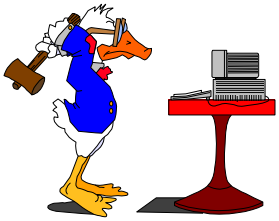
BASIC AIX SECURITY



Jaqui Lynch
lynchj@forsythe.com
Presentation can be found at:
http://www.circle4.com/papers/aixsecurity-oct2013.pdf

FORSYTHE

AGENDA

- Basics
  - Security Intro
  - Permissions
  - Checklists
- Tools that can help
  - OpenSSL, OpenSSH
  - TCP Wrappers
  - Snort, stunnel
- Logging, finding Rootkits
- Incident Handling and laws
- AIX v6 and v7
- PowerSC
- Questions

FORSYTHE

SECURITY TYPES

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

3

FORSYTHE

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

4

FORSYTHE

SANS TOP 10 VULNERABILITIES FROM 2004

- U1 BIND Domain Name System
- U2 Remote Procedure Calls (RPC)
- U3 Apache Web Server
- U4 General UNIX Authentication Accounts with No Passwords or Weak Passwords
- U5 Clear Text Services
- U6 Sendmail
- U7 Simple Network Management Protocol (SNMP)
- U8 Secure Shell (SSH)
- U9 Misconfiguration of Enterprise Services NIS/NFS
- U10 Open Secure Sockets Layer (SSL)

- Sadly this has not changed much
- Many of these are also turned on by default

5

FORSYTHE

SANS TOP 20 CRITICAL SECURITY CONTROLS

HTTP://WWW.SANS.ORG/CRITICAL-SECURITY-CONTROLS/#THREATINDEX

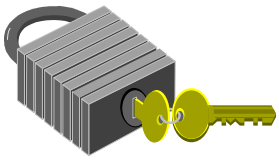
Critical Control 1: Inventory of Authorized and Unauthorized Devices
Critical Control 2: Inventory of Authorized and Unauthorized Software
Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defenses
Critical Control 6: Application Software Security
Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 13: Boundary Defense
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
Critical Control 15: Controlled Access Based on the Need to Know
Critical Control 16: Account Monitoring and Control
Critical Control 17: Data Loss Prevention
Critical Control 18: Incident Response and Management
Critical Control 19: Secure Network Engineering
Critical Control 20: Penetration Tests and Red Team Exercises

6

FORSYTHE

UNIX SECURITY BASICS

Permissions
UID
GID
Dangerous Accounts
Superuser
SUID
Sticky bit
Umask
Backups



FORSYTHE

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.

FORSYTHE

OCTAL PERMISSIONS

4000	SUID on execution	0040	Read by group
2000	SGID on execution	0020	Write by group
1000	Sticky Bit	0010	Execute by group
0400	Read by owner	0004	Read by other
0200	Write by owner	0002	Write by other
0100	Execute by owner	0001	Execute by other

755 Anyone can copy or run the program - Only the owner can change it

+r
+w
+x
+s SUID if u+, SGID if g+
+t Add sticky bit

9

FORSYTHE

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
	It is possible in AIX to code noatime on a filesystem

The above two times can be changed with a command so you should check:

ls -lc	Shows last modification time of the inode

10

FORSYTHE

FILE SECURITY

```
# ls -l messages
-rw-r--r--   1 root     system       1215 Oct 14 19:11 messages
# ls -lu messages
-rw-r--r--   1 root     system       1215 Oct 13 23:59 messages
# ls -lc messages
-rw-r--r--   1 root     system       1215 Oct 14 19:11 messages
```

Then tail messages and:

```
# ls -l messages
-rw-r--r--   1 root     system       1215 Oct 14 19:11 messages
# ls -lu messages
-rw-r--r--   1 root     system       1215 Oct 14 19:23 messages
# ls -lc messages
-rw-r--r--   1 root     system       1215 Oct 14 19:11 messages
```

11

FORSYTHE

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	---	---

12

FORSYTHE

UMASK EXAMPLES

```
Default umask of 022
$touch file1
$mkdir firj1
$ ls -al
total 8
drwxr-xr-x    3 jaqui    system         256 Oct 14 19:31 .
drwxr-xr-x   18 root     system        4096 Oct 14 19:30 ..
drwxr-xr-x    2 jaqui    staff          256 Oct 14 19:31 dirj1
-rw-r--r--    1 jaqui    staff            0 Oct 14 19:30 file1

$umask 007
$touch file2
$mkdir dirj2
$ ls -al
total 8
drwxr-xr-x    4 jaqui    system         256 Oct 14 19:31 .
drwxr-xr-x   18 root     system        4096 Oct 14 19:30 ..
drwxr-xr-x    2 jaqui    staff          256 Oct 14 19:31 dirj1
drwxrwx---    2 jaqui    staff          256 Oct 14 19:31 dirj2
-rw-r--r--    1 jaqui    staff            0 Oct 14 19:30 file1
-rw-rw----    1 jaqui    staff            0 Oct 14 19:31 file2
```

13

FORSYTHE

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
```

14

FORSYTHE

EXAMPLE OF STICKY BIT

```
Use of sticky bit
# ls -al /tmp
drwxrwxrwt   19 bin      bin          4096 Oct 14 19:10 .

# pwd
/usr/local
# mkdir jaquidir
# ls -al jaquidir
total 8
drwxr-xr-x    2 root     system        256 Oct 14 19:16 .
drwxr-xr-x   18 root     system       4096 Oct 14 19:16 ..
# chmod 777 jaquidir
# ls -al jaquidir
total 8
drwxrwxrwx    2 root     system        256 Oct 14 19:16 .
# chown jaqui.sshd jaquidir
# ls -al jaquidir
total 8
drwxrwxrwx    2 jaqui    sshd          256 Oct 14 19:16 .
# chmod +t jaquidir
# ls -al jaquidir
total 8
drwxrwxrwt    2 jaqui    sshd          256 Oct 14 19:16 .
drwxr-xr-x   18 root     system       4096 Oct 14 19:16 ..
```

You can do this with one step – chmod 1777 jaquidir

15

FORSYTHE

ACLS – ACCESS CONTROL LISTS

acledit /usr/local/jaquidir

aclget /usr/local/jaquidir

```
*
* ACL_type   AIXC
*
attributes:
base permissions
    owner(jaqui):  rwx
    group(system):  r-x
    others:  r-x
extended permissions
    disabled

# ls -al /usr/local/jaquidir
drwxr-xr-x    2 jaqui    system        256 Oct 14
19:47 .
drwxr-xr-x   18 root     system       4096 Oct 14
19:30 ..
```

http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/access_control_list_aixc.htm

Extended permissions:
extended permissions: enabled
permit rw- u:dhs
deny r-- u:chas, g:system
specify r-- u:john, g:gateway, g:mail
permit rw- g:account, g:finance

Other commandsL

aclget

aclput

acledit

aclconvert

aclgettypes

16

FORSYTHE

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

17

FORSYTHE

CHECKLIST 1/3

Individual accounts only including for applications
All accounts must have GOOD passwords
Disable tftp if possible
    Use /etc/tftpaccess.ctl to control access
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
    or set them to /bin/false as a login shell
Make regular backups & check restores regularly
Export filesystems that have programs as read-only
Check last login when you login

18

FORSYTHE

CHECKLIST 2/3

System directories - not world or group writable
/etc/hosts.equiv and hosts.lpd should be rwx r-- r– and preferably empty
Remove the + and all comments from your /etc/hosts.equiv and lpd files
Disable unused network services, especially finger, cmsd, ttdbserver
Ensure sendmail or Postfix is at latest version
Do not run sendmail unless you are a mailserver or relay
    Instead set it up in cron to run the queues hourly
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 rw- r-- r– and is owned by root
Ensure /etc/security/passwd is rw for root only
Make sure only root can run last and lastcomm
Turn on password aging and strong but sensible passwords
Set TMOUT in /etc/profile to logout if no activity
Check .forward files are not executable

19

FORSYTHE

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 to 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
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
Scan regularly for .netrc, .rhosts, .shosts and .exrc files
Clean out /etc/inittab, /etc/rc.tcpip – get rid of things that are not needed – but take a copy first

20

FORSYTHE

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: "
```

21

FORSYTHE

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.

22

FORSYTHE

THIRD PARTY TOOLS

http://www-03.ibm.com/systems/power/software/aix/expansionpack/
IBM expansion pack – click on downloads on the right
Includes lsof 4.85, NTPv4, OpenSSH v6.0.0.6102, OpenSSL 0.9.8.2500, Perl, Samba v3.3
http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html
AIX Toolbox for Linux Applications
Includes Sudo 1.6.9p23, GCC plus many of the prereqs for RPM installs
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
Snort 2.9.5.5 (16 Sep, 2013)
http://www.snort.org/snort-downloads
Stunnel 4.56 (March 2013)
https://www.stunnel.org/downloads.html
Logging
swatch
http://sourceforge.net/projects/swatch/
Logsurfer
http://sourceforge.net/projects/logsurfer/?source=directory
Nessus Vulnerability Scanner
http://www.tenable.com/products/nessus

23

FORSYTHE

TCP WRAPPERS AND SSH

Tcp Wrappers - ftp.porcupine.org
Purpose is to wrap services so they can be checked and controlled
SSH – http://www.openssh.org – I now use the one in the expansion pack as it is now not as easy to compile
Wrappers improve security and logging
Allows for secure backups, tunneling and X11 forwarding
Reverse dns lookup can be used to disallow access
Allows tripwires
SSH encrypts logins
SCP allows secure file copies
SFTP replaces FTP
Ensure OpenSSL is installed
Now install the wrapper
Then install OpenSSH
If using the IBM binaries then install using smitty
If Compiling then configure ssh with the wrappers
Do not install or enable support for v1 of ssh

24

FORSYTHE

OPENSSL

I use the one from the IBM expansion pack which is not as up to date

www.openssl.org

Latest is 1.0.1e – have had some problems getting it to compile with GCC on AIX

OpenSSH exects 0.9.8

Provides 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

25

FORSYTHE

OPENSSH

Interfaces with TCP Wrappers for logging and access control

www.openssh.org has the latest which is 6.3 (13 Sep 2013) but you have to compile it for AIX

I use the binary from the IBM expansion pack

Installs openssh.base, etc using smitty

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

26

FORSYTHE

THINGS YOU CAN DO WITH SSH

X11 forwarding that allows the encryption of network X windows traffic so that the data and command streams can't be modified in-flight.

Port forwarding allows the forwarding of TCP/IP connections to a remote system over an encrypted channel. This can also be done using SSL tunnels, but there are many applications that don't support AAL encryption. These applications - such as POP or SNMP - can instead be tunneled through secure SSH channels. This can also be used to tunnel through the firewall rather than allowing other less secure ports to be opened.

Backup using tar via an SSH tunnel.

Add SSH to the rdist/rsync configs and tunnel them.

Run PPP over an SSH tunnel.

Support is also provided for a number of other tools and techniques including Socks support, AFS/Kerberos support and PGP key support.

OpenSSH compresses data before encryption using zlib. This can improve overall performance.

OpenSSH uses the OpenSSL cryptographic library.

Remote commands

ssh jaqui@server command

tar -cvzf - /freddy | ssh root@nimit "cat > /backups/freddy.tar.gz"

tar -cvzf - /freddy | ssh root@nimit "cat > /dev/rmt0"

Setting SSH up for simple administration

http://www.ibmsystemsmag.com/aix/tipstechniques/systemsmanagement/SSH_simplifies_administration/

27

FORSYTHE

PROGRAMS AND TOOLS FOR SSH

ssh - client

sshd - server

/etc/ssh/ssh_config client configuration file

/etc/ssh/sshd_config daemon configuration file

ssh-agent – authentication agent for loading private keys into memory

ssh-add – tool to load keys into ssh-agent

ssh-keygen – tool to generate and manage keys

scp – secure file copy

SFTP – secure replacement for FTP

Generally only transfers as binary

28

FORSYTHE

TUNNELING TELNET AND FTP

On ssh server.com
ssh -R 1234:localhost:23 -l jaqui ssh.client.com
This maps port 1234 (note >1024) on ssh.client.com to the servers port 23 (telnet) and starts an encrypted session
Now from client.com
telnet localhost 1234
You're now connecting via a secure tunnel back to the server.
ssh -L 1234:ftphost:21 ssh.host.com
Now from client - ftp localhost 1234

29

FORSYTHE

TCP WRAPPERS

Purpose is to wrap services
ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6-ipv6.4.tar.gz
Wrapper called by inetd and checks rules files
Uses 2 files to control access
/etc/hosts.allow and hosts.deny
Attempts get logged and then attempt is authorized or denied
Two ways to install
1. Replace the current service
2. Install tcpd into /usr/local/bin and insert it into the inetd.conf line
I prefer option 2
Lets you post banners whether the service is granted or not

30

FORSYTHE

TCP WRAPPERS CONFIGURATION

After downloading and untarring
vi Makefile
STYLE = -DPROCESS_OPTIONS # Enable language extensions.
FACILITY= LOG_DAEMON # LOG_MAIL is what most sendmail daemons use
SEVERITY= LOG_INFO
Uncomment IPV6=-DHAVE-IPV6
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

31

FORSYTHE

/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

32

FORSYTHE

/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

33

FORSYTHE

/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

34

FORSYTHE

/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

35

FORSYTHE

/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
xmservd	:	.abc.com,123.123.123.4
rlogind	:	LOCAL,.abc.com,123.123.123.4
rexecd	:	LOCAL, 192.168.1.
smtpd	:	LOCAL, 192.168.1.
sendmail	:	LOCAL, 192.168.1. EXCEPT 192.168.1.4
Telnetd	:	LOCAL, 192.168.1. : BANNERS /etc/motd

36

FORSYTHE

SNORT

http://www.snort.org

Latest version is v2.9.5.5

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

37

FORSYTHE

STUNNEL

http://www.stunnel.org

Latest version is 4.56

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

38

FORSYTHE

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

39

FORSYTHE

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

40

FORSYTHE

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

41

FORSYTHE

LOGGING

touch /usr/local/logs/syslog & authlog & mailog & 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/mailog
auth.notice	/usr/local/logs/authlog
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

42

FORSYTHE

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

……

43

FORSYTHE

ROOTKITS

Hackers install these on the system

Modify ps, ls, pids, logs, ifconfig, netstat …

Hide in directories like ". " or ".. "

find / -name ".*"

Looks for hidden directories such as ".. "

There is a space above after the ..

Rooted?

44

FORSYTHE

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)

try du, ls, ps, and netstat with the -/ option

If this works then a rootkit has probably been installed

Use ps

ps -no-headers -ef | wc
ls -d /proc /[0-9]* | wc
(The above two commands should show the same number.)

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

45

FORSYTHE

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

46

FORSYTHE

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/

47

FORSYTHE

FINDING ACTIVE NETWORK PORTS

lsof

http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/lsof/

Use command to check for open ports

lsof | grep TCP or grep UDP

netstat –tulp (on Linux not AIX)

On AIX

- netstat | more
- First section is active connections

showmount and showmount –e

rpcinfo and rpcinfo -p

48

FORSYTHE

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

FORSYTHE

RESPONSE PLAN

Who to contact and how
- Technical people, management, etc

Corporate policies for who to engage and when
Copies of all security policies
Copy of evidentiary gathering rules
Clearly written AUP (acceptable use policy) that employees sign yearly

FORSYTHE

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 and other commands
    print and sign with witness if needs be
If email - copy of raw headers for the messages
Username, phone number, etc
Email address including mail node

FORSYTHE

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
http://whatismyipaddress.com/find-headers
http://www.jahitchcock.com/cyberstalked/header.htm
http://www.cyberbullying.info/resources/headers.php

Paper on Email and Website Tracing
http://www.circle4.com/papers/s1724-aug06.pdf

Info on Email Headers in general:
http://whatismyipaddress.com/email-header

FORSYTHE

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

53

FORSYTHE

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 for computers and electronic evidence
http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

LAW Research
http://www4.law.cornell.edu/uscode
http://www.thecre.com/fedlaw/default.htm
http://www.findlaw.com

54

FORSYTHE

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 HIPAA AND SOX …….

55

FORSYTHE

SECURITY ADVISORIES

http://www14.software.ibm.com/webapp/set2/subscriptions/onvdq
Choose the operating system under heading then under topic select security advisories
Also check out the CERT alerts at:
http://www.us-cert.gov/ncas/alerts/
National Vulnerability Database
http://web.nvd.nist.gov/view/vuln/search

56

FORSYTHE

SECURITY PRE AIX V6

Auditing
- Audit framework
- AIX Security Expert (v5.3 tl05) – low, medium or high

Authorization
- DAC (discretionary access control)
- Local passwords, LDAP integration, Kerberos and longer passphrases
- Up to 255 character passwords and different hashing algorithms introduced in AIX v5.3

Access Control
- Loadable authorization modules, PAM, File Permission Manager, ACLs (access control lists) and limited RBAC (role based access control)
- Mandatory access control (or multi-level security) refers to various certifications

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)

57

FORSYTHE

NEW IN AIX V6 1/3

See Advanced AIX v6 Security Features Redbook at http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg247430.html?

Auditing
- Added Cobit/SOX compliance reporting

AIX Security Expert Enhancements
- Provides password policy enforcement, violation and security activity reports, firewall architecture and malicious software prevention
- SOX turns on auditing and disables root logins
- Also turns on IPSec with filter rules to prevent port scans
- Options of low, medium, high or SOX
- LDAP integration for propagation

http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert.htm

Enhanced RBAC added to Access Control.
- This is required for WPARs (workload partitions)
- Now the default at install time
- Replaces many functions of SUDO
- Use swrole to change roles
- 3 key elements – authorizations, roles and privileges
- Over 150 granular controls to define roles
- Ability to centralize policies on an LDAP server

58

FORSYTHE

NEW IN AIX V6 2/3

CLiC enhanced to include PCKS11 and is a prerequisite for the new encrypted filesystem
Encrypted filesystem (EFS)
- Automatically encrypts and decrypts files

Key based
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)
Centralized Key Management for EFS stored in LDAP (6.1 tl04)
See article at:
http://www.ibmsystemsmag.com/aix/administrator/security/Locking-Down-Files-With-Encrypted-File-System/

59

FORSYTHE

NEW IN AIX V6 3/3

Secure by default
- Install time option
- Installs a minimum set of filesets (about 100)
- You add what you need later
- Most network filesets not installed

File Permission Manager
- Intent is to reduce setuid bit programs
- New fpm command
- Multiple levels

Secure FTP
- Encrypts both the data and command channels
- Built on OpenSSL
- Useful where clients do not have SSH
- Is basically ftp using SSL

Trusted execution added for integrity checking.
- Uses a TSD (trusted signature database)
- New trustchk command
- Ensures important binaries are not altered

Trusted AIX
- Removes concept of root
- Uses MAC (mandatory access controls) and requires auditing

60

FORSYTHE

NEW IN AIX V7

Primarily enhancements:

Enhanced encryption for EFS, IPSec and trusted Execution

Hardware accelerated encryption

Updates for Common Criteria CAPP/EAL4+ security certification

Support for xlC V11 ProPolice stack protection feature

Support for up to 2048 groups

AIX Security Expert

RBAC enhancements

- Enhanced to add domain support
- Retrofitted to AIX v6 tl06

Domains can be used to control access to volume groups, filesystems, files and devices

Secure by default

http://web.nvd.nist.gov/view/ncp/repository?tier=&product=IBM+AIX+6.1&category=&authority=&keyword=

In the above you will find security templates for AIXPERT from NIST

61

FORSYTHE

IMPORTANCE OF STAYING CURRENT

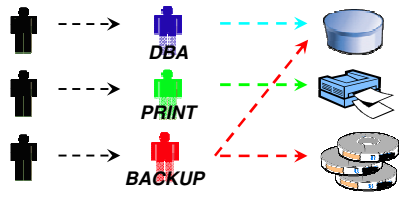
- AIX 6.1 tl08 sp3 and AIX 7.1 tl02 sp3 fixed multiple security problems
  - IV42124 for bos.net.tcp.client (IPV6)
  - IV43580 for infiniband
  - IV42933 for tftp
- VIOS 2.2.2.3 FP26 SP2 also closes those holes
- Programs like sendmail and snmp need to be watched

62

FORSYTHE

AIX V6.1 / 7.1 SECURITY: RBAC

Provides greater security and increased administration flexibility



Authorizations
Mechanism to grant access to commands or certain functionality. Context aware.

Roles
A container for authorizations that can be assigned to a user.

Privileges
Process attribute that allows process to bypass a security restriction. Not context aware.

aix	device fs network proc ras security **system** wpar	**boot** config install stat	create halt **info** reboot shutdown	"create boot image" "halt the system" "display boot information" "reboot the system" "shutdown the system"

New in AIX 7: Domain Role Based Access Control

New in PowerVM 2.2: RBAC on the Virtual I/O Server

```
# lssecattr -c -F /usr/sbin/bootinfo
/usr/sbin/bootinfo:
        accessauths = aix.system.boot.info
        innateprivs = PV_DAC_R,PV_DAC_W,PV_DEV_CONFIG,PV_KER_RAS
```

`/etc/security/privcmds`

63

FORSYTHE

DOMAIN BASED ROLE BASED ACCESS CONTROL

Domains supported by system are stored in configuration file:
/etc/security/domains

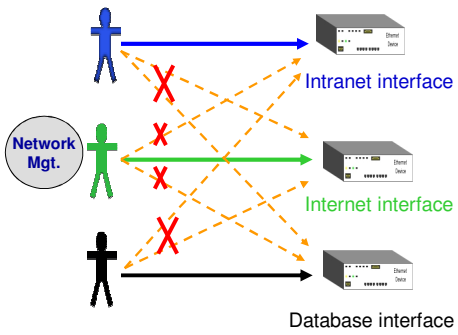
```
domain-name:
id = <number>
msg = <description of domain>
```

Domain Assigned Object Database /etc/security/domobjs holds definition of objects which require domains access checks

```
/dev/hrvg:
domains=HR,IT
conflictsets=payroll
type=device
secflags=FSF_DOM_ANY
```

Each user would be optionally associated with a domain or set of domains
User's domain stored in /etc/security/user database in new `domains` attribute
New commands

```
mkdom, lsdom, chdom, rmdom
```



- **Various type of objects can be put in domains**
  - Filesystems & Volume Groups
  - Network Interfaces & Network Ports
  - Devices

64

FORSYTHE

AUDITING ENHANCEMENTS: ROLE-BASED AUDITING

Role-based auditing

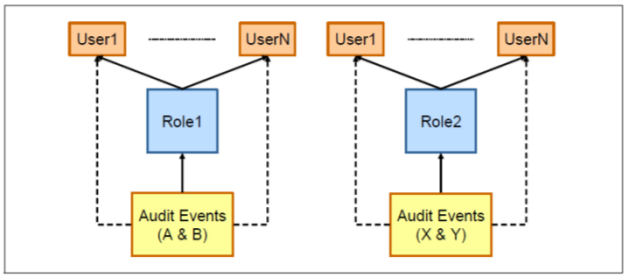
Auditing has been enhanced to audit events on per role basis

Provides more flexibility to monitor system based on roles

Auditing events are assigned to roles that are in turn assigned to users

New `auditclasses` attribute for `mkrole` / `chrole` commands

New `roles` stanza in `/etc/security/audit/config` file



65

FORSYTHE

LDAP

- LDAP module integrated into AIX now
- Case sensitive LDAP user names
- LDAP alias support for users
- Caching enhancements
- lsldap now covers advanced accounting and AIX security expert
- Supports Windows 2008 AD and ADAM

66

FORSYTHE

MISCELLANEOUS

- AIX password policies
  Disallow username in password
  Disallow a particular pattern in password
- chpasswd support for LDAP
  new –R LDAP option
- System group write permissions removed from ODM
- NGROUPS_MAX increased from 128 to 2048 per user
  Now a tunable for sys0

67

FORSYTHE

POWERSC

Trusted Boot

Insures that the Operating System has not been inadvertently or maliciously altered to compromise the security of the system

Trusted Logging

Provides a central tamperproof repository for the system and audit logs

Trusted Network Connect

Detect AIX virtual machines that do not meet the corporate patch policies and my have potential vulnerabilities

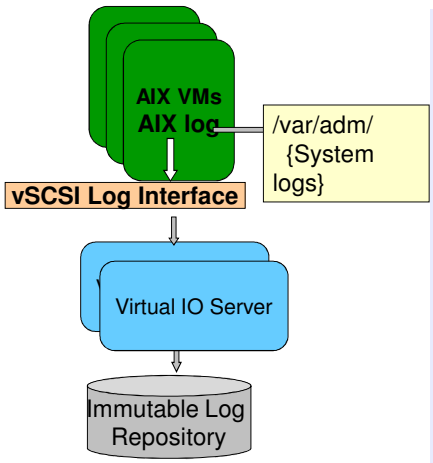
Security Compliance Automation (also sold as PowerSC Express Edition)

Assures that the settings in the operating system match security standards for Payment Card Industry (PCI), or US Department of Defense Security Technical Implementation Guide (DOD STIG) or the SOX/Cobit standards

68

FORSYTHE

PowerSC Trusted Logging – How does it work?

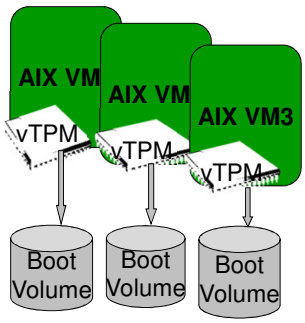


- AIX Logs use a Special Log Virtual SCSI Device
- Log Virtual SCSI device is created and managed by VIOS
- Logging data is written to an Immutable Repository or storage connected to the VIOS Server
- As the data is stored the AIX VM cannot alter or remove logs owned by VIO Server
- Normal AIX Logs in the VM are still available as well

69

FORSYTHE

PowerSC Trusted Boot – How does it work?



- Each Virtual Machine has its own vTPM Configured using HMC/SDMC
- During the AIX Boot process Measurements are taken and Compared to vTPM contents
- PowerVM Hypervisor and PowerSC work together to metric the boot process and store the metrics in the vTPM
- Trusted Status is available for "Attestation" using OpenPTS Monitor

* This feature requires Firmware 7.4 or above

70

FORSYTHE

POWERSC EDITIONS SECURITY AND COMPLIANCE OPTIONS

- **PowerSC Express**
  - *Basic compliance for AIX*
- **PowerSC Standard**
  - *Security and compliance for virtual & cloud environments*

PowerSC Editions	Express	Standard
Security and Compliance Automation	✓	✓
Trusted Logging		✓
Trusted Boot**		✓*
Trusted Network Connect and Patch Management		✓

PowerSC Standard Edition Installation Requires
AIX PowerSC Standard software Package
AIX Version 6 TL7 or higher or AIX 7 TL1 or higher
VIOS level v2.2.1 and above
Firmware(eFW7.4) and above for the "Trusted Boot" Feature

71

FORSYTHE

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/systems/resources/systems_p_os_aix_security_vpn_techref_m98chang.pdf
AIX Advanced Security
http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg247430.html?Open

72

FORSYTHE

HELPFUL SITES 1/2

http://cs-www.ncsl.nist.gov/tools/tools.htm
http://nvd.nist.gov/scapproducts.cfm
http://www.us-cert.gov/ncas/alerts
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.networksolutions.com/cgi-bin/whois/whois
http://whois.net
http://www.geektools.com
http://www-03.ibm.com/security/products/

73

FORSYTHE

HELPFUL SITES 2/2

- AIX v6 Security
- http://publib.boulder.ibm.com/infocenter/pseries/v6r1/index.jsp?topic=/com.ibm.aix.security/doc/security/security-kickoff.htm
- AIX v7 Security
- http://publib.boulder.ibm.com/infocenter/aix/v7r1/index.jsp?topic=/com.ibm.aix.security/doc/security/security-kickoff.htm
- 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/support/techdocs/atsmastr.nsf/WebIndex/TD105143
- http://www.sans.org/reading-room/whitepapers/unix/unix-system-management-security-differences-linux-solaris-aix-hp-ux-936?show=unix-system-management-security-differences-linux-solaris-aix-hp-ux-936&cat=unix
- http://www.usdoj.gov/criminal/cybercrime/
- Includes articles on reporting cybercrime
- Other
- http://www.linuxsecurity.com
- http://www.haltabuse.org – Working to halt online abuse
- http://www.scambusters.org
- http://getnetwise.org
- http://privacyrights.org

74

FORSYTHE

THANK YOU FOR YOUR TIME

If you have questions please email me at:
lynchj@forsythe.com

Presentation can be found at:
http://www.circle4.com/papers/aixsecurity-oct2013.pdf

Check out our movies at:
http://www.circle4.com/movies/

More Forsythe Talks Info at:
http://www.circle4.com/forsythetalks.html

FORSYTHE