
  - Postfix
  - Qmail
  - Exim
  - Courier
  - Smail, Zmail
- BIND 4,8
  - DJBDNS
  - PowerDNS
  - BIND 9
  - MyDNS

WU-FTP
- PureFTP
- ProFTP
- SFTP, scp, WinSCP (part of OpenSSH, SSH)
- Rsync over SSH

R-Suite (rsh, rcp, etc.)
- SSH
- OpenSSH

...and many others.

Check BugTRAQ and CERT for any app you're considering.

Securing Services: SNMP

- SNMP lacks any authentication capabilities, which results in vulnerability to a variety of security threats:
  - masquerading occurrences (unauthorized entity attempting to perform management operations by assuming the identity of an authorized management entity)
  - modification of information (unauthorized entity attempting to alter a message generated by an authorized entity so that the message results in unauthorized accounting management or configuration management operations)
  - message sequence and timing modifications (unauthorized entity reorders, delays, or copies and later replays a message generated by an authorized entity.)
  - disclosure (unauthorized entity extracts values stored in managed objects, or learns of notifiable events by monitoring exchanges between managers and agents.)

  (From http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid17)
  - Brute force community guessing
  - Community string dictionary attacks
  - Many people never even change the community strings!

Service Hardening: FTP

- FTP Daemons are notorious for security flaws, but good choices include PureFTPd, ProFTPd.
- Systems Admins should NEVER use FTP or telnet from their account!
- Case 1: Elimination of FTP from your network.
- Case 2: Keep FTP but make as secure as possible.

Service Hardening: Eliminate FTP

- If you think you might be able to eliminate FTP:
  - Use SCP, Rsync over SSH, and HTTP to virtually eliminate FTP from your network.
  - SFTP (FTP tunneled over SSH) is available in both SSH and OpenSSH but free SCP clients such as WinSCP and Konqueror's fish:// ioslave might be a better alternative.

Service Hardening: Keep FTP

- If you still need FTP:
  - Replace anonymous FTP services with HTTP or HTTPS download and upload services.
  - FTP can be chrooted and/ or completely sandboxed using UML – highly recommended!
  - ProFTPd and PureFTPd both have built in chrooting for each user and can authenticate against most major auth stores like / etc/ passwd, LDAP, and various SQL servers.
  - Get on the security announcement mailing list for any FTP daemon you choose!

Service Hardening: OpenSSH

- OpenSSH is an open-source version of SSH.
- SSH and OpenSSH allow you to log in to multiple servers, but only enter a passphrase once!
- scp (part of ssh/ openssh) allow you to easily script file uploads and downloads, just like you would with rcp!
- SSH automatically securely tunnels X11 over the Internet…
  - … as well as nearly any other TCP-based protocol!
- SSH initially takes more effort to learn than FTP, but saves so much in just a few weeks!
- SSH can be used in conjunction with rsync for high-speed differential file synchronization across a WAN or LAN link!

Service Hardening: OpenSSH Session

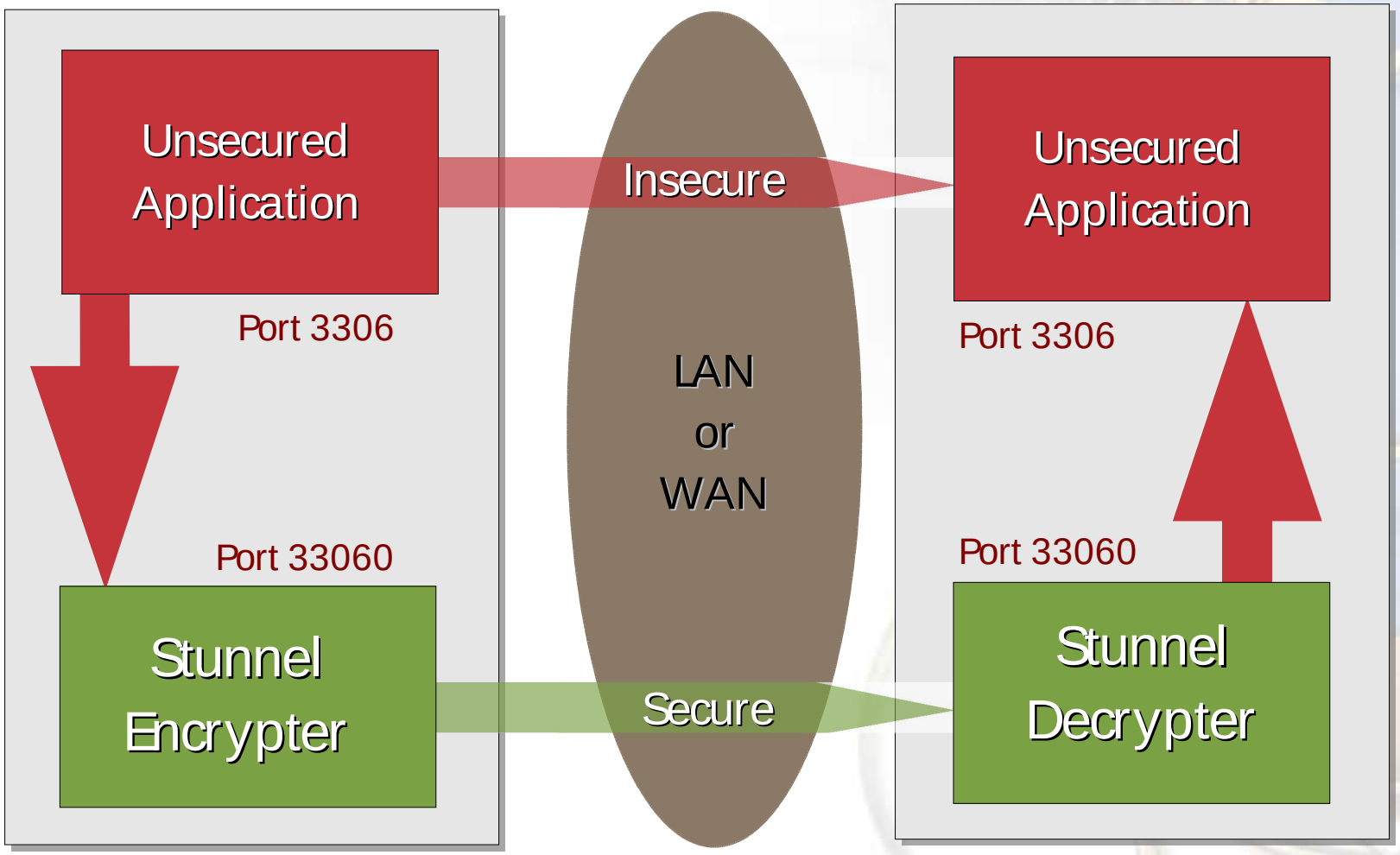
jamie@rs001:~ - Shell - Konsole <2>

Session Edit View Bookmarks Settings Help

```
http://www.gentoo.org/projects/keychain
 Copyright 2002 Gentoo Technologies, Inc.; Distributed under the GPL
 * Found existing ssh-agent at PID 1581

bash-2.05b$ touch test
bash-2.05b$ scp -q test rs001:
bash-2.05b$ ssh rs001
Linux rs001 2.4.21 #1 Tue Jul 22 07:01:19 CDT 2003 i686 unknown

Most of the programs included with the Debian GNU/Linux system are
freely redistributable; the exact distribution terms for each prog
are described in the individual files in /usr/share/doc/*/copyrigh

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Sat Aug  2 07:38:01 2003

Sat Aug  2 jamie@rs001:~
ls -al test
-rw-r--r--    1 jamie    jamie        2876 Aug  2 07:40 test

Sat Aug  2 jamie@rs001:~
```

New Shell

Server Hardening: Secure Tunnel (stunnel) Redirection



Server Hardening: Strip It!

- Core concept: **Think Minimal!** Key places to remove software:
  - rpm -qa | less to list system packages (dpkg -l | less on Debian – don't forget to check any rpm repositories on Debian and Gentoo too.) Be careful not to remove core services, such as package management commands (i.e., rpm) and Perl or Python languages.
  - Disable unneeded services /etc/inetd and /etc/xinetd.d.
  - Disable unneeded services in /etc/rc.* scripts.
  - Do you really need X11? Change default runlevel in /etc/inittab
- When building new servers, install bare minimum and then add software as needed. (This is a little easier on Debian or Gentoo.)

Server Hardening: Upgrade it!

- Core Concept: **Upgrade everything frequently**. You don't need to upgrade core facilities (such as glibc or GCC) but you should stay patched up with the latest security updates.
- Debian: make sure you have security.debian.org in your apt.sources file, cron an "apt-get update" command, and occasionally log in and run "apt-get dist-upgrade" to upgrade the system. (You can cron apt-get upgrade but it's riskier.) If you cron the upgrade, be careful to be on stable and only pull security updates to minimize package breakage.
- Gentoo: cron "emerge rsync" and occasionally run "emerge world" to update the whole system. Don't cron emerge world!!
- Red Hat: use up2date, but make sure you monitor any installs (i.e., don't use cron).
- SuSE: use YaST2 to point your sources at SuSE and download updates as needed.

Server Hardening: Eternal Vigilance!

- Vigilance will save you. Maybe.
- Cultivate paranoia.
- "Candy-coated security!" Firewalls are only a tiny piece of the whole puzzle!
- Learn the Windows SysAdmin's Mantra: "Upgrade, upgrade, upgrade."
- Length, strong passwords with alphanumerics and punctuation. The strongest password can be accidentally sent over a weak link.
- Don't export your DISPLAY variable when using SSH!

Only the Paranoid Survive.

Andy Groves
CEO, Intel Corp. (ret.)

Server Hardening: InetD Intro

- InetD is a "super-server."
  - Just one daemon to answer for multiple daemons on multiple ports.
  - Reduces memory and processor utilization for seldom used processes.
  - Should only be used for less used services (such as telnet or FTP) since an instance of telnet or FTP must be forked for each incoming connection.
- By itself, InetD doesn't do any checking at all, which brings us to…

Server Hardening: TCP Wrappers

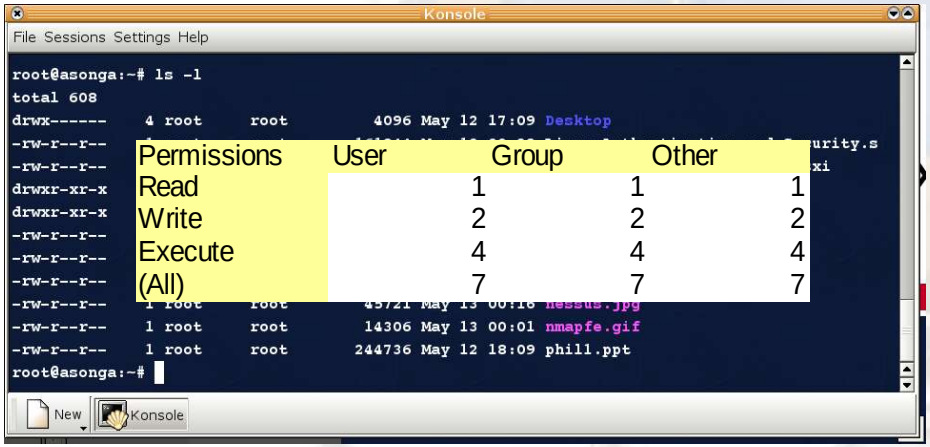
- TCP Wrappers allows "wrapping" the forked process that InetD kicks off with another program that checks the incoming connection's hostname or IP.
- TCP Wrappers was written by Wietse Venema, the author of the secure Postfix MTA.
- TCP Wrapper's checks are based ONLY on IP or hostname.

Service Hardening: XinetD

- Can be compiled with builtin libwrap (TCP Wrappers) support. Use hosts.{allow|deny}! More efficient than using tcpd!
- TCP Wrappers can't rate-limit connections. XinetD can restrict and limit based on:
  - access time of day
  - rate of incoming connections (minimize DoS attacks)
  - number of incoming connections from specific hosts
  - total number of connections for a service.
  - number of simultaneous connections from a host
- Bind only to specific IP's. Useful for internal services in a DMZ.
- Redirection. Allows you to redirect a TCP stream to another host, which can be NAT'd or on an internal machine.
- Extensive Logging features and IPV6 support.

Server Hardening: Kernel Hardening

- POSIX Capabilities
- GRSecurity
- LIDS
- Linux Security Modules (LSM)
- NSA SE-Linux
- ACLs (for files) (support Ext2, Ext3, ReiserFS, XFS, JFS)
  - Samba



Permissions	User	Group	Other
Read	1	1	1
Write	2	2	2
Execute	4	4	4
(All)	7	7	7

Service Hardening: Bastille Linux

- Hardening Script
- Supports:
  - Red Hat
  - Mandrake
  - SuSE
  - Turbo
  - Debian
  - HP-UX
  - Mac OS X
- Focus on knowledge transfer
- Covers most major areas of lock down for a single host.

Service Hardening: Sandboxing

- Change Rooting:
  - chroot
  - Wietse Venema's chrootuid
- Virtualization:
  - VMWare GSX and ESX virtualization
  - Bochs, Plex86
  - * User Mode Linux

Service Hardening: Firewalls

- Each machine can (and should) run its own netfilter firewall.
- LPR, single disk routers & firewalls
- IPFWAdm
- IPChains
- IPTables (aka Netfilter)
- Passive Firewalls
- Active Firewalls
- Packet Filter Firewalls vs. Proxy Services
- SOCKS

Service Hardening: DMZ

- Move core services that might normally be exposed to the Internet into a DMZ (De-Militarized Zone)
- DMZ's are essentially another zone added to a firewall that filters communication both between the external network and the DMZ hosts as well as between the *internal* network and the DMZ hosts.
- Even if hosts in the DMZ are cracked, the internal machines should not be exposed to risk.
- Internal machines should always initiate communications (push, pull) to the DMZ machines, not the other way around.
- Core services for DMZ are Mail, Web Proxy, and Virtual Private Networks (VPNs).
- VPNs should be heavily protected and isolated.

Service Hardening: Mail in a DMZ

- Architecture:
  - SMTP Mail flows into a network through a relay
  - SMTP Mail flows out of the network through a relay.
  - Internally and externally, port 25 traffic is sent to the mail relay.
  - Perdition* as an external POP3/ IMAP proxy server – filters traffic on 143 or 110, or preferably restricts to 993 or 995. Combine with XinetD for best results.
- More Advantages:
  - Protect MS Exchange
  - Content Filtering
  - Virus Scanning
- Webmail

Service Hardening: Proxy in a DMZ

- Typical:
  - All internal web traffic goes through the proxy
  - All incoming web traffic hits the web server in the DMZ
- Proxy servers include Apache and Squid
- Squid can reverse proxy
- Load Balancing:
  - Round Robin
  - LVS (Piranha)

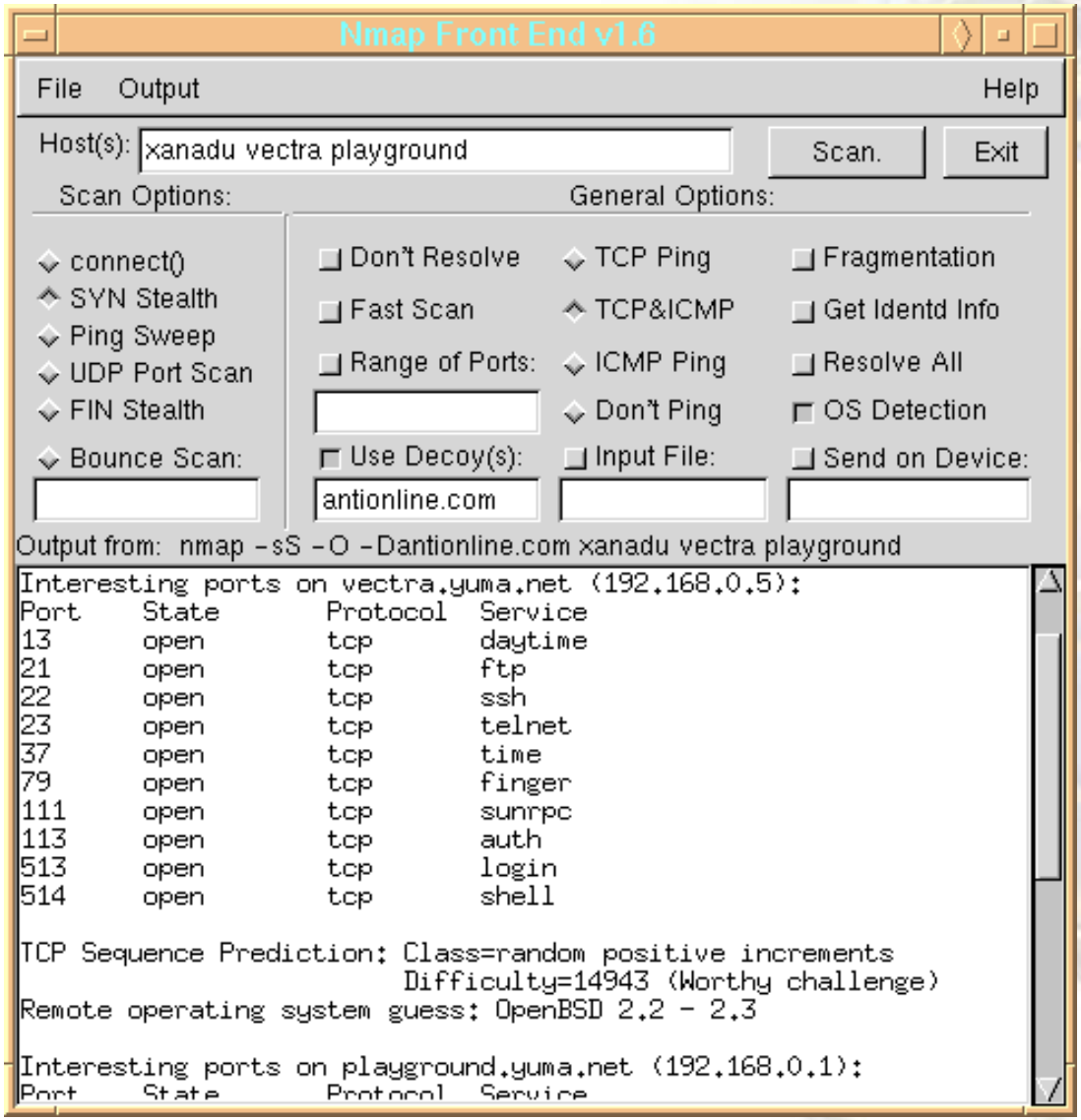
Server Hardening: VPNs

- IPSec (FreeSWAN)
  - Free built-in L2TP client in Windows 2000, XP, combine with IPSec Tool
- SSH (OpenSSH)
- CIPE
- VTUN
- PPTP (PoPToP, pptpclient)
  - Weak protocol
  - Free built-in clients in Windows 98, ME, 2000, XP

Cracking

- "Hacking" vs. "Cracking"
  - White Hat
  - Grey Hat
  - Black Hat
- Conferences
  - HOPE (2600.com)
  - DEFCON
  - Black Hat Briefings
- Honeypots

Cracking: Port Scanning



Cracking: Packet Sniffing

- tcpdump
- Ethereal
- Ifstatus

The Ethereal Network Analyzer

File Edit Capture Display Tools Help

No.	Len	Time	Source	Destination	Protocol	Info
1	77	0.000000	24.94.186.99	pow.zing.org	DNS (UDP)	Standard query
2	77	0.010000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
3	164	0.060000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
4	70	0.070000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
5	71	0.080000	pow.zing.org	f.root-servers.net	DNS (UDP)	Standard query
6	161	0.120000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
7	158	0.130000	f.root-servers.net	pow.zing.org	DNS (UDP)	Standard query response
8	77	9.990904	24.94.186.99	pow.zing.org	DNS (UDP)	Standard query
9	77	9.990904	pow.zing.org	i.got.net	DNS (UDP)	Standard query
10	148	10.090904	i.got.net	pow.zing.org	DNS (UDP)	Standard query response
11	148	10.090904	pow.zing.org	24.94.186.99	DNS (UDP)	Standard query response

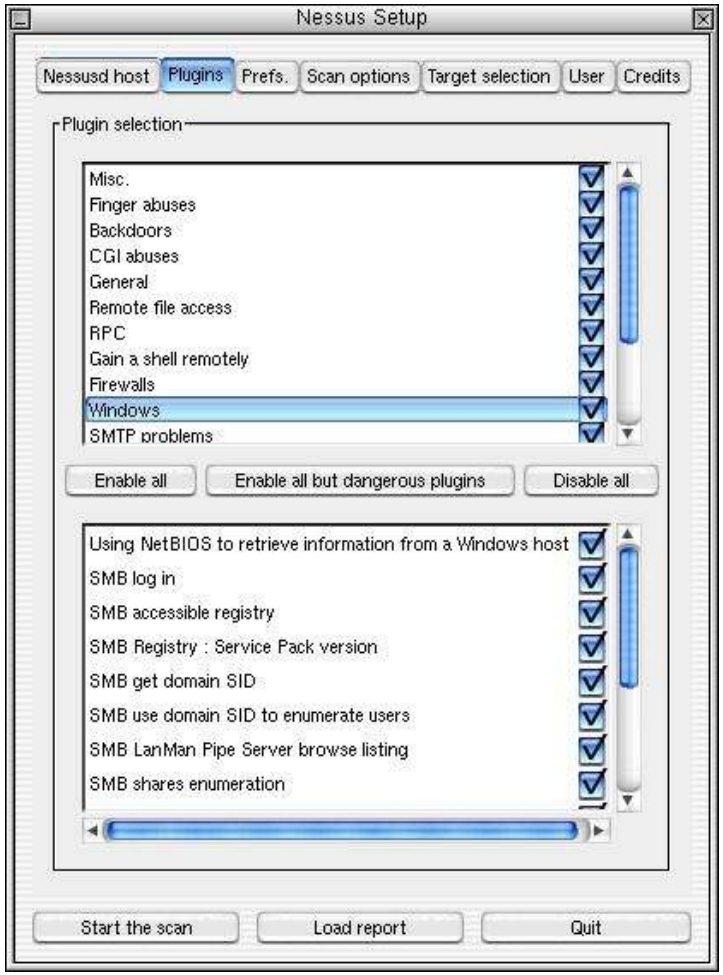
```
⊞ Frame (77 on wire, 77 captured)
⊞ Ethernet II
⊞ Internet Protocol
⊞ User Datagram Protocol
⊟ DNS query
  ├ Transaction ID: 0x83c8
  ⊞ Flags: 0x0000 (Standard query)
  ├ Questions: 1
  ├ Answer RRs: 0
  ├ Authority RRs: 0
  ├ Additional RRs: 0
  ⊟ Queries
    ⊟ www.brunching.com: type A, class inet
      ├ Name: www.brunching.com
      ├ Type: Host address
      └ Class: inet
```

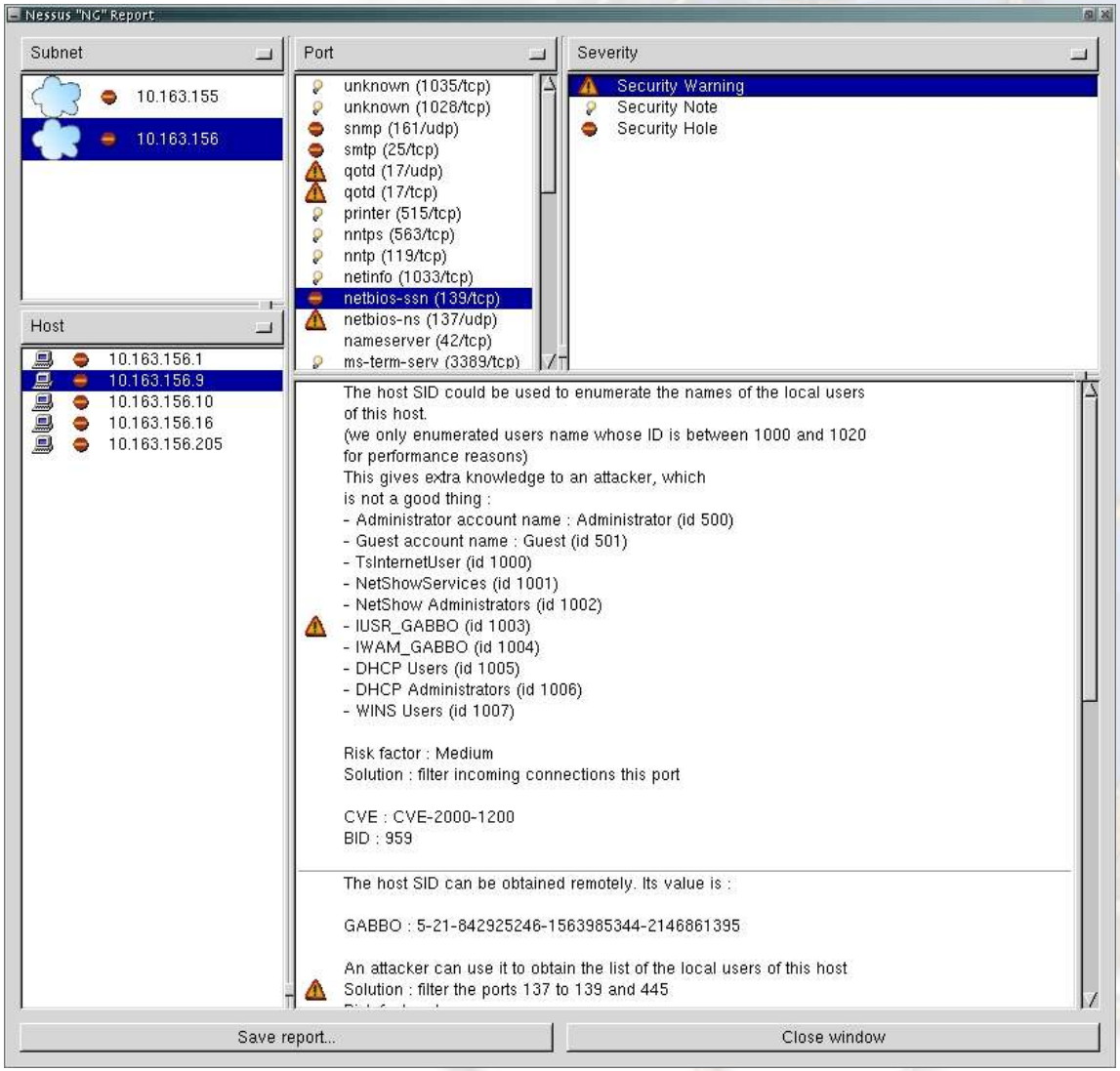
```
0000  00 50 73 2c 44 c1 08 00  20 2b 01 05 08 00 45 00   .Ps,D... .+....E.
0010  00 3f 4b e7 00 00 40 11  84 ac ce 39 24 5a cf 6f   .?K...@. ...9$Z.o
0020  e8 17 07 f4 00 35 00 2b  18 c0 83 c8 00 00 00 01   .....5.+ ........
0030  00 00 00 00 00 00 03 77  77 77 09 62 72 75 6e 63   .......w ww.brunc
0040  68 69 6e 67 03 63 6f 6d  00 00 01 00 01            hing.com .....
```

Filter: File: dns.pcap Drops: 0

Cracking: Vulnerability Testing

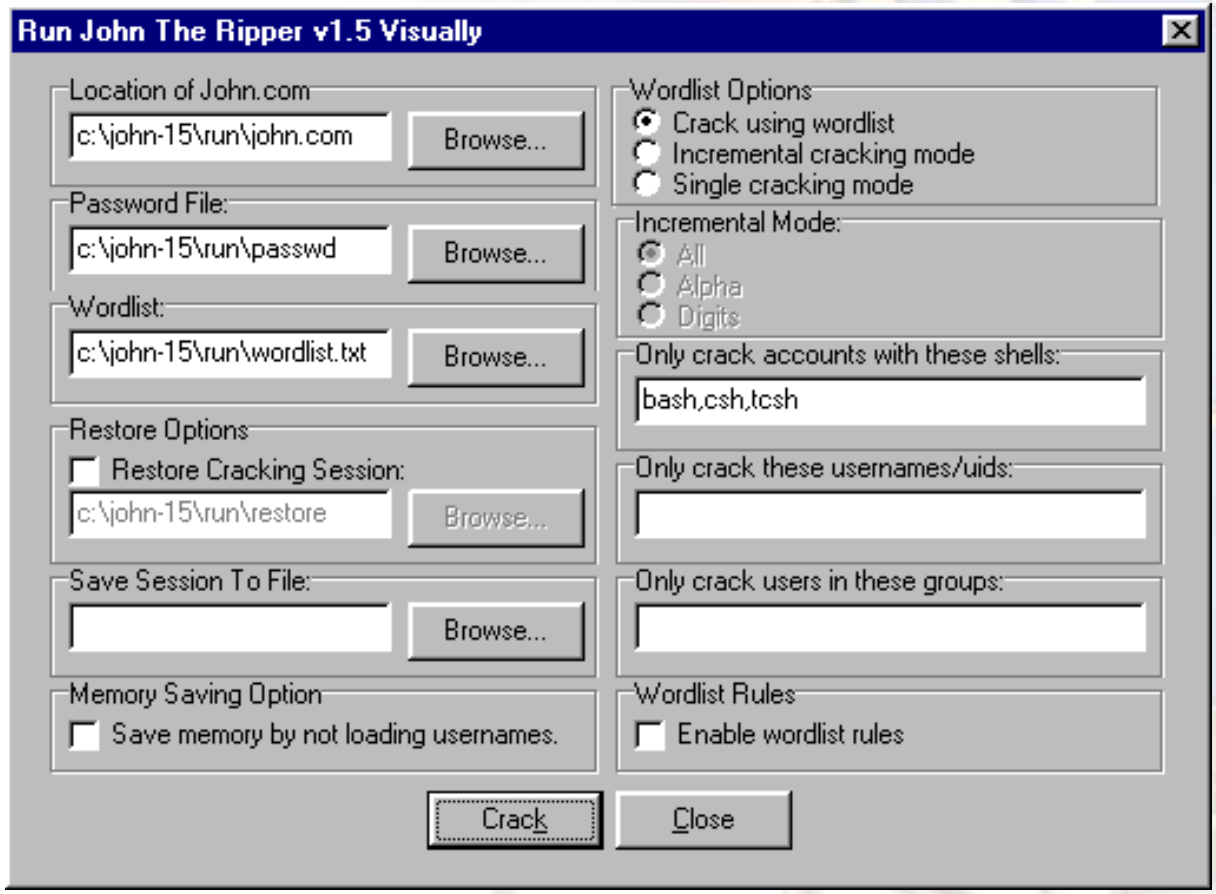
- Nessus





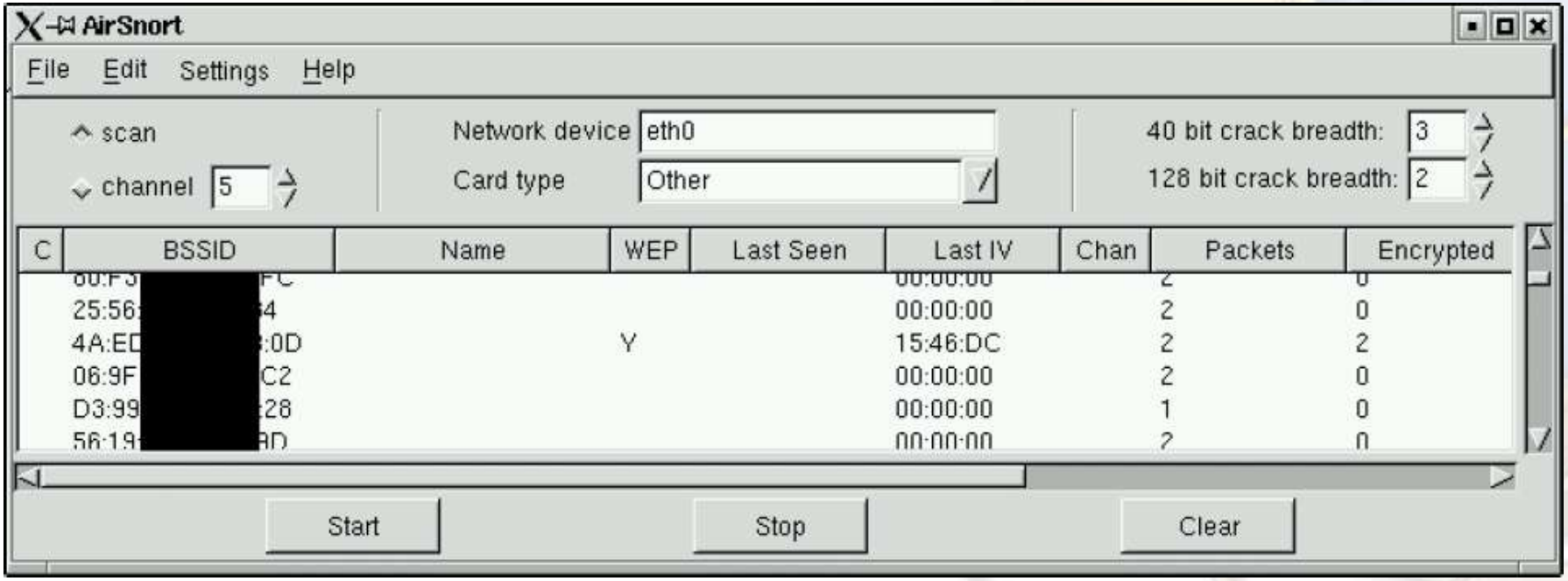
Cracking: Passwords

- Crack
- John the Ripper
- pam_crack
- pam_pwcheck
- Distributed John



Cracking: Wireless "Security"

- WEP: This is a joke, right?
  - Airsnort
  - Wepattack
  - Kismet Wireless



Detecting Intrusion: SysLogd

- Remote syslogd (loghost)
  - Remote Syslog Loghost is inherently INSECURE: Clear text over UDP!
  - Use CIPE, VTUN, or even IPSec to encrypt your syslog messages. REMEMBER! Don't assume your LAN is secure!
- Alternative system loggers:
  - * metalog – caching, remote logging, regex, external scripts
  - msyslog – integrity checking, log to MySQL, PostgreSQL
  - syslog-ng – clean log forwarding, TCP rather than UDP

Detecting Intrusion: Viruses & Trojans

- There are less than five known "viruses" for Linux, and no known virus vulnerabilities in any recent version of commercial-grade Linux.
- Protect Windows with these Linux anti-virus tools:
  - Sophos
  - Trend Micro
  - RAV Antivirus
  - Avast
  - Symantec
  - Central Command
  - Bit Defender
  - Kaspersky

Detecting Intrusion: Intrusion Detection Systems

- Intrusion Detection Systems:
  - Knowledge-based, "Expert Systems", uses database of common attacks
  - Behavioral, "Pattern and anomaly checking", tracks against a baseline of normal behavior.
- A *Host-based IDS* (HIDS) works inside an individual host and normally tracks misuse (internal) and intrusion (external). Syslog tracking is a big part of this, as is file-integrity checking (covered later).
  - Well-known HIDS: **SWATCH, *LIDS.**
- A *Network IDS* (NIDS) works by looking for known or unknown patterns as they travel the network.
  - Well-known NIDS: ***Snort, *Nessus** (covered later)

Detecting Intrusion: File Integrity Checkers

- What are they? File Integrity Checkers monitor crucial system files for changes, which could signal that your machine has been cracked. ("hacked")
- Tripwire
- * Prelude
- AIDE
- Osiris
- Samhain
- As with all security software, use caution; some can introduce the very vulnerabilities they're designed to avoid. It's often best to use security software included with your distribution.
- RPM can act as a simple file integrity checker using the -Va switch.

Detecting Intrusion: Root Kit Checkers

- Chkrootkit*
  - scans for rootkits *after* you think you've been rooted
  - built-in promiscuity tester, pattern search for many rk's.
- Rkdet
  - proactively scans for rootkits on the fly, as they're being installed.
  - similar to file-checking IDS's, except that it specifically watches for changes to core system files such as ps and netstat.
  - probably install this *before* you're rooted. ;-)
- ifstatus

Other Topics

- Public Key Infrastructure (PKI) tools:
  - PHPki (PHP)
  - IDX-PKI (Perl + PHP)
  - PKIT (PKI Tools) (Java)
- Biometrics
  - Identix (hand, fingerprint)
  - Signplus (signature)
  - Secugen (fingerprint)
  - BioAPI.org
- Physical Security
  - X10

Additional Information

- www.Google.com
- www.SecurityFocus.com
- www.CERT.org
- www.FreshMeat.net
- www.SourceForge.net
- www.SlashDot.Org
- www.LinuxSecurity.com

- www.HP.com/ hps/ linux/
- www.HP.com/ hps/ security/

- Contact Info:
  - www.JamieBecker.com
  - Jamie@JamieBecker.com
  - Jamieson.Becker@HP.cor

HP WORLD 2003

Solutions and Technology Conference & Expo

Interex, Encompass and HP bring you a powerful new HP World.

interex

shared knowledge • shared power

encompass

AN HP USER GROUP

hp

invent