BEDROCK
security services

Auditing and Hardening Unix Systems

Using CIS benchmarks on SUSE Linux

André Carrington, P.Eng, CISSP, CISM

- Unix experience: 13 years
  - SunOS; NeXTSTEP; Sun Interactive; Wyse Unix; BSD; Solaris; QNX; HP-UX; Mandrake Linux; RedHat Linux; SUSE Linux; AIX
  - As a user, developer, system administrator, webmaster, security specialist, security architect
- Professional IT experience: 13 years
  - Recent: A Large Telco, Center for Internet Security (CIS), a commercial bank, etc.
  - Also passed the CISA exam

What is hardening?

Applying security controls to information systems to make them hard to exploit for unauthorized purposes.

Preventing the candy-bar phenomenon: hard and crunchy on the outside, but soft and chewy on the inside.

What should be hardened?

That is a risk-based decision.

Any information system component can be compromised, so hardening guidelines and standards exist for:

- Servers
- Databases
- Workstations
- Routers
- Wireless access points
- Web server software
- E-mail server software

Assertions about hardening…

Hardening is:

- Effective
- Necessary to perform due diligence
- Measurable
- Detailed/skilled work – that can be automated!

Hardening is effective

According to the Center for Internet Security (CIS):

The vast majority of cyber attacks exploit known vulnerabilities for which a patch or security configuration control is available.

Solution: 80-100% of known vulnerabilities are blocked by implementing the CIS consensus benchmark configuration controls and applying available patches.

http://www.cisecurity.org/Documents/Reducing_Over_80.htm
(based on studies by NSA, MITRE and Solutionary)

We’ll come back to the other assertions…

How do you harden a Unix system?

- Protect the system during setup
- Setup from scratch (or scan/review)
- Backup configuration files
- Apply patches
- Turn on system accounting/logging
- Turn off unneeded services
- Use secure services
- Tune file/directory permissions
- Tune system administration accounts
- Tune kernel parameters

E.g. Use secure services: SSH

- Configure and use SSH
  - A tunnel that is encrypted and mutually authenticated that allows:
    - SSH v2 instead of telnet
    - SFTP, SCP instead of FTP, TFTP, rcp, rdist
    - X-Windows in a secure manner
  - Servers are authenticated with public keys stored on the client
  - Clients are authenticated with public keys or passwords

SSH configuration script

```
cp sshd_config sshd_config.tmp
   awk '/^#? *Protocol/ { print "Protocol 2"; next };
      /^#? *X11Forwarding/ \
         { print "X11Forwarding yes"; next };
      /^#? *IgnoreRhosts/ \
         { print "IgnoreRhosts yes"; next };
    /^#? *HostbasedAuthentication/ \
         { print "HostbasedAuthentication no"; next };
      /^#? *PermitRootLogin/ \
         { print "PermitRootLogin no"; next };
      /^#? *PermitEmptyPasswords/ \
         { print "PermitEmptyPasswords no"; next };
      /^#? *Banner/ \
         { print "Banner /etc/issue.net"; next };
      {print}' sshd_config.tmp > sshd_config
   rm sshd_config.tmp
```

E.g. Tune file/directory permissions

- Review permissions & requirements:
  - passwd, shadow, group
  - User home directories & dot files
  - World-writable files
  - World-writable directories – sticky bit
  - Set-UID and set-GID files
  - Nosuid option re: mounted file systems
  - Unowned files

Set-UID/GID files

- Find them:

```
for PART in `awk '($6 != "0") { print $2 }' /etc/fstab`; do
        find $PART \( -perm -04000 -o -perm -02000 \) \
        -type f -xdev –print
done
```

- Compare them to a baseline (e.g. expected system files per a brand new installation – also included with some tools)

- Watch for changes with a file integrity checker (and watch for new ones with a cron job)

E.g. Tune kernel parameters

```
cat <<END_SCRIPT >> /etc/sysctl.conf
# Following 11 lines added by CISecurity Benchmark sec 4.1
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.tcp_syncookies=1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
END_SCRIPT
chown root:root /etc/sysctl.conf
chmod 0600 /etc/sysctl.conf

cat <<END_SCRIPT >> /etc/sysctl.conf
# Following 3 lines added by CISecurity Benchmark sec 4.2
net.ipv4.ip_forward = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
END_SCRIPT
chown root:root /etc/sysctl.conf
chmod 0600 /etc/sysctl.conf
```

That seems like a lot of work!

How to make it easier

- Some vendors/resellers have images
  - Dell, Oracle
- For your own installation images:
  - Assemble scripts & baselines from standards like the CIS benchmarks
- Use the 80/20 rule—select controls based on overall priorities/risks

Some issues may arise.

- Some application functions may not work right away
  - Sometimes this identifies non-secure practices in vendor products
  - Consider your options and resolve the conflict as needed
- Use standards that differentiate between:
  - Actions that generally won’t break functions
  - Actions that may…

Standards Organizations

- Center for Internet Security
- NIST (including DISA)
- NSA
- ISF

Vendors also provide hardening guidelines

The Center for Internet Security (CIS)

- Modeled after other community initiatives, e.g., transportation safety
- A not-for-profit consortium of <u>users</u>
- Focused on the common needs of the global Internet community
- Convenes and facilitates consensus teams that develop detailed operational best practices

The CIS consensus process

- Teams are formed with security experts from CIS public and private sector member organizations
  - I've worked on teams with DISA, DOE, NIST, Cisco, Jay Beale, etc.
- An initial benchmark draft is obtained or developed
- Consensus is established via conference call discussion & e-mail

Note: Benchmarks & scoring tools are made available free to all users globally via the CIS website

How do I audit my system?

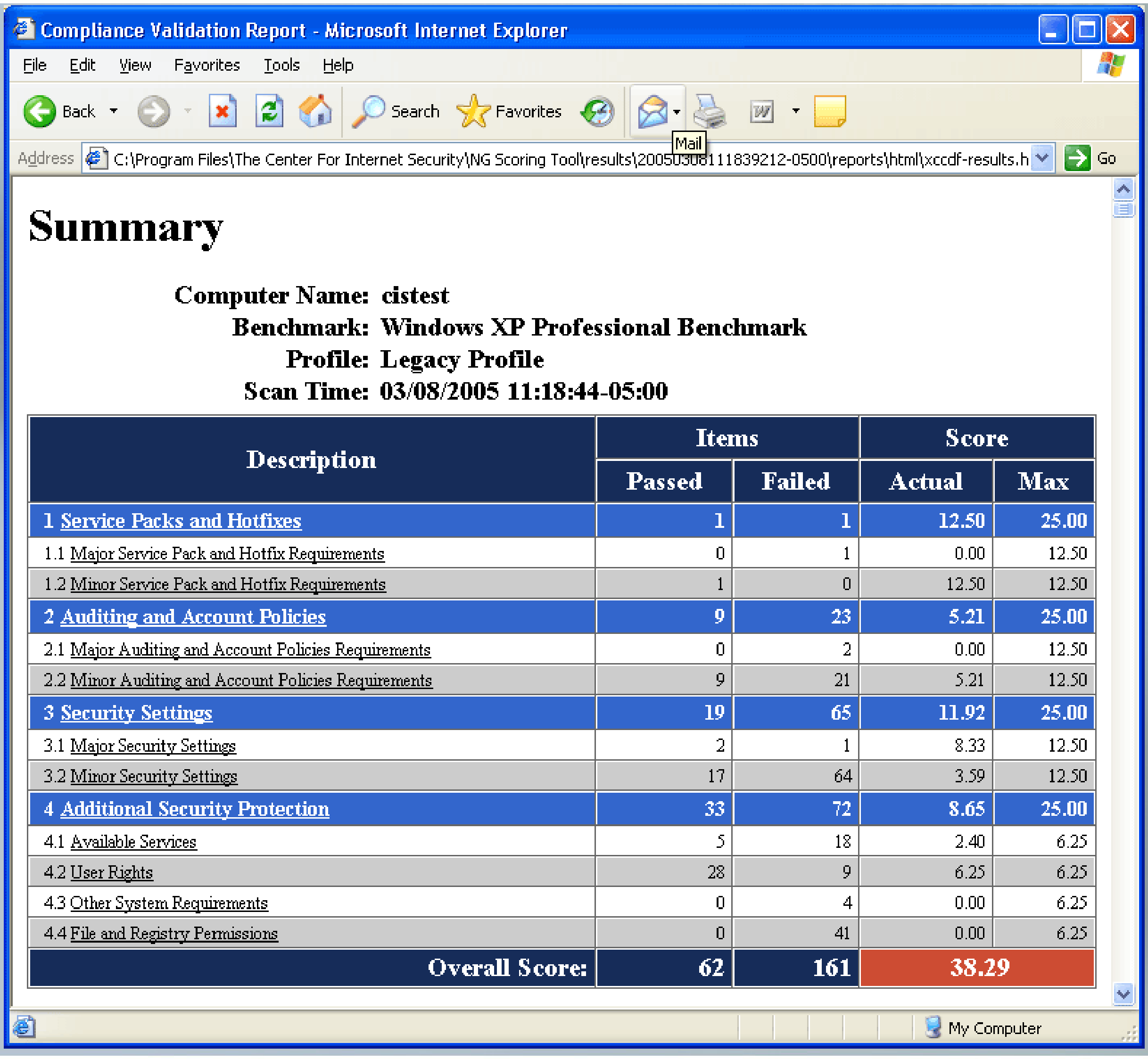
The technical part of the audit can be automated.

- Free scoring tools
  - CIS scoring tools are free for individual use within…
  - VA Scanners are focused on vulnerabilities in network services
  - Address local users; prevent candy bars
  - Assists with intrusion detection
  - Other platforms: Cisco RAT; MBSA
- Commercial enterprise management tools
  - There are many: ISS, Computer Associates, etc.
  - Some can score against published standards

The old CIS scoring tool was text-based (default installation sample).

```
*** CIS Ruler Run ***
Starting at time 20051010-19:58:57

Positive: 1.1 System appears to have been patched within the last month.
Negative: 1.2 sshd_config parameter Protocol is not set.
…
Negative: 8.10 Current umask setting in file /etc/profile is 022 -- it should be
 stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.login is 022 -- it should
be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.cshrc is 000 -- it should
be stronger to block group-read/write/execute.
Negative: 8.11 Coredumps aren't deactivated.
Preliminary rating given at time: Mon Oct 1 19:58:58 2005

        Preliminary rating = 5.85 / 10.00

Positive: 6.6 No non-standard world-writable files.
Positive: 6.7 No non-standard SUID/SGID programs found.
Ending run at time: Mon Oct 1 19:58:59 2005

        Final rating = 6.15 / 10.00
```

The new scoring tool is in development (Windows sample)


Compliance Validation Report - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Mail
Address
C:\Program Files\The Center For Internet Security\NG Scoring Tool\results\20050308111839212-0500\reports\html\xccdf-results.h
Go
My Computer

Summary

Computer Name: cistest
Benchmark: Windows XP Professional Benchmark
Profile: Legacy Profile
Scan Time: 03/08/2005 11:18:44-05:00

Description	Items		Score	
	Passed	Failed	Actual	Max
1 Service Packs and Hotfixes	1	1	12.50	25.00
1.1 Major Service Pack and Hotfix Requirements	0	1	0.00	12.50
1.2 Minor Service Pack and Hotfix Requirements	1	0	12.50	12.50
2 Auditing and Account Policies	9	23	5.21	25.00
2.1 Major Auditing and Account Policies Requirements	0	2	0.00	12.50
2.2 Minor Auditing and Account Policies Requirements	9	21	5.21	12.50
3 Security Settings	19	65	11.92	25.00
3.1 Major Security Settings	2	1	8.33	12.50
3.2 Minor Security Settings	17	64	3.59	12.50
4 Additional Security Protection	33	72	8.65	25.00
4.1 Available Services	5	18	2.40	6.25
4.2 User Rights	28	9	6.25	6.25
4.3 Other System Requirements	0	4	0.00	6.25
4.4 File and Registry Permissions	0	41	0.00	6.25
Overall Score:	62	161	38.29	

The Audit process

- Policy
- Processes
- Configuration
- Activity

Audit

- Policy
- Processes
  - Deployment
  - Administration
  - Monitoring
- Configuration
- Activity

Audit

- Policy
- Processes
  - Deployment
  - Administration
    - Change Management
    - Patch Management
    - Backup and Recovery
  - Monitoring
- Configuration
- Activity

Audit

- Policy
- Processes
  - Deployment
  - Administration
  - Monitoring
    - Vulnerability Assessment
    - Log Review & HIDS
    - Compliance Review
- Configuration
- Activity

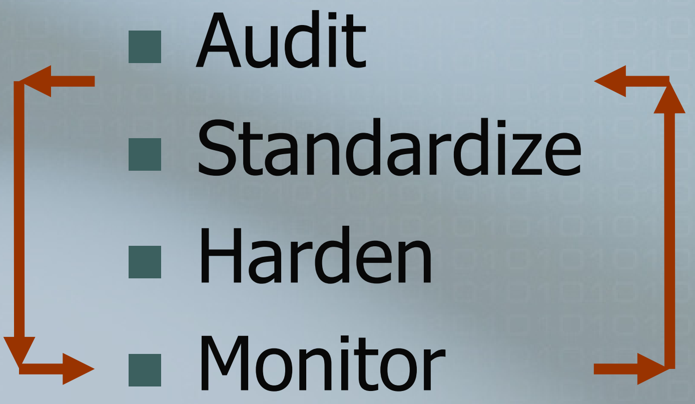
Audit

- Policy
- Processes
- Configuration
  - Scoring tools
  - Hardening scripts
- Activity

Audit

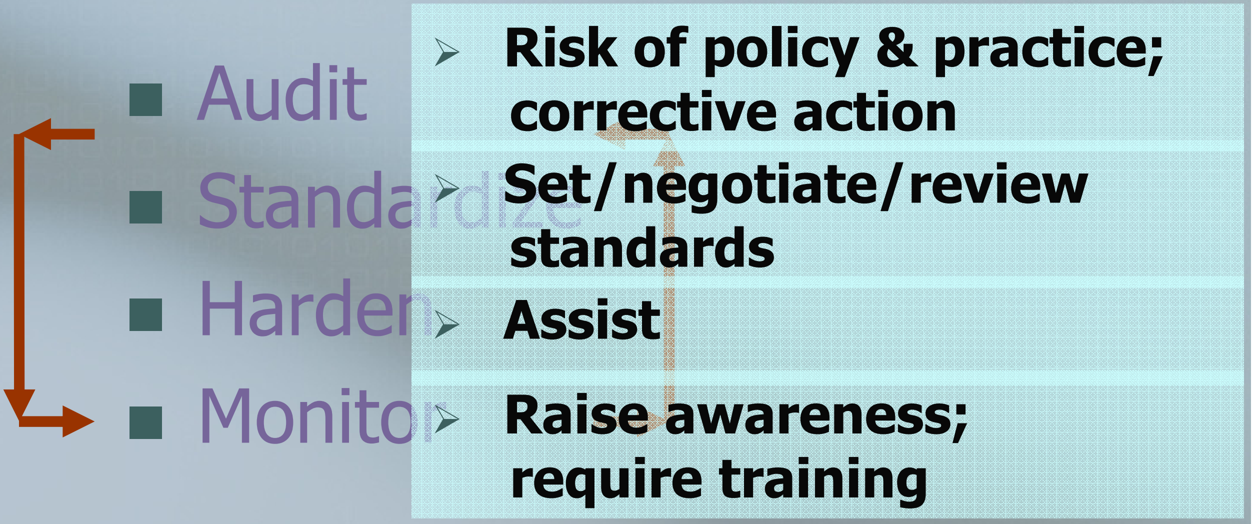
- Policy
- Processes
- Configuration
- Activity
  - User Login Attempts
  - File changes
  - Root shell commands
  - Errors

How audit fits into the lifecycle



- Audit
- Standardize
- Harden
- Monitor

The management view of it…



- Audit
- Standardize
- Harden
- Monitor

- Risk of policy & practice; corrective action
- Set/negotiate/review standards
- Assist
- Raise awareness; require training

In conclusion

I have addressed the assertions that hardening is:

- Effective
- Necessary to perform due diligence
- Measurable
- Detailed/skilled work – that can be automated!

Thank-you for your time.

André Carrington, P.Eng, CISSP, CISM