



A10

Basic AIX Security

Jaqui Lynch

**IBM System p,
AIX and Linux
TECHNICAL UNIVERSITY**
01-05 Oct 2007
San Antonio, TX



© IBM Corporation 2007

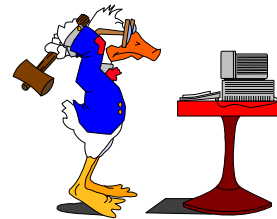
AIX Basic Security

Jaqui Lynch

Mainline Information Systems

Email – jaqui.lynch@mainline.com

<http://www.circle4.com/papers/a10security.pdf>



Mainline: solutions you need
from people you trust

Agenda

- Basics
 - Security Types
 - Permissions
- Freeware/Shareware Tools that can help
 - TCP Wrappers & Secure Shell
 - OpenSSL
 - stunnel
 - OpenSSH
 - Snort
 - Ftp
- Logging, finding Rootkits
- Scanners and Tools
- Questions

Mainline: solutions you need
from people you trust

Security Types

- Physical
- Local
 - Keep system patched!!!
 - Microcode/firmware
 - BIOS on HMC and consoles
 - Operating Systems
- Files and filesystems
- Passwords
- Kernel
- Network



Copyright 2000, The Halifax Herald Limited

Mainline: solutions you need
from people you trust

Levels & Types of Attacks

- Levels
 - Root access break-in
 - Replacement of materials
 - Damage done
 - Just looking
 - Theft of proprietary information
 - Denial of service
 - Worms and Trojans
- Types
 - Embarrassment (replace banners, home page, etc)
 - Denial of service (syn-flood connections)
 - Ping of Death
 - Stealing proprietary code
 - Pornography
 - Harassment or threats - stalking
 - Email Spam or bulk subscribes
 - Hate mail
 - Buffer Overflow

Mainline: solutions you need from people you trust

SANS Top 20

<http://www.sans.org/top20/#threatindex>

- Top Vulnerabilities in Operating Systems
 - W1. Internet Explorer
 - W2. Windows Libraries
 - W3. Microsoft Office and Outlook Express
 - W4. Windows Services
 - W5. Windows Configuration Weaknesses
 - M1. Mac OS X
 - U1. UNIX Configuration Weaknesses
- Top Vulnerabilities in Cross-Platform Applications
 - C1. Web Applications
 - C2. Database Software
 - C3. P2P File Sharing Applications
 - C4. Instant Messaging
 - C5. Media Players
 - C6. DNS Servers
 - C7. Backup Software
 - C8. Security, Enterprise and Directory Management Servers
- Top Vulnerabilities in Networking Products
 - N1. VoIP Servers and Phones
 - N2. Network and Other devices Common Configuration Weaknesses

V7.0 November 15, 2006

Mainline: solutions you need from people you trust

AIX Security Advisories

- <https://www14.software.ibm.com/webapp/set2/subscriptions/ijhifoe?mode=2>
 - Go to the above link to subscribe

VULNERABILITY SUMMARY VULNERABILITY:

BIND remote DNS cache poisoning

PLATFORMS: AIX 5.2, 5.3

SOLUTION: Apply the APAR, interim fix or workaround as described below.

THREAT: DNS cache may be poisoned due to weak DNS query IDs.

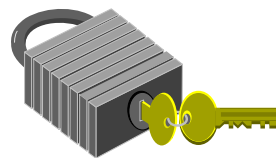
CERT VU Number: CVE-2007-2926 CVE Number: 252735

- <http://www.kb.cert.org/vuls/>
 - CERT vulnerability database
 - Allows you to search vulnerabilities

Mainline: solutions you need
from people you trust

UNIX Security Basics

- Permissions
- UID
- GID
- Dangerous Accounts
- Superuser
- SUID
- Sticky bit
- Umask
- Backups



Mainline: solutions you need
from people you trust

Security Pre AIX v6

- Auditing
 - Audit framework
 - AIX Security Expert (v5.3 tl05)
- Authorization
 - DAC (discretionary access control)
 - Local passwords, LDAP integration, Kerberos and longer passphrases
- Access Control
 - Loadable authorization modules, PAM, File Permission Manager, ACLs (access control lists) and limited RBAC (role based access control)
- Encryption
 - Crypto cards have been available for some time
 - In v5.3 introduction of CLiC (Crypto library in C) support
 - Ability to perform tape encryption
- Integrity checking
 - Trusted Computing Base
 - Stack execution disable (v5.3 tl04) – designed to prevent buffer overflows
- Network Security
 - IP security, OpenSSH, IP v6, TCP Wrappers, IP filters, Secure TCP and AIX Security Expert
- System Hardening
 - CAPP – controlled access protection profile
 - AIX Security Expert
 - File Protection Manager (v5.3 tl06)

Mainline: solutions you need
from people you trust

New in AIX v6 1/2

- See redbook at
 - [http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg247430.html?](http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg247430.html?Open)
Open
- Cobit SOX level added to AIX Security Expert
- Enhanced RBAC added to Access Control.
 - This is required for WPARs (workload partitions)
 - Now the default at install time
 - Replaces many functions of SUDO
- CLiC enhanced to include PCKS11 and is a prerequisite for the new encrypted filesystem
- Encrypted filesystem (EFS)
 - Automatically encrypts and decrypts files
 - Key based
- Trusted execution added for integrity checking.
 - Uses a TSD (trusted signature database)
 - New trustchk command
- Trusted AIX
 - Removes concept of root
 - Uses MAC (mandatory access controls_ and requires auditing

Mainline: solutions you need
from people you trust

New in AIX v6 2/2

- Secure by default
 - Install time option
 - Installs a minimum set of filesets (about 100)
 - You add what you need later
- File Permission Manager
 - Intent is to reduce setuid bit programs
 - New fpm command
 - Multiple levels
- Encrypted File System
 - Depends on CLIC
 - Option on a JFS2 filesystem
 - Encrypts and decrypts on a per file basis
 - New "ls -aU" shows an e if encrypted (rwxr-xr-xe)
 - Uses keys
 - If user has the keys in their keystore then this is transparent to them
 - efsmgr and efskeymgr commands
 - Must be explicitly enabled using "efsenable -a)
- Secure FTP
 - Encrypts both the data and command channels
 - Built on OpenSSL
 - Useful where clients do not have SSH

Mainline: solutions you need
from people you trust

File Security

- ls -l shows:
- -rwxr-xr-x 1 jaqui jgroup 4320 Feb 9 12:19 files
- - file's type (- for file, D for directory)
- rwxr-xr-x file's permissions
 - if rwxr-xr-xe then file is encrypted
- 1 no. of hard links the file has
- jaqui name of the files owner (if a number then this is the Uid)
- jgroup name of the group (if a number then this is the Gid)
- 4320 size of file in bytes
- Feb 9 12:19 file's modification time
- files the file's name

- ls -l shows modification time for file
- ls -lu shows last accessed time
- The above two times can be changed with a command so you should check:
- ls -lc inode last change time

Mainline: solutions you need
from people you trust

Permissions

- r read
 - w write
 - x execute
 - s SUID or SGID
 - t sticky bit
 - e Encrypted
-
- aaa bbb ccc
 - aaa file's owner permissions
 - bbb users who are in the file's group
 - ccc everyone else on the system (except uid 0)
 - Permissions apply to devices, named sockets, files, directories and FIFOs.



Mainline: solutions you need from people you trust

Octal Permissions

- 4000 SUID on execution
- 2000 SGID on execution
- 1000 Sticky Bit
- 0400 Read by owner
- 0200 Write by owner
- 0100 Execute by owner
- 0040 Read by group
- 0020 Write by group
- 0010 Execute by group
- 0004 Read by other
- 0002 Write by other
- 0001 Execute by other
- 755 Anyone can copy or run the program - Only the owner can change it

Mainline: solutions you need from people you trust

Umask

- Specifies the permissions you do not want given by default to newly created files and directories.
- By default on most systems:
 - New files are 666 (anyone can read/write)
 - New programs are 777 (all rwx)
- root should be 022 and all others 077

- **Common Umask Values**

Umask	User	Group	Other
• 0000	rwx	rwx	rwx
• 0002	rwx	rwx	r-x
• 0007	rwx	rwx	---
• 0022	rwx	r-x	r-x
• 0037	rwx	r-x	---
• 0077	rwx	---	---

Mainline: solutions you need from people you trust

SUID, SGID, Sticky Bit

- SUID Sets UID to program's owner at execution
- SGID Sets GID to program's group at execution
 - Also used to share files in a directory
 - All files and subdirectories will inherit the group
- Sticky
 - If set on a dir then only root or owner can delete or rename (see /tmp drwxrwxrwt)
 - Old usage was: Causes program to be left in swap space after termination. Used for programs that were executed frequently - outmoded.
- The su command is an SUID program.
- To find them:
 - find / -perm -004000 -o -perm -002000 \) -type f -print
 - or ncheck -s filesystem-name

Mainline: solutions you need from people you trust

Files to Clean Out

- Backup file first – I use filename-JLdate
- /etc/services
- Password and group files
 - Know who is in there and why
- /etc/inetd.conf
 - Delete services – don't just comment them out
 - Check whenever you install maintenance
- /etc/inittab
- /etc/rc.tcpip
 - Do you need sendmail, ATM, SNMP?
- /etc/rc.local and other rc files
 - Don't make changes to inittab to add things
 - Instead kick off an rc.local from inittab and make your changes to rc.local

Mainline: solutions you need
from people you trust

Checklist 1/3



Individual accounts only including for applications
All accounts must have GOOD passwords
Disable tftp if possible
Remove .rhost and core files nightly
Ensure /etc/passwd can't be read anonymously by UUCP or TFTP
Check the SU log regularly
Only allow root to login at the console (force su or sudo) if at all
Set console as only trusted location for root
Set umask to 033 or 077 (077 = rwx --- ---)
Scan regularly for SUID/SGID files & for crack
Change default password on all system default accounts
Get rid of guest
Disable dormant or temporarily inactive accounts
Make regular backups & check restores regularly
Export filesystems that have programs as read-only
Check last login when you login

Mainline: solutions you need
from people you trust

Checklist 2/3

System directories - not world or group writable
/etc/hosts.equiv and hosts.lpd should be rwx r-- r--
Remove the + and all comments from your /etc/hosts.equiv and lpd files
Disable finger and who and w
Make sure fingerd is recent and disabled
Ensure sendmail or Postfix is at latest version
Do not run sendmail unless you are a mailserver or relay
Make sure ftpd is current and disabled (try secure FTP or SFTP in SSH)
Ensure anonymous FTP & tftp can't get the /etc/passwd file
Make sure /etc/ftpusers contains root, uucp, bin, etc
Scan periodically for hidden directories ("..")
Check /etc/passwd for users with uid 0 regularly
Ensure /etc/passwd is rwx r-- r--
Make sure only root can run last and lastcomm
Turn on password aging and strong but sensible passwords
Set TMOU in /etc/profile to logout if no activity

Mainline: solutions you need
from people you trust

Checklist 3/3

User account directories should be rwx - unless there is a group sharing need
Set up system logging (by default you have pretty much nothing)
Back logs up tpo a central server for searching, etc
Set up accounting (and auditing if needed)
Disable ntalk, rlogin in /etc/inetd.conf and /etc/services
Document your install and all changes
Create a recovery list and a list of valid uids/gids
For tftp - create a /etc/tftpaccess.ctl file
Ensure only root has write access to system binaries
Ensure shadow password file is not readable to anyone but root
Ensure accounting files are not writable
No binaries on NFS filesystems
Set nodev, nosuid & noexec on NFS exported f/s
Never export a filesystem to the world
NFS export files to fully qualified names or IPs
Keep system properly patched
Set up NTP or a similar time protocol to keep time

Mainline: solutions you need
from people you trust

Login banners

- /etc/motd
 - Sample on next slide
- Change the herald for the system
 - /etc/security/login.cfg

default:

```
sak_enabled = false
logintimes =
logindisable = 0
logininterval = 0
loginreenable = 0
logindelay = 0
```

```
herald = "Unauthorized use of this system is prohibited \n\n\r Login: "
```

Mainline: solutions you need
from people you trust

Sample /etc/motd

Use of this computer/workstation and of the XXXX network is authorized solely for purposes consistent with XXXX's policies and procedures.

Unauthorized access to credit data is prohibited by law and any unauthorized access to information located on this computer and/or any XXXX network may result in disciplinary action and/or criminal prosecution.

Authorized users who suspect that their computer and/or XXXX-provided network accounts have been accessed without their permission are expected to immediately change their passwords and report such incident to the XXXX Computer access security department.

Mainline: solutions you need
from people you trust

Third Party Tools

- SUDO 1.6.9p4 (Aug 16, 07)
 - <http://www.gratisoft.us/sudo/>
- TCP Wrappers 7.6-ipv6-4
 - Provides logging for attempts at network services
 - ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6-ipv6.4.tar.gz
- OpenSSH 4.6p1 (Mar 9, 07)
 - <http://www.openssh.org/>
- Snort 2.7.0.1 (Aug 6, 07)
 - <http://www.snort.org/dl/>
- Openssl 0.9.8e
 - <http://www.openssl.org>
- Stunnel 4.20
 - <http://www.stunnel.org/>
- LSOF
 - <http://people.freebsd.org/~abe/>
- Logging
 - Swatch, logsurfer

Mainline: solutions you need
from people you trust

TCP Wrappers and SSH

- TcpW - <ftp.porcupine.org>
- SSH – <http://www.openssh.org>
- Wrappers improve security and logging
- Reverse dns lookup can be used to disallow access
- Allows tripwires
- SSH encrypts logins
- SCP allows secure file copies
- SFTP replaces FTP
- First install the wrappers – there is a new version that can now handle IPv6
- Then install OpenSSL and SSH and configure ssh with the wrappers – do not install or enable support for v1 of ssh

Mainline: solutions you need
from people you trust

TCP Wrappers Configuration

- vi Makefile
 - STYLE = -DPROCESS_OPTIONS # Enable language extensions.
 - FACILITY= LOG_DAEMON # LOG_MAIL is what most sendmail daemons use
 - SEVERITY= LOG_INFO
 - Causes tcpd to log everything to daemon.info
 - # Paranoid mode implies hostname lookup (normally a double lookup).
PARANOID= -DPARANOID
- make clean
- make aix
- cp tcpd /usr/local/bin
- cp tcpd.h to ssh source directories
- cp libwrap.a /usr/local/lib
- vi inetd.conf, hosts.allow, hosts,deny
- refresh –s inetd

Mainline: solutions you need from people you trust

OpenSSL

- OpenSSL
 - www.openssl.org
 - OpenSSL 0.9.8d fixes known security holes
 - Latest is 0.9.8e – have had some problems getting it to compile with GCC
 - Provide SSL v2 and v3 implementations
 - Provide TLS (transport layer security)
 - If using GCC to compile:
 - Ensure enough space in /usr/local (I make it a filesystem)
 - ./Configure aix-gcc --prefix=/usr/local --openssldir=/usr/local/openssl
 - make
 - make test
 - make install

Mainline: solutions you need from people you trust

OpenSSH

- OpenSSH
 - www.openssh.org
 - If using GCC to compile:
 - Ensure enough space in /usr/local (I make it a filesystem)
 - Install OpenSSL first
 - It may require that you have a /var/empty directory
 - `./configure aix-gcc --with-tcp-wrappers --with-ssl-dir=/usr/local/openssl`
 - `make`
 - `make test`
 - `make install`
 - Start /usr/local/sbin/sshd
 - After testing access set up sshd to start at boot from /etc/rc.local
 - Free SSH Clients at:
 - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Mainline: solutions you need
from people you trust

/etc/inetd.conf wrapped

```
ftp  stream tcp6  nowait root  /usr/local/bin/tcpd /usr/sbin/ftpd -u 002 -l  ftpd
telnet stream tcp6  nowait root  /usr/local/bin/tcpd /usr/sbin/telnetd  telnetd -a
exec  stream tcp6  nowait root  /usr/local/bin/tcpd /usr/sbin/rexecd  rexecd
dtspc stream tcp  nowait root  /usr/local/bin/tcpd /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
```

Below: Wrap service but ensure it will never work
/bin/false must be added to valid shells in /etc/security/login.cfg

```
rlogin stream tcp6  nowait root  /usr/local/bin/tcpd /bin/false
netstat stream tcp  nowait nobody /usr/local/bin/tcpd /bin/false
```

Delete everything else out of inetd.conf – don't just comment it out.
You should also check inetd.conf regularly

Some things do not play well
NIM – do not wrap bootp or tftpd

Mainline: solutions you need
from people you trust

/etc/hosts.deny

1. ALL:ALL

Or:

2. ALL:ALL spawn (echo -e "\n Tcp Wrappers \: Refused \n \

By: \$(uname -n) \n Process: %d (pid %p) \n \

Host: %c \n Date: \$(date) \n \

" | mail -s tcpw@\$(uname -n). %u@%h ->%d. admin@sys.com)

I use method 1.

Do not get fancy here – deny it all and explicitly enable in hosts.allow

Mainline: solutions you need
from people you trust

/etc/hosts.allow Options

- Telnetd: 123.123.123.4 : options
- Options are:
 - RFC931
 - Does an ident lookup to the originator
 - I don't use this as I have no idea what the person is really running on that port on their system
 - BANNERS path/filename
 - Displays a banner whether service is granted or not
 - I use this all the time – think of it as MOTD for SSH
 - SPAWN (commands)
 - Used to execute a command such as safe_finger and then mailing the response to a security person
 - Only used for denied connections
 - I don't use safe_finger as I have no idea what the person is really running on that port on their system

Mainline: solutions you need
from people you trust

/etc/hosts.allow

Log but don't really protect

```
ftpd : all
sshd : all
rshd : all
krshd : all
tftpd : all
bootpd : all
rlogind: all
krlogind: all
telnetd : all
dtspcd : all
```

Mainline: solutions you need
from people you trust

/etc/hosts.allow

Log and protect

```
Portmap      : 192.168.1. 192.168.5.3
vsftpd       : LOCAL, 192.168.1.
in.ftpd, ftpd : .abc.com,192.168.1.4
sshd         : all
dtspcd       : 192.168.1.0/255.255.255.0
xmsservd     : .abc.com,123.123.123.4
rexecd       : LOCAL,.abc.com,123.123.123.4
rexecd, telnetd : LOCAL, 192.168.1.
smtpd        : LOCAL, 192.168.1.
sendmail     : LOCAL, 192.168.1. EXCEPT 192.168.1.4
```

Mainline: solutions you need
from people you trust

Snort

- www.snort.org
- Latest version is v2.7.0.1 (Aug07)
- Intrusion detection tool
- Can be used as a packet sniffer like tcpdump
- Can be used as a packet logger for debugging
- Basically a network sniffer with flexible language allowing you to write rules
- Requires libpcap from www.tcpdump.org
- Get management permission from security department

Mainline: solutions you need
from people you trust

Stunnel

- www.stunnel.org
- Latest version is 4.2.0
- Wrapper utility for encrypting TCP sessions via SSL
- Needs OpenSSL
- Can secure daemons
 - Imap, pop, ldap
 - With no changes to the daemons
- Built-in TCP wrappers support (compile)
- Can use hosts.allow format

Mainline: solutions you need
from people you trust

Log Facility

auth.notice /usr/local/logs/syslog
facility.priority action

- Auth authorization systems i.e. login
- Cron used by cron and at
- Daemon system/network daemons
- Kern kernel messages
- Lpr printing
- Mail mail system
- Mark used for timestamps
- News news/nntp system
- User default – used for any program
- Uucp reserved for uucp
- Local0...7 local use

Mainline: solutions you need
from people you trust

Log Priority

- Debug debugging – useful if paranoid
- Info informational msgs
- Notice things that may require attention
- Warning warnings
- Err errors
- Crit critical things like hardware errors
- Alert deal with it NOW
- Emerg Ouch

Mainline: solutions you need
from people you trust

Possible Log Actions

- /dev/console Log to the console
 - /path/file Write messages to file
 - @loghost Log to a central host
 - Jaqui,jim Email jaqui and jim
 - * Send messages to all logged in users
-
- Use swatch or logsurfer or similar to postprocess the logs looking for telltale signs

Mainline: solutions you need
from people you trust

Logging

- touch /usr/local/logs/syslog & maillog & infolog
- Edit /etc/syslog.conf so it looks something like:
 - *.emerg /usr/local/logs/syslog
 - *.alert /usr/local/logs/syslog
 - *.err /usr/local/logs/syslog
 - *.crit /usr/local/logs/syslog
 - mail.debug /usr/local/logs/maillog
 - auth.notice /usr/local/logs/syslog
 - daemon.info /usr/local/logs/infolog
 - *.emerg /dev/console
- refresh -s syslogd
 - I normally stopsrc and startsrc the syslogd
- Note use of separate logs to allow for easier postprocessing
- Ensure logs are cycled daily and monitored
- Move logs out of default /var location to own filesystem
 - If /var fills up things get ugly fast
 - I create /usr/local/logs



Mainline: solutions you need
from people you trust

Some Hacker Tools

- Everything you use plus:
- Xscan – scans subnet for open xservers and logs all the keystrokes
- Wzap – removes a users info from wtmp
- Directories with names like “..” or “...”
- Showmount –e ipaddr - find nfs exports
- Nmap – often used for DOS attacks
- Ident scanning – to find ports owned by root
- Sam Spade
 - www.samspade.org
 - Used to crawl and suck down your whole web site

Mainline: solutions you need
from people you trust

Rootkits

- Hackers install these on the system
- Modify ps, ls, pids, logs, ifconfig, netstat ...
- `ps -no-headers -ef | wc -l`
 - Should show the same result as:
- `ls -d /proc /[0-9]* | wc -l`
- If no-headers does not work – remove it and subtract 1 from the total
- Hide in directories like “. “ or “.. “



Rooted?

Mainline: solutions you need
from people you trust

Detecting Rootkits

- `file /dev/* | grep text`
- Look for things like `/dev/ptyw` ASCII text
- `find / -perm -4000 -print` (suid files)
- `find / -perm -2000 -print` (sgid files)
- `find / -name “.*”`
 - Looks for hidden directories such as “..”
- try `du`, `ls`, `ps`, and `netstat` with the `-/` option
 - If this works then a rootkit has probably been installed
- Use `safe` (saved to `cd`) copied of `top`, `lsof` and `tcplist` to check the system
- Look for binary zeroes in `utmp` & `wtmp` & `lastlog` to see if someone used `zap`

Mainline: solutions you need
from people you trust

How to detect sniffers

- `ifconfig -a | grep PROMISC`
- `nmap` – www.insecure.org/nmap
 - `nmap -p 1-65535 systemname`
 - Scans all ports on the system
- `netstat -a`
- `lsof | grep UDP` or `grep TCP`

Mainline: solutions you need
from people you trust

Scan yourself

- Get management permission first
- Saint
 - <http://www.saintcorporation.com/>
- ISS (Internet Security Systems)
 - <http://xforce.iss.net/>
- nmap
 - `nmap -sTU <remote host>`
- nessus
 - www.nessus.org
- Also portsentry to monitor ports
 - <http://sourceforge.net/projects/sentrytools/>

Mainline: solutions you need
from people you trust

Finding active network ports

- lsof
 - <http://ftp.cerias.purdue.edu/pub/tools/unix/syutils/lsof/>
 - Use command to check for open ports
 - `lsof | grep TCP` or `grep UDP`
- `netstat -tulp` (on Linux not AIX)
- `showmount` and `showmount -e`
- `rpcinfo` and `rpcinfo -p`

Mainline: solutions you need
from people you trust

Incident Reporting

- Gathering Evidence
 - Know the legal issues
- Who to contact and how
- abuse@ your site or the attack site
- FBI or Police
- Local Computer Crime bureau
- Have an Emergency Response Team with a clear set of policies and procedures
- Know your companies policies and procedures ahead of time

Mainline: solutions you need
from people you trust

Gathering Evidence

- CHAIN OF CUSTODY
- Preservation Letters (see USC 18-2704)
- Copies of all logs (signed and dated)
 - Ensure you copy with permissions and dates preserved!
- Output from last and lastcomm commands
- Output from ls -al and other commands
- Output from lsof
- If email - copy of raw headers for the messages
- Username, phone number, etc
- Email address including mail node
 - See next slide

Mainline: solutions you need
from people you trust

Obtaining Email Headers

- Instructions for most clients are at:
 - <http://www.spamcop.net/fom-serve/cache/19.html>
 - <http://www.haltabuse.org/help/headers/index.shtml>
- Paper on Email and Website Tracing
 - <http://www.circle4.com/papers/s1724-aug06.pdf>
- Info on Email Headers in general:
 - <http://www.stopspam.org/email/headers.html>
 - <http://tgos.org/newbie/xheader.html>

Mainline: solutions you need
from people you trust

Cybercrime Laws – www.findlaw.com

- **Note – I am not a lawyer but read these**
- 18USC1030 – Computer Fraud & Abuse Act 1986
 - Covers access to protected systems and hacking
- The Net Act 1997 – “no electronic theft act”
 - Changes copyright laws to include the net and to no longer require financial gain – closed “La Macchia” loophole
- 18USC2511 – Interception & disclosure of wire, electronic & oral communications
 - Protects systems administrators
 - Section 2520 covers damages
- Others
 - USC 18-2510 Definitions
 - USC 15-7404 NSF Cyber security research
 - USC 26-7612 Summonses for computer software
 - USC 20-6777 Internet safety for minors

Mainline: solutions you need
from people you trust

More on Laws

- 18USC2703 & 2707
 - Stored wire, electronic communications & transaction records access – covers how to get info from ISPs
- 18USC875
 - interstate/foreign threats such as ransom, extortion, kidnap & injury
- 18USC2261
 - crossing state lines or forcing/tricking someone to cross with intent to injure or harass
 - Domestic Violence Act
- Hate crimes & Harassment by Surveillance
- Entrapment, defamation, eavesdropping
- Invasion of Privacy
- Federal search and seizure guidelines
 - http://www.cybercrime.gov/s&smanual2002.htm#_I_
- <http://www4.law.cornell.edu/uscode>
- <http://www.thecre.com/fedlaw/default.htm>
- <http://www.findlaw.com>

Mainline: solutions you need
from people you trust

Other Interesting Laws

- 40USC759 – Computer Security Act of 1987
- 18USC2701 – Electronic Communications Privacy Act
- 5USC552 – Electronic Freedom of Information Act
- EO13133 – working group on unlawful conduct on the internet 8/16/99
- EO13103 – Computer software piracy sep/oct 1998
- Anticybersquatting law – Nov 99
 - Curtail trend of registering others names to sell them for profit
- Digital Millenium Copyright Act Oct 1998
 - Guidelines for ISPs whose clients infringe copyright laws
- Digital Signature Act – May 1999

- AND MANY MANY MORE PLUS HPIAA AND SOX

Mainline: solutions you need
from people you trust

Articles/Redbooks worth Reading

- Internet security lecture at Wright on rootkits
 - <http://www.cs.wright.edu/people/faculty/pmateti/Courses/499/Fortification/obrien.html>
- SANS Analysis of various rootkits
 - <http://www.sans.org/> and then search on rootkit
 - http://www.sans.org/reading_room/whitepapers/linux/901.php
 - Linux rootkits for beginners – from prevention to removal
- Analysis of the Knark Rootkit
 - <http://www.securityfocus.com/> and search on knark
- <http://www.linuxsecurity.com>
 - Security Quick Reference Guide
- AIX IP Security
 - <http://www-03.ibm.com/servers/aix/products/ibmsw/security/vpn/techref/m98chang.pdf>
- AIX Advanced Security
 - <http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg247430.html?Open>

Mainline: solutions you need
from people you trust

Helpful Sites 1/2

- <http://cs-www.ncsl.nist.gov/tools/tools.htm>
- <http://www.cert.org>
- <http://ciac.llnl.gov>
- <http://www.infragard.net>
- <http://www.htcia.org>
- <http://www.cerias.purdue.edu/>
- <http://www.defcon.org>
- <http://www.first.org>
- <http://www.securityfocus.com> – Bugtraq plus many other useful items
- <http://www.sampade.org> - put in ip address to find domain
- <http://www.networksolutions.com/cgi-bin/whois/whois>
- <http://www.geektools.com>
- <http://www.deja.com> - deja news (now groups.google.com)
- <http://www-03.ibm.com/security/products/>
- <http://www.sans.org/top20/#index> - SANS top 20

Mainline: solutions you need
from people you trust

Helpful Sites 2/2

- <http://www.haltabuse.org> – Working to halt online abuse
- <http://www.scambusters.org>
- <http://www.cauce.org>
- <http://getnetwise.org>
- <http://privacyrights.org>
- <http://www.hackingexposed.com>
- <http://www.usdoj.gov/criminal/cybercrime/>
 - Includes articles on reporting cybercrime
- <http://www.linuxsecurity.com>
- AIX Security Expert
 - http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert.htm
- AIX Hardening
 - http://www-03.ibm.com/servers/aix/whitepapers/aix_security.html
- AIX Security
 - <http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/security-kickoff.htm>

Mainline: solutions you need
from people you trust

Questions



jaqui@circle4.com

Mainline: solutions you need
from people you trust