# CIS Benchmarks

By Russ McRee

## Prerequisites

Java Runtime Environment (for Red Hat Linux testing)

CIS is the Center for Internet Security, a non-profit enterprise whose mission is to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. In step with their mission the Center offers CIS Benchmarks that are the epitomy of sound requirements and standards. Developed by consensus, largely with the help of the user community, these benchmarks are based on "recognized best practices for deployment, configuration, and operation of networked systems."[1] The CIS Benchmarks encompass the trifecta of Internet-based attacks and disruptions: technology (software and hardware), process (system and network administration) and human (end user and management behavior). The benchmarks are publicly available to everyone, at no charge. While non-profit, CIS does promote membership on a sliding fee scale based on size and nature of organization, but membership is not a requirement to make use of these fine tools. Simply defined, the CIS Benchmarks "enumerate security configuration settings and actions that "harden" your systems. They are unique, not because the settings and actions are unknown to any security specialist, but because consensus among hundreds of security professionals worldwide has defined these particular configurations."[2]

We will endeavor to apply the benchmarks to three unique systems for your consideration: Windows Server 2003, Red Hat Linux (CentOS), and the Apache web server. The various benchmarks can be downloaded after answering a few questions on the Center's site.[3] Privacy is important to CIS, and although they ask for certain personal information, including name and email address from persons downloading CIS products, this information is not divulged to any third party and is used only to communicate urgent product information fixes, seek advice and feedback about CIS's services, and invite participation in CIS's consensus process.

If you intend to use this column as a guideline, under Select Benchmark Package(s) select Windows Server 2003, Linux Level 1, and Apache Level 1&2. On the download page, for Windows testing, I typically choose the NG Scoring Tool packages that offers a self-contained JVM, eliminating the need to install a full JVM on a server on which it may have no business. Unfortunately, to test Red Hat installations, you need to download the scoring tool that does not include a JVM and ensure that one is installed on the server in question.

Tenable Network Security's Nessus Vulnerability Scanner v3.0 and Security Center v3.2 are certified for certain CIS Benchmarks and can be used to conduct agent-less configuration audits.

CIS's VP Dave Shackleford advised *toolsmith* that:

1. CIS is currently working on the following new and updated benchmarks: HP-UX, Red Hat Enterprise, Solaris 10 Update 3, Windows 2003 Server, FreeRADIUS, OpenLDAP, IIS, and Virtual Machine security. Cisco IOS and PIX OS updates are pending, as well as HP Multi-function print devices, Apache, Oracle, and hopefully either JunOS or Check Point. They will also be releasing Debian Linux and MySQL shortly (they are complete, but being formatted right now).
2. They have been working with the IT Compliance Institute, the SANS SCORE team, and many others to include compliance mapping to many benchmark recommendations – over time, this will be a great collaborative effort for auditors and security professionals alike.
3. They will be releasing a new tool called CIS-CAT (CIS configuration assessment tool) very soon, with full Windows support later in the year (it will only have Unix and Linux support out of the gate).

## Windows Server 2003

Deploying the CIS Next Generation Scoring Tool on a Windows Server 2003 system is as easy as copying or downloading the `ng_scoring_tool-gui-1.0-win32.exe` to the system you wish to assess and executing it. A 94MB install will ensue. Engage the GUI from the Start menu or your installation directory. Under Benchmark, choose *Windows Server 2003 Benchmark* (no other options) and the appropriate profile for your server under Profile, then click *Score*. Another window will open and ask you to select *Yes*, *No*, or *Unknown* radio buttons for questions that represent benchmark items that cannot be scored automatically.

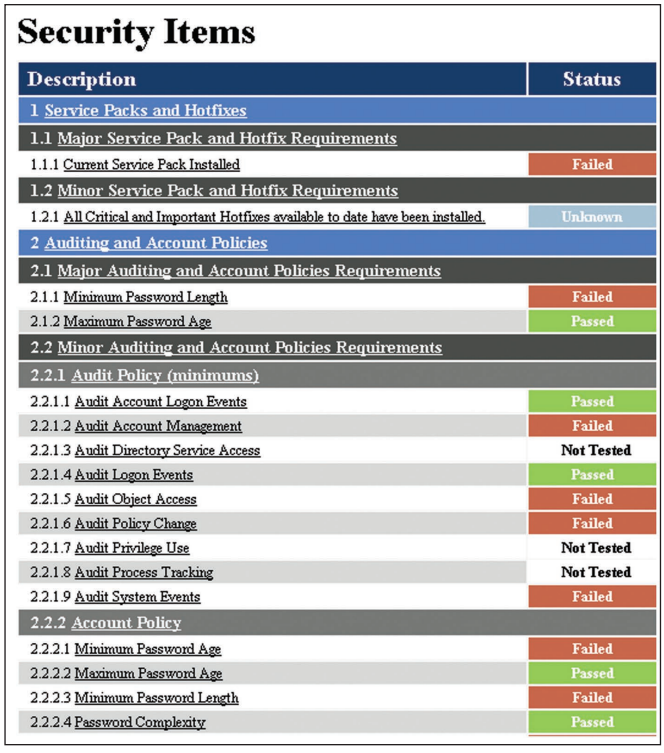
Once the Scoring Tool completes its run, you will have the option to review Benchmark, User, and Service reports. User and Service reports closely follow their naming conventions, returning user accounts and installed service. The Bench-

1 http://www.cisecurity.org/charter.html

2 http://www.cisecurity.org/bench.html

3 http://www.cisecurity.org/sub_form.html

mark report is significant in its findings. Major categories include Service Packs and Hotfixes, Auditing and Account Policies, Security Settings, and Additional Security Protection, with a number of detailed subcategories including Audit Policy, Logs, and User Rights.



**Security Items**

| Description | Status |
|---|---|
| 1 Service Packs and Hotfixes | |
| 1.1 Major Service Pack and Hotfix Requirements | |
| 1.1.1 Current Service Pack Installed | Failed |
| 1.2 Minor Service Pack and Hotfix Requirements | |
| 1.2.1 All Critical and Important Hotfixes available to date have been installed. | Unknown |
| 2 Auditing and Account Policies | |
| 2.1 Major Auditing and Account Policies Requirements | |
| 2.1.1 Minimum Password Length | Failed |
| 2.1.2 Maximum Password Age | Passed |
| 2.2 Minor Auditing and Account Policies Requirements | |
| 2.2.1 Audit Policy (minimums) | |
| 2.2.1.1 Audit Account Logon Events | Passed |
| 2.2.1.2 Audit Account Management | Failed |
| 2.2.1.3 Audit Directory Service Access | Not Tested |
| 2.2.1.4 Audit Logon Events | Passed |
| 2.2.1.5 Audit Object Access | Failed |
| 2.2.1.6 Audit Policy Change | Failed |
| 2.2.1.7 Audit Privilege Use | Not Tested |
| 2.2.1.8 Audit Process Tracking | Not Tested |
| 2.2.1.9 Audit System Events | Failed |
| 2.2.2 Account Policy | |
| 2.2.2.1 Minimum Password Age | Failed |
| 2.2.2.2 Maximum Password Age | Passed |
| 2.2.2.3 Minimum Password Length | Failed |
| 2.2.2.4 Password Complexity | Passed |

**Figure 1 – Windows Server 2003 Benchmark Findings**

These reports are built with XCCDF, a specification language for writing security checklists, benchmarks, and related kinds of documents. "The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices."[4] NSA is developing the XCCDF specification and documents/schemas are available.[5] The public availability of this specification offers you the opportunity to contribute, or create your own checklists.

## Linux Level 1

I tested the NG Scoring Tool 1.0 for Linux, specifically Red Hat, on a server that had a JRE installed. I unzipped `ng_scoring_tool-1.0-linux-nojvm.tar.bz2`, as downloaded from CIS, on a Windows workstation using WinRAR, then moved `ng_scoring_tool-1.0-linux.jar` over to the Linux server with WinSCP. Determine the java binary path and sequence your installation commands as follows, from the directory where you put `ng_scoring_tool-1.0-linux.jar`:

```
/usr/java/jdk1.5.0_09/jre/bin/java -jar ng_
scoring_tool-1.0-linux.jar –console
```

You will be prompted to read and accept an agreement, then prompted to choose the install path. The default of `/opt/CISngtool`, with Typical settings, should be acceptable. Note that it also creates an uninstaller for your use later, once you have completed your audit.

You may need to establish Java environment variables, depending on the account you are using and how you have installed the JRE. The easiest method is to do this:

Edit `vi .bash_profile` with these changes to the user's environment variables.

Add `:/usr/java/jre1.5.0_06/bin` to the PATH reference, add `JAVA_HOME=/usr/java/jre1.5.0_06` after the PATH reference, and

add `JAVA_HOME` to the export reference after PATH.

To complete the benchmark process execute

```
cd /opt/CISngtool
./ng.sh
```

Please select a benchmark from one of the following:

(1) *Redhat Linux Benchmark v1.0.5 August, 2006*

(2) *SuSE Linux Enterprise Server Benchmark v1.0*

Enter the benchmark # to use (1-2): 1

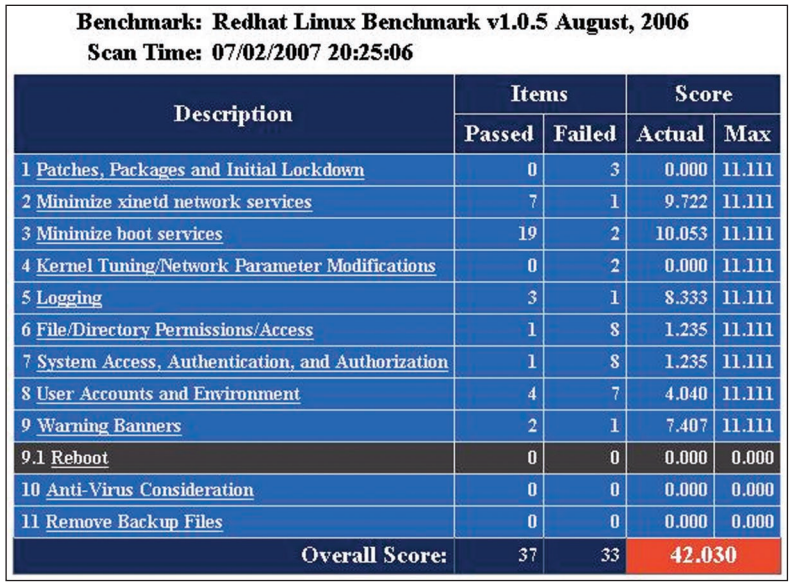
Executing '*Redhat Linux Benchmark v1.0.5 August, 2006*'

Processing completed.

XML results can be found in '`/opt/CISngtool/results/20070702202502496-0700`'.

HTML results can be found in '`/opt/CISngtool/results/20070702202502496-0700/reports/html`'.

Oh my, looks like there is some work to be done to harden this server.



**Benchmark: Redhat Linux Benchmark v1.0.5 August, 2006**
**Scan Time: 07/02/2007 20:25:06**

| Description | Items | | Score | |
|---|---|---|---|---|
| | Passed | Failed | Actual | Max |
| 1 Patches, Packages and Initial Lockdown | 0 | 3 | 0.000 | 11.111 |
| 2 Minimize xinetd network services | 7 | 1 | 9.722 | 11.111 |
| 3 Minimize boot services | 19 | 2 | 10.053 | 11.111 |
| 4 Kernel Tuning/Network Parameter Modifications | 0 | 2 | 0.000 | 11.111 |
| 5 Logging | 3 | 1 | 8.333 | 11.111 |
| 6 File/Directory Permissions/Access | 1 | 8 | 1.235 | 11.111 |
| 7 System Access, Authentication, and Authorization | 1 | 8 | 1.235 | 11.111 |
| 8 User Accounts and Environment | 4 | 7 | 4.040 | 11.111 |
| 9 Warning Banners | 2 | 1 | 7.407 | 11.111 |
| 9.1 Reboot | 0 | 0 | 0.000 | 0.000 |
| 10 Anti-Virus Consideration | 0 | 0 | 0.000 | 0.000 |
| 11 Remove Backup Files | 0 | 0 | 0.000 | 0.000 |
| Overall Score: | 37 | 33 | 42.030 | |

**Figure 2: Redhat Linux Benchmark Results**

4 http://nvd.nist.gov/xccdf.cfm

5 http://nvd.nist.gov/xccdf.cfm

As with all HTML NG Scoring Tool reports, each report heading is a URL link that will drill down into further details and remediation methodology useful to achieve compliance.

## Apache Level 1&2

To run the Apache benchmark, copy or download `cis_score_tool_apache_v2.0.8.sh.gz` to your Apache server (on Linux). The command sequence below may vary slightly for you and is dependent on where Apache is installed, as well as system defaults (they vary somewhat across distributions). In a root terminal, execute as follows:

```
gzip –d cis_score_tool_apache_v2.0.8.sh.gz
sh cis_score_tool_apache_v2.0.8.sh
```

You will be offered Terms of Use to which you have to agree, then it will decompress an `apache` directory in your working directory.

```
cd apache
chmod 700 benchmark.pl
./benchmark.pl –c /etc/apache/httpd.conf
```

Again you will be presented with questions, enter to continue, and answer correctly. Ideally, you can answer *yes* to questions like "Downloaded the Apache source and MD5 Checksums from httpd.apache.org?" or "Applied the current distribution patches?" Once complete, the scoring script will finish and you will be presented with findings.

After running the Apache scoring scripts against a server in my charge I discovered the file permissions were a bit lax.

Section 1.24 Update Ownership and Permissions for Enhanced Security

*[PASSED] Document Root "/var/www/htdocs" group is "root".*
*[PASSED] Owner of Document Root "/var/www/htdocs" is root.*
*[VERIFY] Log directory "/var/log/apache" group is properly set.*
***[FAILED] Permissions on Log directory "/var/log/apache" should be "664".***
*[PASSED] Owner of Log directory "/var/log/apache" is root.*
*[VERIFY] CGI directory "/var/www/cgi-bin/" group is properly set.*
***[FAILED] Permissions on CGI directory "/var/www/cgi-bin/" should be "555".***
*[PASSED] Owner of CGI directory "/var/www/cgi-bin/" is root.*
*[VERIFY] Server Bin directory "/usr/bin/" group is properly set.*
***[FAILED] Permissions on Server Bin directory "/usr/bin/" should be "550".***
*[PASSED] Owner of Server Bin directory "/usr/bin/" is root.*

To remediate, as *root*, I executed `chmod 664 /var/log/apache`, `chmod 555 /var/www/cgi-bin/`, and `chmod 550 /usr/bin/`. I then ran benchmark.pl again and voila.

*Section 1.24 Update Ownership and Permissions for Enhanced Security*

*[PASSED] Owner of Server Conf directory "/usr/conf/" is root.*
*[VERIFY] Server Conf directory "/usr/conf/" group is properly set.*
*[PASSED] Document Root "/var/www/htdocs" group is "root".*
*[PASSED] Owner of Document Root "/var/www/htdocs" is root.*
*[VERIFY] Log directory "/var/log/apache" group is properly set.*
***[PASSED] Permissions on Log directory "/var/log/apache" set to "664".***
*[PASSED] Owner of Log directory "/var/log/apache" is root.*
*[VERIFY] CGI directory "/var/www/cgi-bin/" group is properly set.*
***[PASSED] Permissions on CGI directory "/var/www/cgi-bin/" set to "555".***
*[PASSED] Owner of CGI directory "/var/www/cgi-bin/" is root.*
*[VERIFY] Server Bin directory "/usr/bin/" group is properly set.*
***[PASSED] Permissions on Server Bin directory "/usr/bin/" set to "550".***
*[PASSED] Owner of Server Bin directory "/usr/bin/" is root.*

As with the Windows Server 2003 results, you will be offered more than enough information to harden your Apache installation, and the CIS Apache Benchmark PDF is included in the apache directory after you uncompress `cis_score_tool_apache_v2.0.8.sh.gz`.

## Benefits and drawbacks

Anyone with adequate systems administration skills will find these benchmarks easy to run. Security administrators and engineer will find them essential to run. The only drawback I have ever identified in running these benchmarks against a system is the simple fact that I can not resist then immediately hardening it in an effort to improve its score. It is downright addictive for systems geeks. This can consume hours of your time, lots of coffee, and a good deal of testing to ensure that you do not tune a system right out of a useful state. The bonus is, even if you deploy the recommended improvements in small steps, every step you take will improve the system's security posture.

The benchmarks are free, time and effort to remediate are your only real costs to use these tools.

## In conclusion

The CIS Benchmarks are tools that will bring you immediate, verifiable benefit, serving only to improve your Internet stance and perhaps lend to a little more sleep. No matter what system you run the scoring tools against, or harden using a benchmark as reference, you will ensure a better, more secure system.

Go forth and propagate secure systems.

Cheers..until next month.

## About the Author

*Russ McRee, GCIH, CISSP, is a security analyst working for Expedia. He is a member of numerous security organizations and maintains holisticinfosec.org. Contact him at russ@holisticinfosec.org.*