CIS NG Scoring Tool and Dashboard

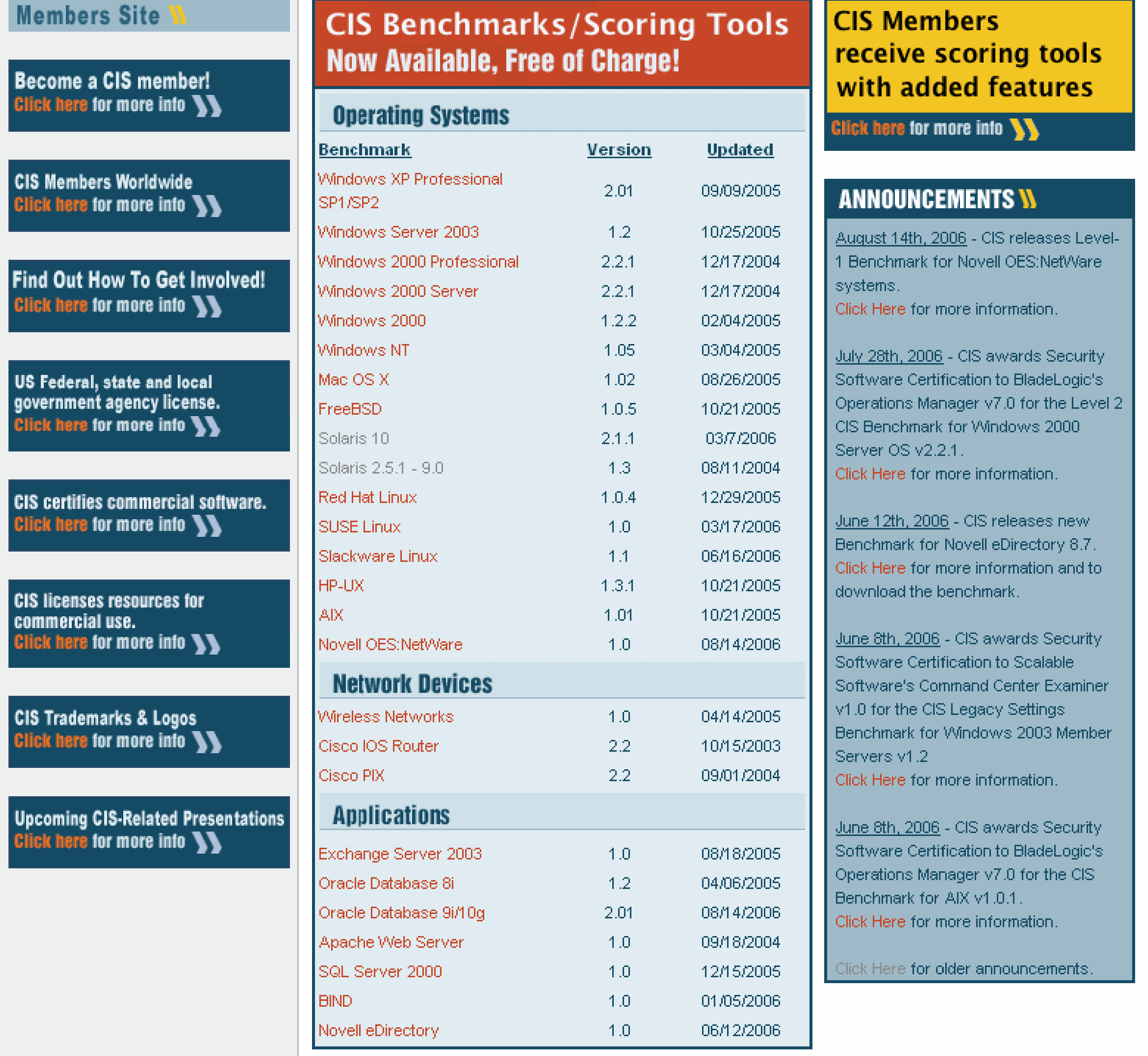
Dave Waltermire

Clint Kreitner

the CENTER for INTERNET SECURITY

Questions we're often asked about XCCDF

- What technical expertise is needed to create and modify configuration benchmarks in XCCDF?
- Is an XCCDF editor available?
- What human readable formats can an XCCDF benchmark be translated into?
- Does XCCDF help tool vendors?



Become a CIS member!
Click here for more info

CIS Members Worldwide
Click here for more info

Find Out How To Get Involved!
Click here for more info

US Federal, state and local government agency license.
Click here for more info

CIS certifies commercial software.
Click here for more info

CIS licenses resources for commercial use.
Click here for more info

CIS Trademarks & Logos
Click here for more info

Upcoming CIS-Related Presentations
Click here for more info

CIS Benchmarks/Scoring Tools Now Available, Free of Charge!

Operating Systems

Benchmark	Version	Updated
Windows XP Professional SP1/SP2	2.01	09/09/2005
Windows Server 2003	1.2	10/25/2005
Windows 2000 Professional	2.2.1	12/17/2004
Windows 2000 Server	2.2.1	12/17/2004
Windows 2000	1.2.2	02/04/2005
Windows NT	1.05	03/04/2005
Mac OS X	1.02	08/26/2005
FreeBSD	1.0.5	10/21/2005
Solaris 10	2.1.1	03/7/2006
Solaris 2.5.1 - 9.0	1.3	08/11/2004
Red Hat Linux	1.0.4	12/29/2005
SUSE Linux	1.0	03/17/2006
Slackware Linux	1.1	06/16/2006
HP-UX	1.3.1	10/21/2005
AIX	1.01	10/21/2005
Novell OES:NetWare	1.0	08/14/2006

Network Devices

Benchmark	Version	Updated
Wireless Networks	1.0	04/14/2005
Cisco IOS Router	2.2	10/15/2003
Cisco PIX	2.2	09/01/2004

Applications

Benchmark	Version	Updated
Exchange Server 2003	1.0	08/18/2005
Oracle Database 8i	1.2	04/06/2005
Oracle Database 9i/10g	2.01	08/14/2006
Apache Web Server	1.0	09/18/2004
SQL Server 2000	1.0	12/15/2005
BIND	1.0	01/05/2006
Novell eDirectory	1.0	06/12/2006

CIS Members receive scoring tools with added features
Click here for more info

ANNOUNCEMENTS

August 14th, 2006 - CIS releases Level-1 Benchmark for Novell OES:NetWare systems.
Click Here for more information.

July 28th, 2006 - CIS awards Security Software Certification to BladeLogic's Operations Manager v7.0 for the Level 2 CIS Benchmark for Windows 2000 Server OS v2.2.1.
Click Here for more information.

June 12th, 2006 - CIS releases new Benchmark for Novell eDirectory 8.7.
Click Here for more information and to download the benchmark.

June 8th, 2006 - CIS awards Security Software Certification to Scalable Software's Command Center Examiner v1.0 for the CIS Legacy Settings Benchmark for Windows 2003 Member Servers v1.2
Click Here for more information.

June 8th, 2006 - CIS awards Security Software Certification to BladeLogic's Operations Manager v7.0 for the CIS Benchmark for AIX v1.0.1.
Click Here for more information.

Click Here for older announcements.

the CENTER for
INTERNET SECURITY

Windows XP Professional

Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Baseline Security Settings

Version 2.01
August, 2005

http://www.cisecurity.org

Editors: Jeff Shawgo
Sidney Faber
Nancy Whitney
windows-feedback@lists.cisecurity.org

Setting:	Legacy	Enterprise		Specialized Security – Limited Functionality
		Desktop	Mobile	
2.2.1.9 Audit System Events	Success (minimum)			
2.2.2 Account Policy				
2.2.2.1 Minimum Password Age	1 day			
2.2.2.2 Maximum Password Age	90 days			
2.2.2.3 Minimum Password Length	8 characters			12 characters
2.2.2.4 Password Complexity	Enabled			
2.2.2.5 Password History	24 passwords remembered			
2.2.2.6 Store Passwords using Reversible Encryption	Disabled			
2.2.3 Account Lockout Policy				
2.2.3.1 Account Lockout Duration	15 minutes			15 minutes
2.2.3.2 Account Lockout Threshold	50 attempts			10 attempts
2.2.3.3 Reset Account Lockout After	15 minutes			15 minutes
2.2.4 Event Log Settings – Application, Security, and System Logs				
2.2.4.1 Application Log				
2.2.4.1.1 Maximum Event Log Size	16 MB			
2.2.4.1.2 Restrict Guest Access	Enabled			
2.2.4.1.3 Log Retention Method	As Needed			
2.2.4.1.4 Log Retention	<Not Defined>			
2.2.4.2 Security Log				
2.2.4.2.1 Maximum Event Log Size	80 MB			
2.2.4.2.2 Restrict Guest	Enabled			

How the consensus benchmark process works

- Teams are formed with security experts from public and private sector organizations
- A consensus benchmark draft is developed via email and conference call discussion
- A scoring tool is developed
- Both are made available free to all users globally via the CIS website

  (http://www.cisecurity.org)

Scoring tools are used to:

- Harden systems before putting them into operation
- Monitor compliance with organizational policies
- Document FISMA compliance
- Support the audit process

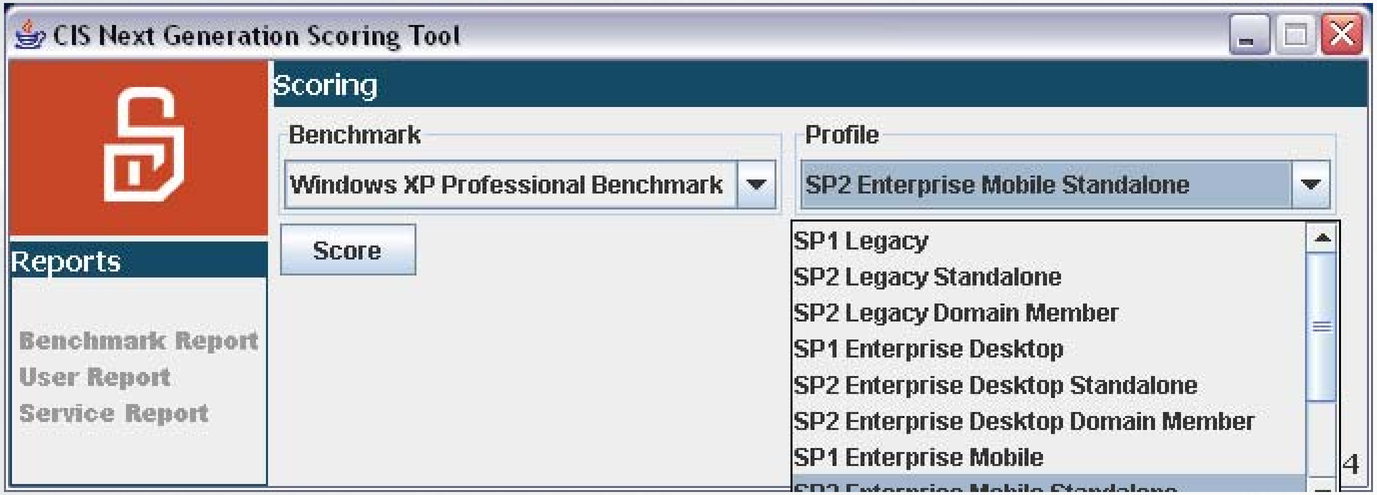
CIS NG Scoring Tool

- The reference implementation for XCCDF and OVAL
- Scores actual configuration of systems against appropriate benchmark standard (0 to 100)
- GUI version
- Command line version

NG Tool History and Usage

- GUI & CLI NG Tool for Windows (2000, XP, Server 2003) released Sept 2005
  - 34,233 downloads in 2005
  - 42,041 downloads Jan-Jun 2006
- CLI NG Tool for Solaris 10 released March 2006
  - 6721 downloads Jan-Jun 2006

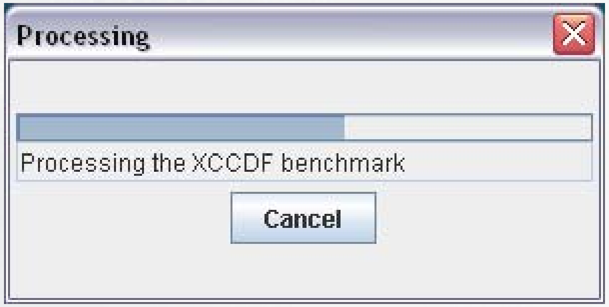
GUI Mode



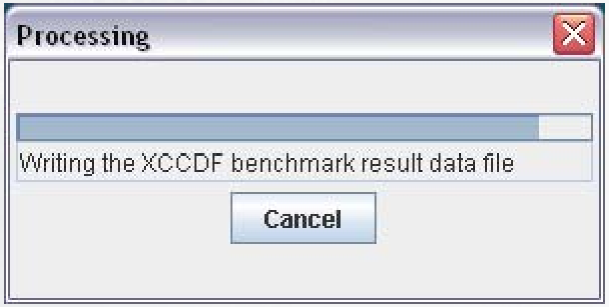
Benchmark: Windows XP Professional Benchmark

Profile: SP2 Enterprise Mobile Standalone

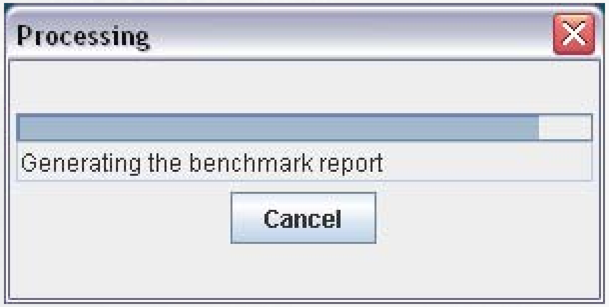
- SP1 Legacy
- SP2 Legacy Standalone
- SP2 Legacy Domain Member
- SP1 Enterprise Desktop
- SP2 Enterprise Desktop Standalone
- SP2 Enterprise Desktop Domain Member
- SP1 Enterprise Mobile
- SP2 Enterprise Mobile Standalone



Processing the XCCDF benchmark

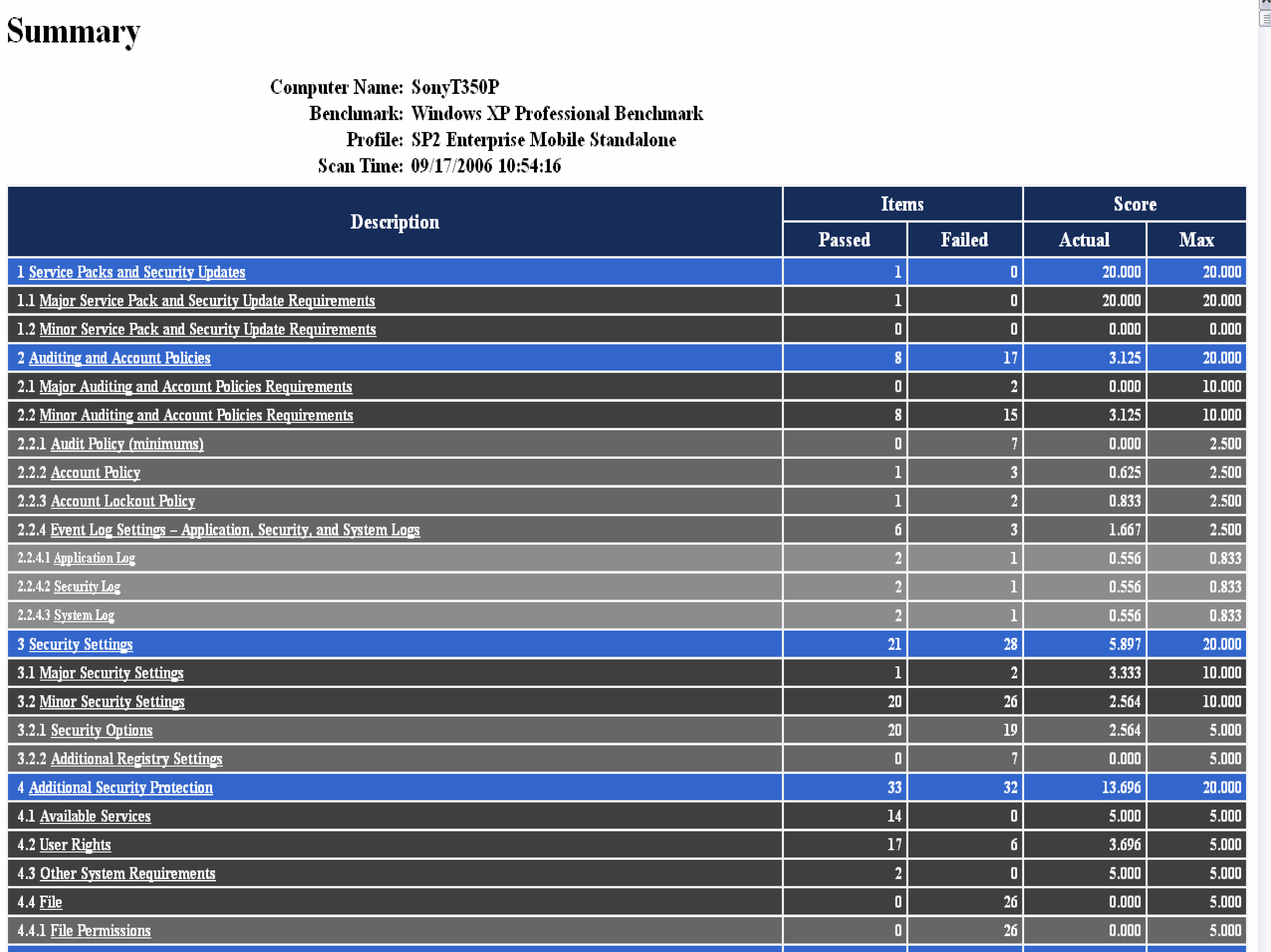


Writing the XCCDF benchmark result data file



Processing

Generating the benchmark report

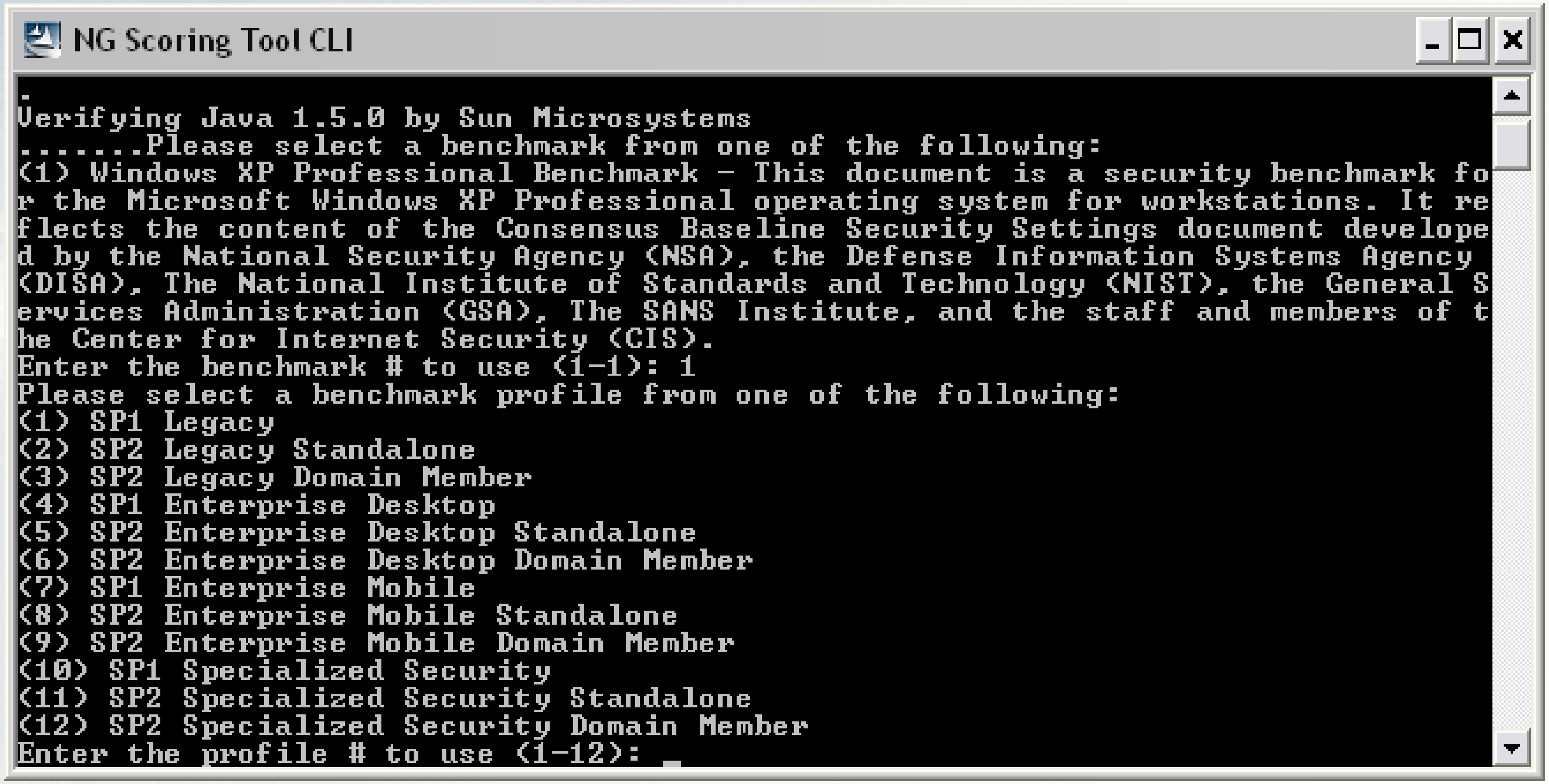


Summary

Computer Name: SonyT350P
Benchmark: Windows XP Professional Benchmark
Profile: SP2 Enterprise Mobile Standalone
Scan Time: 09/17/2006 10:54:16

Description	Items		Score	
	Passed	Failed	Actual	Max
1 Service Packs and Security Updates	1	0	20.000	20.000
1.1 Major Service Pack and Security Update Requirements	1	0	20.000	20.000
1.2 Minor Service Pack and Security Update Requirements	0	0	0.000	0.000
2 Auditing and Account Policies	8	17	3.125	20.000
2.1 Major Auditing and Account Policies Requirements	0	2	0.000	10.000
2.2 Minor Auditing and Account Policies Requirements	8	15	3.125	10.000
2.2.1 Audit Policy (minimums)	0	7	0.000	2.500
2.2.2 Account Policy	1	3	0.625	2.500
2.2.3 Account Lockout Policy	1	2	0.833	2.500
2.2.4 Event Log Settings – Application, Security, and System Logs	6	3	1.667	2.500
2.2.4.1 Application Log	2	1	0.556	0.833
2.2.4.2 Security Log	2	1	0.556	0.833
2.2.4.3 System Log	2	1	0.556	0.833
3 Security Settings	21	28	5.897	20.000
3.1 Major Security Settings	1	2	3.333	10.000
3.2 Minor Security Settings	20	26	2.564	10.000
3.2.1 Security Options	20	19	2.564	5.000
3.2.2 Additional Registry Settings	0	7	0.000	5.000
4 Additional Security Protection	33	32	13.696	20.000
4.1 Available Services	14	0	5.000	5.000
4.2 User Rights	17	6	3.696	5.000
4.3 Other System Requirements	2	0	5.000	5.000
4.4 File	0	26	0.000	5.000
4.4.1 File Permissions	0	26	0.000	5.000

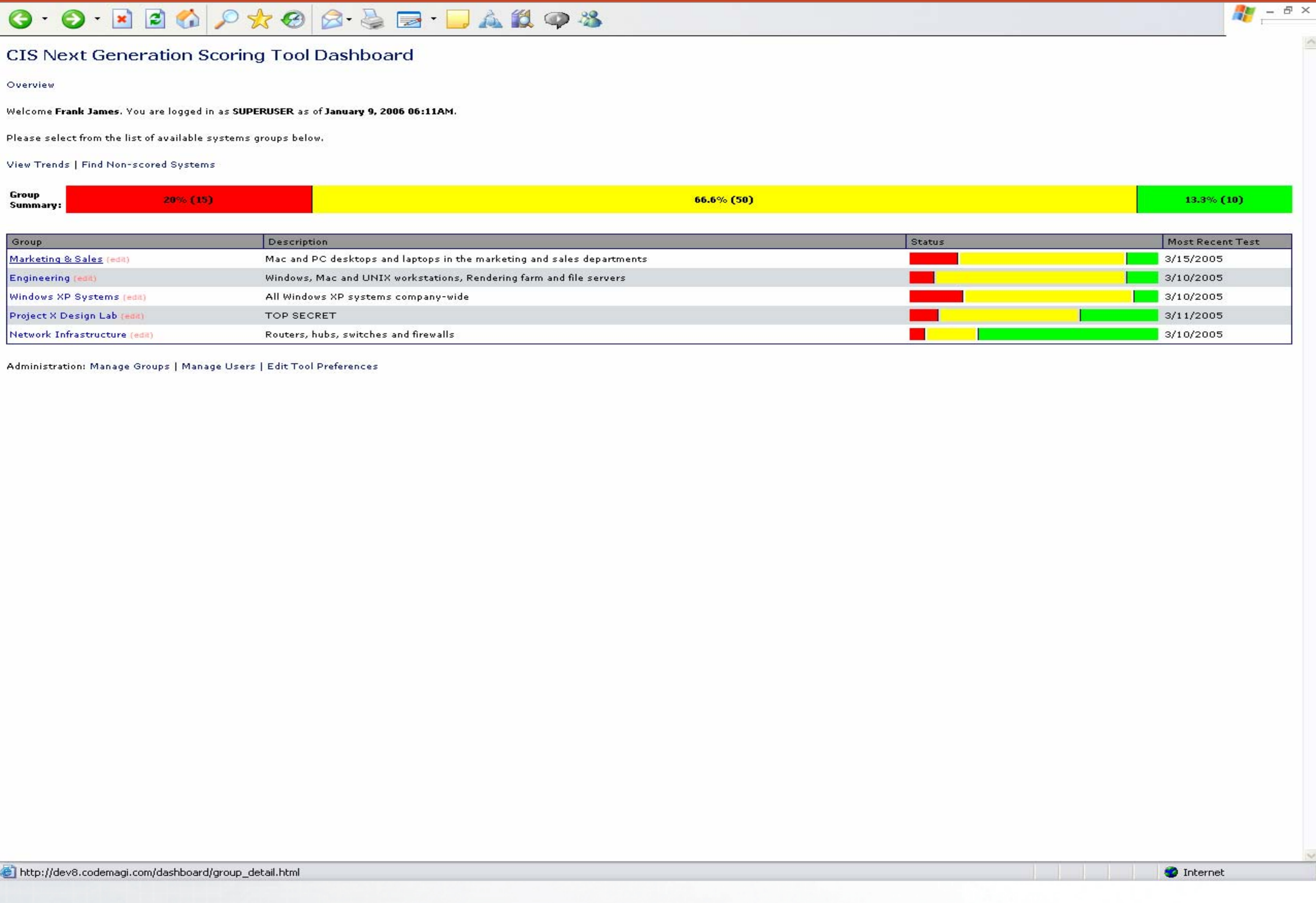
Command Line Mode with the CIS Dashboard



```
.
Verifying Java 1.5.0 by Sun Microsystems
.......Please select a benchmark from one of the following:
(1) Windows XP Professional Benchmark - This document is a security benchmark fo
r the Microsoft Windows XP Professional operating system for workstations. It re
flects the content of the Consensus Baseline Security Settings document develope
d by the National Security Agency (NSA), the Defense Information Systems Agency
(DISA), The National Institute of Standards and Technology (NIST), the General S
ervices Administration (GSA), The SANS Institute, and the staff and members of t
he Center for Internet Security (CIS).
Enter the benchmark # to use (1-1): 1
Please select a benchmark profile from one of the following:
(1) SP1 Legacy
(2) SP2 Legacy Standalone
(3) SP2 Legacy Domain Member
(4) SP1 Enterprise Desktop
(5) SP2 Enterprise Desktop Standalone
(6) SP2 Enterprise Desktop Domain Member
(7) SP1 Enterprise Mobile
(8) SP2 Enterprise Mobile Standalone
(9) SP2 Enterprise Mobile Domain Member
(10) SP1 Specialized Security
(11) SP2 Specialized Security Standalone
(12) SP2 Specialized Security Domain Member
Enter the profile # to use (1-12): _
```

CIS Dashboard

- Configuration status of systems via red-yellow-green displays
  - Reports extent of compliance with benchmark standards
    - For various organizational divisions or sub-net hosts
    - Reveals trends over time
- Aids FISMA reporting of configuration status
  - Regular and ad-hoc reports from SQL database



CIS Next Generation Scoring Tool Dashboard

Overview

Welcome **Frank James**. You are logged in as **SUPERUSER** as of **January 9, 2006 06:11AM**.

Please select from the list of available systems groups below.

View Trends | Find Non-scored Systems

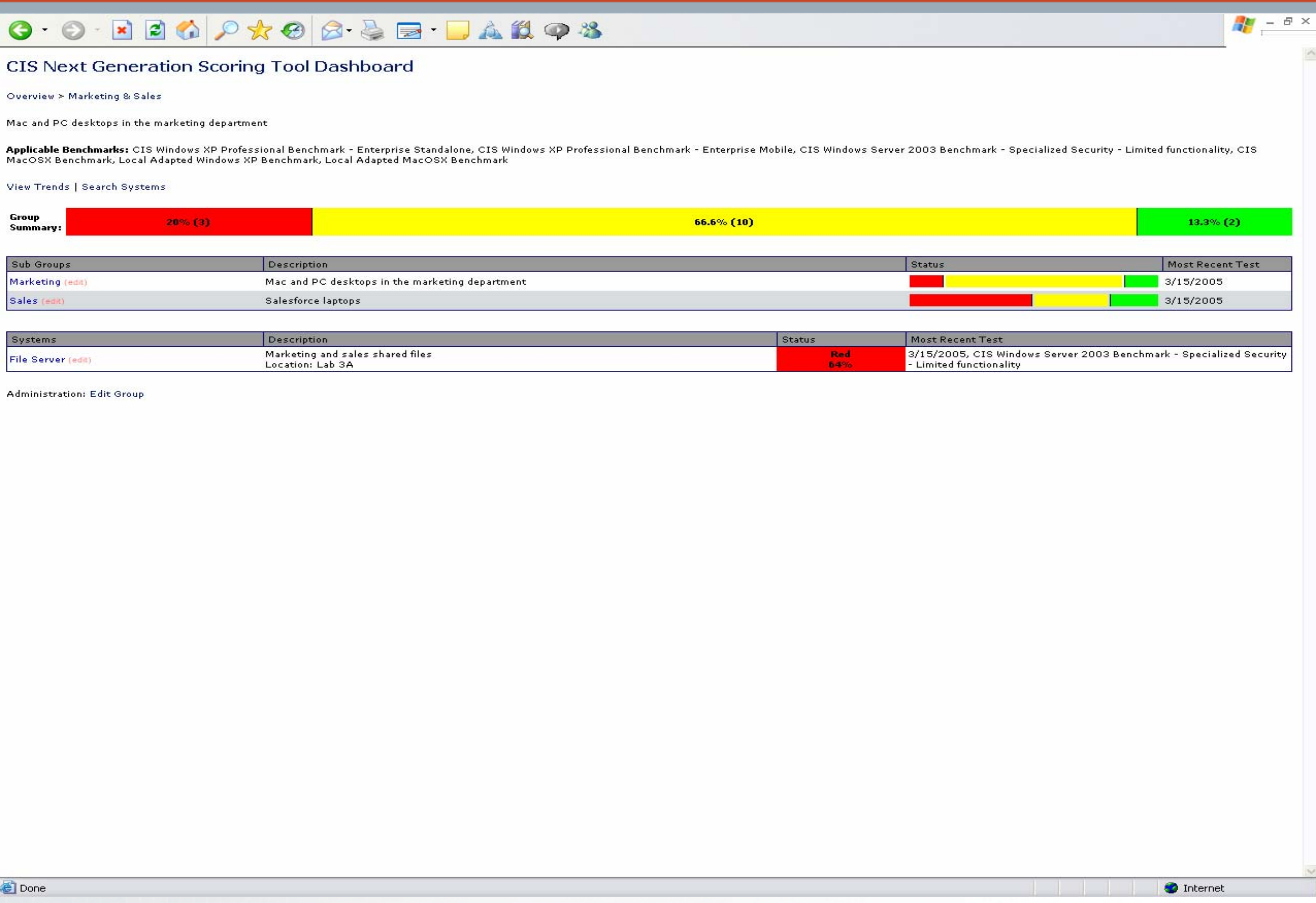
Group Summary:	🟥 20% (15)	🟨 66.6% (50)	🟩 13.3% (10)

Group	Description	Status	Most Recent Test
Marketing & Sales (edit)	Mac and PC desktops and laptops in the marketing and sales departments	🟥🟨🟩	3/15/2005
Engineering (edit)	Windows, Mac and UNIX workstations, Rendering farm and file servers	🟥🟨🟩	3/10/2005
Windows XP Systems (edit)	All Windows XP systems company-wide	🟥🟨🟩	3/10/2005
Project X Design Lab (edit)	TOP SECRET	🟥🟨🟩	3/11/2005
Network Infrastructure (edit)	Routers, hubs, switches and firewalls	🟥🟨🟩	3/10/2005

Administration: Manage Groups | Manage Users | Edit Tool Preferences

http://dev8.codemagi.com/dashboard/group_detail.html

Internet



CIS Next Generation Scoring Tool Dashboard

Overview > Marketing & Sales

Mac and PC desktops in the marketing department

Applicable Benchmarks: CIS Windows XP Professional Benchmark - Enterprise Standalone, CIS Windows XP Professional Benchmark - Enterprise Mobile, CIS Windows Server 2003 Benchmark - Specialized Security - Limited functionality, CIS MacOSX Benchmark, Local Adapted Windows XP Benchmark, Local Adapted MacOSX Benchmark

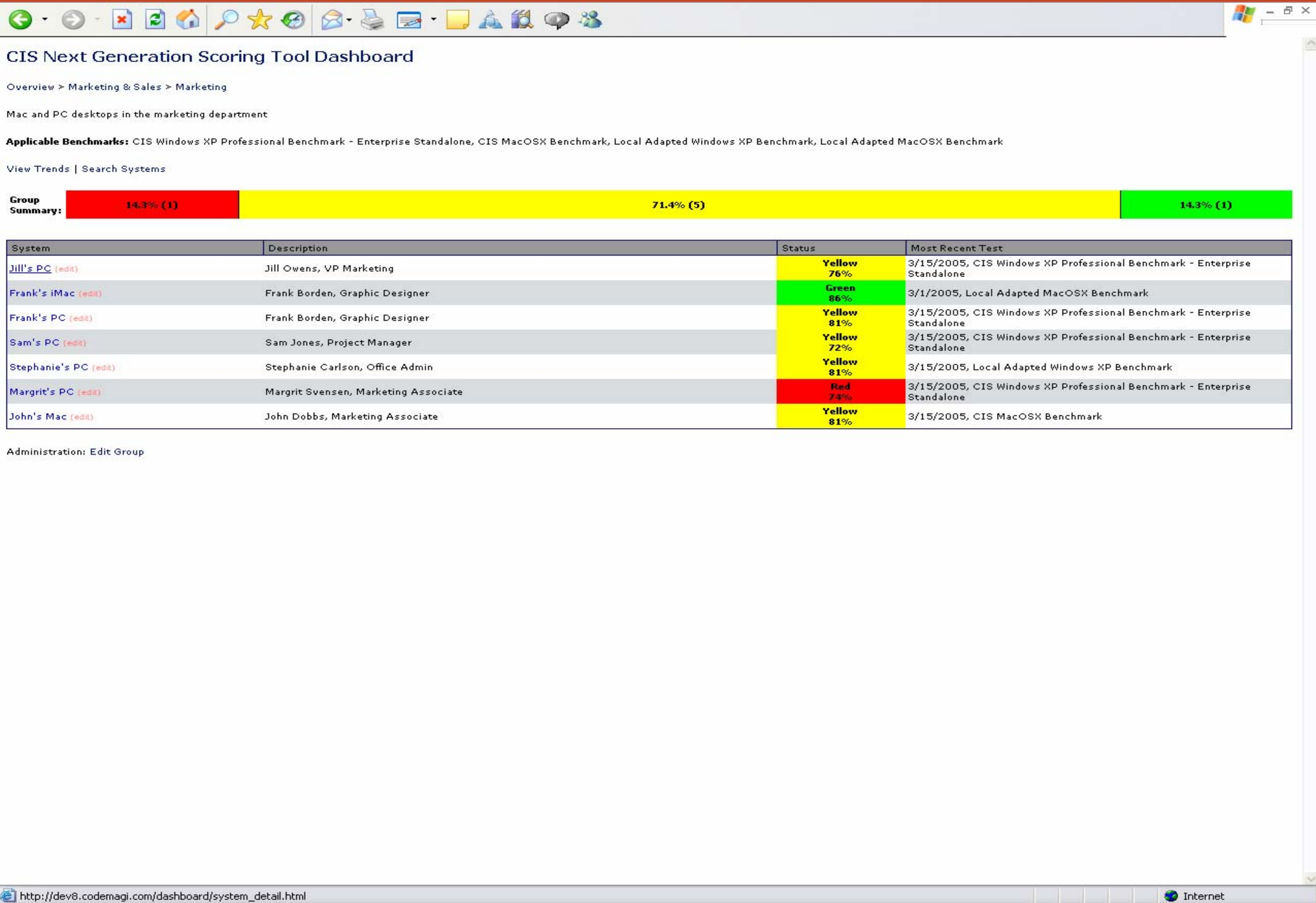
View Trends | Search Systems

Group Summary:	🟥 20% (3)	🟨 66.6% (10)	🟩 13.3% (2)

Sub Groups	Description	Status	Most Recent Test
Marketing (edit)	Mac and PC desktops in the marketing department	🟥🟨🟩	3/15/2005
Sales (edit)	Salesforce laptops	🟥🟨🟩	3/15/2005

Systems	Description	Status	Most Recent Test
File Server (edit)	Marketing and sales shared files Location: Lab 3A	Red 64%	3/15/2005, CIS Windows Server 2003 Benchmark - Specialized Security - Limited functionality

Administration: Edit Group



CIS Next Generation Scoring Tool Dashboard

Overview > Marketing & Sales > Marketing

Mac and PC desktops in the marketing department

Applicable Benchmarks: CIS Windows XP Professional Benchmark - Enterprise Standalone, CIS MacOSX Benchmark, Local Adapted Windows XP Benchmark, Local Adapted MacOSX Benchmark

View Trends | Search Systems

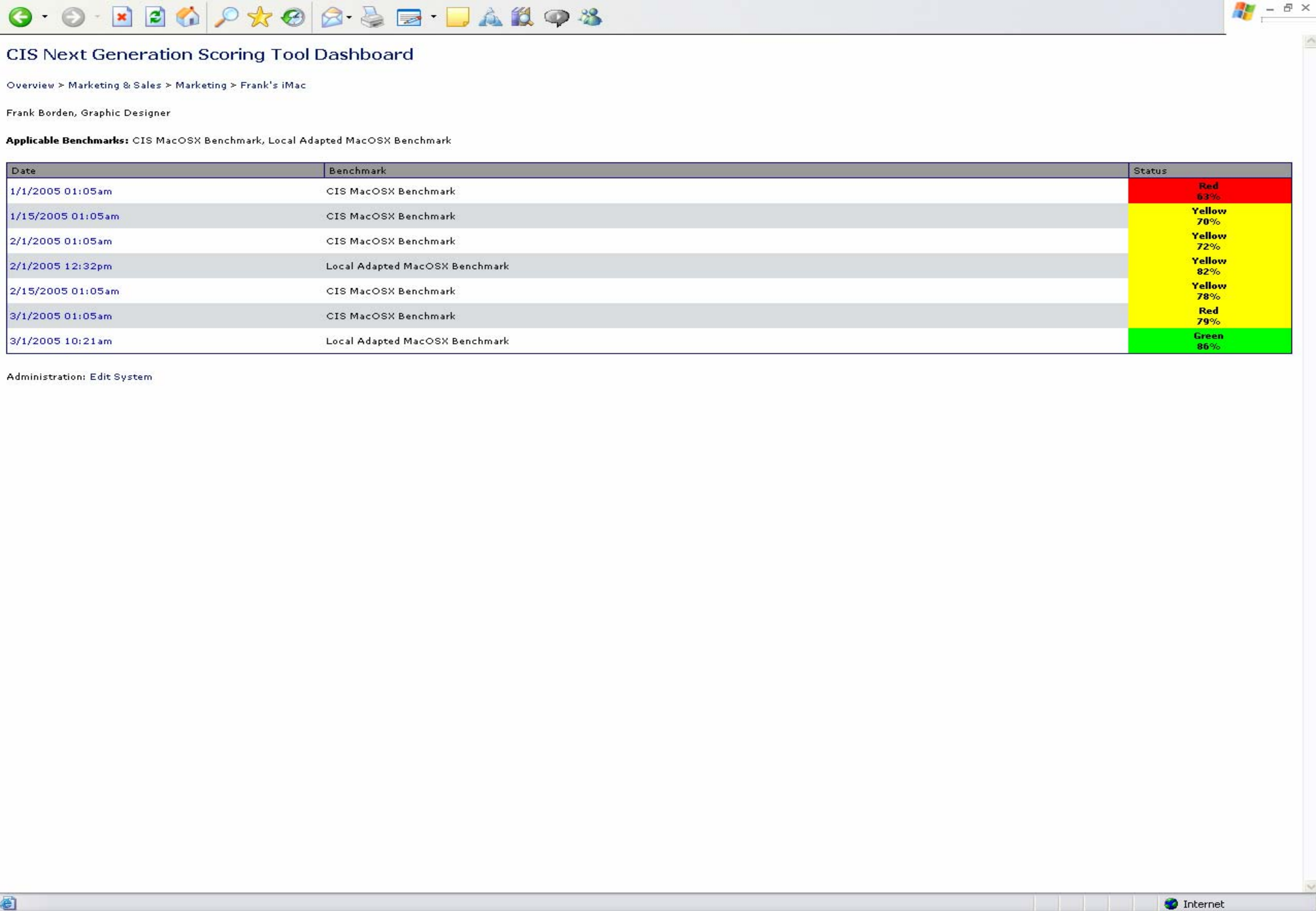
Group Summary:	🟥 14.3% (1)	🟨 71.4% (5)	🟩 14.3% (1)

System	Description	Status	Most Recent Test
Jill's PC (edit)	Jill Owens, VP Marketing	Yellow 76%	3/15/2005, CIS Windows XP Professional Benchmark - Enterprise Standalone
Frank's iMac (edit)	Frank Borden, Graphic Designer	Green 86%	3/1/2005, Local Adapted MacOSX Benchmark
Frank's PC (edit)	Frank Borden, Graphic Designer	Yellow 81%	3/15/2005, CIS Windows XP Professional Benchmark - Enterprise Standalone
Sam's PC (edit)	Sam Jones, Project Manager	Yellow 72%	3/15/2005, CIS Windows XP Professional Benchmark - Enterprise Standalone
Stephanie's PC (edit)	Stephanie Carlson, Office Admin	Yellow 81%	3/15/2005, Local Adapted Windows XP Benchmark
Margrit's PC (edit)	Margrit Svensen, Marketing Associate	Red 74%	3/15/2005, CIS Windows XP Professional Benchmark - Enterprise Standalone
John's Mac (edit)	John Dobbs, Marketing Associate	Yellow 81%	3/15/2005, CIS MacOSX Benchmark

Administration: Edit Group

http://dev8.codemagi.com/dashboard/system_detail.html

the CENTER for
INTERNET SECURITY



CIS Next Generation Scoring Tool Dashboard

Overview > Marketing & Sales > Marketing > Frank's iMac

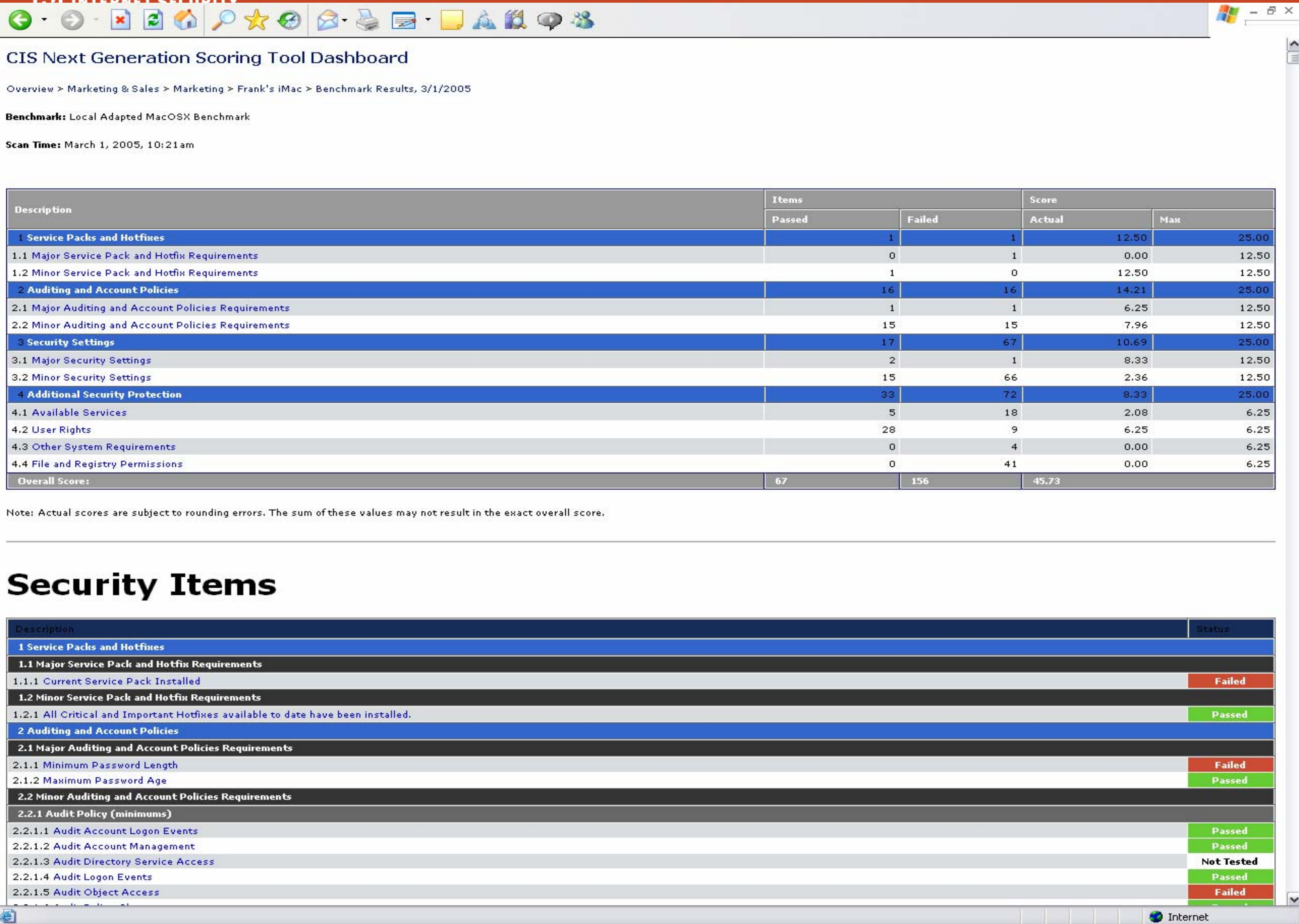
Frank Borden, Graphic Designer

Applicable Benchmarks: CIS MacOSX Benchmark, Local Adapted MacOSX Benchmark

Date	Benchmark	Status
1/1/2005 01:05am	CIS MacOSX Benchmark	**Red** **63%**
1/15/2005 01:05am	CIS MacOSX Benchmark	**Yellow** **70%**
2/1/2005 01:05am	CIS MacOSX Benchmark	**Yellow** **72%**
2/1/2005 12:32pm	Local Adapted MacOSX Benchmark	**Yellow** **82%**
2/15/2005 01:05am	CIS MacOSX Benchmark	**Yellow** **78%**
3/1/2005 01:05am	CIS MacOSX Benchmark	**Red** **79%**
3/1/2005 10:21am	Local Adapted MacOSX Benchmark	**Green** **86%**

Administration: Edit System

the CENTER for INTERNET SECURITY



CIS Next Generation Scoring Tool Dashboard

Overview > Marketing & Sales > Marketing > Frank's iMac > Benchmark Results, 3/1/2005

Benchmark: Local Adapted MacOSX Benchmark

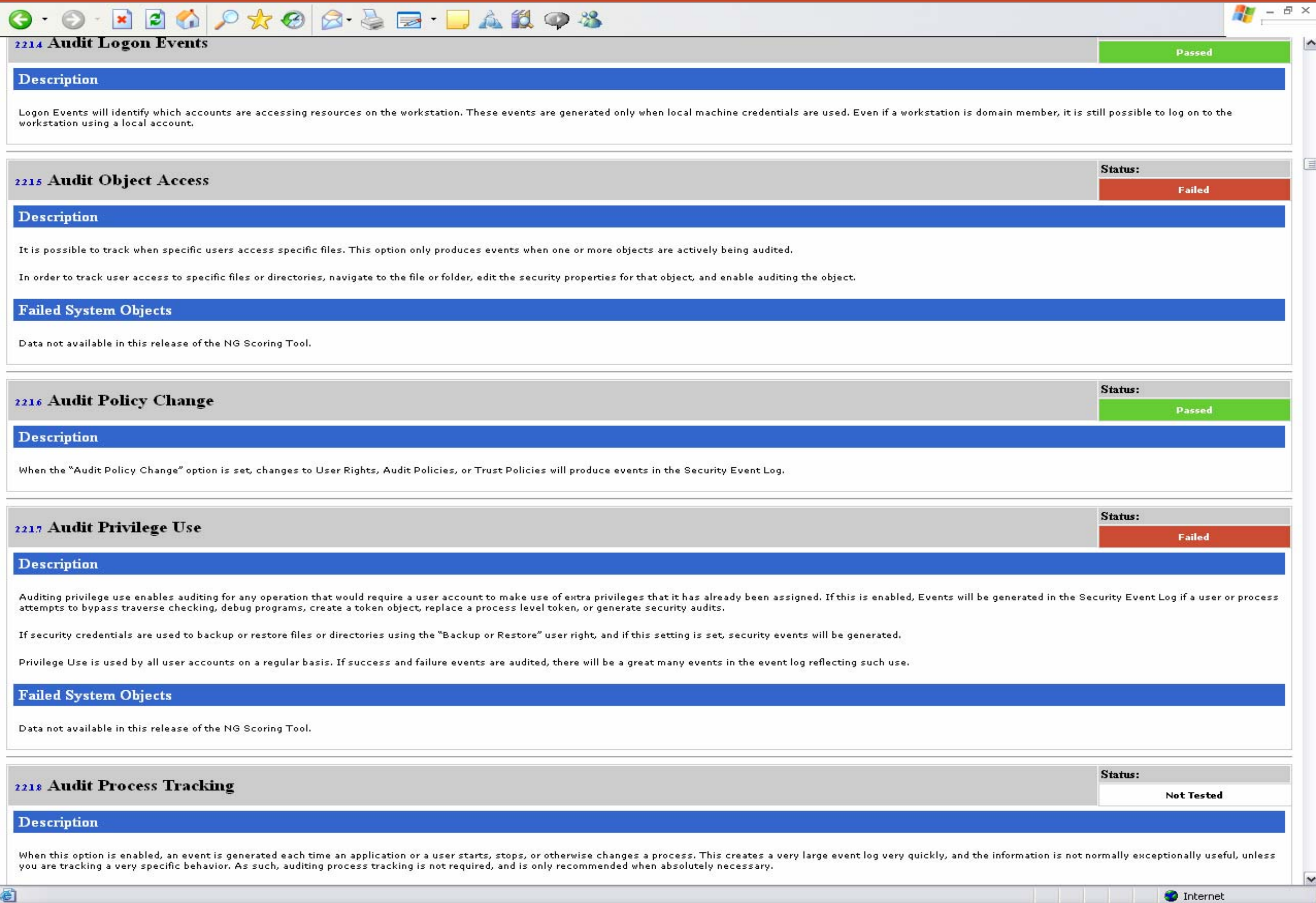
Scan Time: March 1, 2005, 10:21am

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	16	16	14.21	25.00
2.1 Major Auditing and Account Policies Requirements	1	1	6.25	12.50
2.2 Minor Auditing and Account Policies Requirements	15	15	7.96	12.50
3 Security Settings	17	67	10.69	25.00
3.1 Major Security Settings	2	1	8.33	12.50
3.2 Minor Security Settings	15	66	2.36	12.50
4 Additional Security Protection	33	72	8.33	25.00
4.1 Available Services	5	18	2.08	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:	67	156	45.73	

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

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.	Passed
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	Passed
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



2214 Audit Logon Events

Passed

Description

Logon Events will identify which accounts are accessing resources on the workstation. These events are generated only when local machine credentials are used. Even if a workstation is domain member, it is still possible to log on to the workstation using a local account.

2215 Audit Object Access

Status:

Failed

Description

It is possible to track when specific users access specific files. This option only produces events when one or more objects are actively being audited.

In order to track user access to specific files or directories, navigate to the file or folder, edit the security properties for that object, and enable auditing the object.

Failed System Objects

Data not available in this release of the NG Scoring Tool.

2216 Audit Policy Change

Status:

Passed

Description

When the "Audit Policy Change" option is set, changes to User Rights, Audit Policies, or Trust Policies will produce events in the Security Event Log.

2217 Audit Privilege Use

Status:

Failed

Description

Auditing privilege use enables auditing for any operation that would require a user account to make use of extra privileges that it has already been assigned. If this is enabled, Events will be generated in the Security Event Log if a user or process attempts to bypass traverse checking, debug programs, create a token object, replace a process level token, or generate security audits.

If security credentials are used to backup or restore files or directories using the "Backup or Restore" user right, and if this setting is set, security events will be generated.

Privilege Use is used by all user accounts on a regular basis. If success and failure events are audited, there will be a great many events in the event log reflecting such use.

Failed System Objects

Data not available in this release of the NG Scoring Tool.

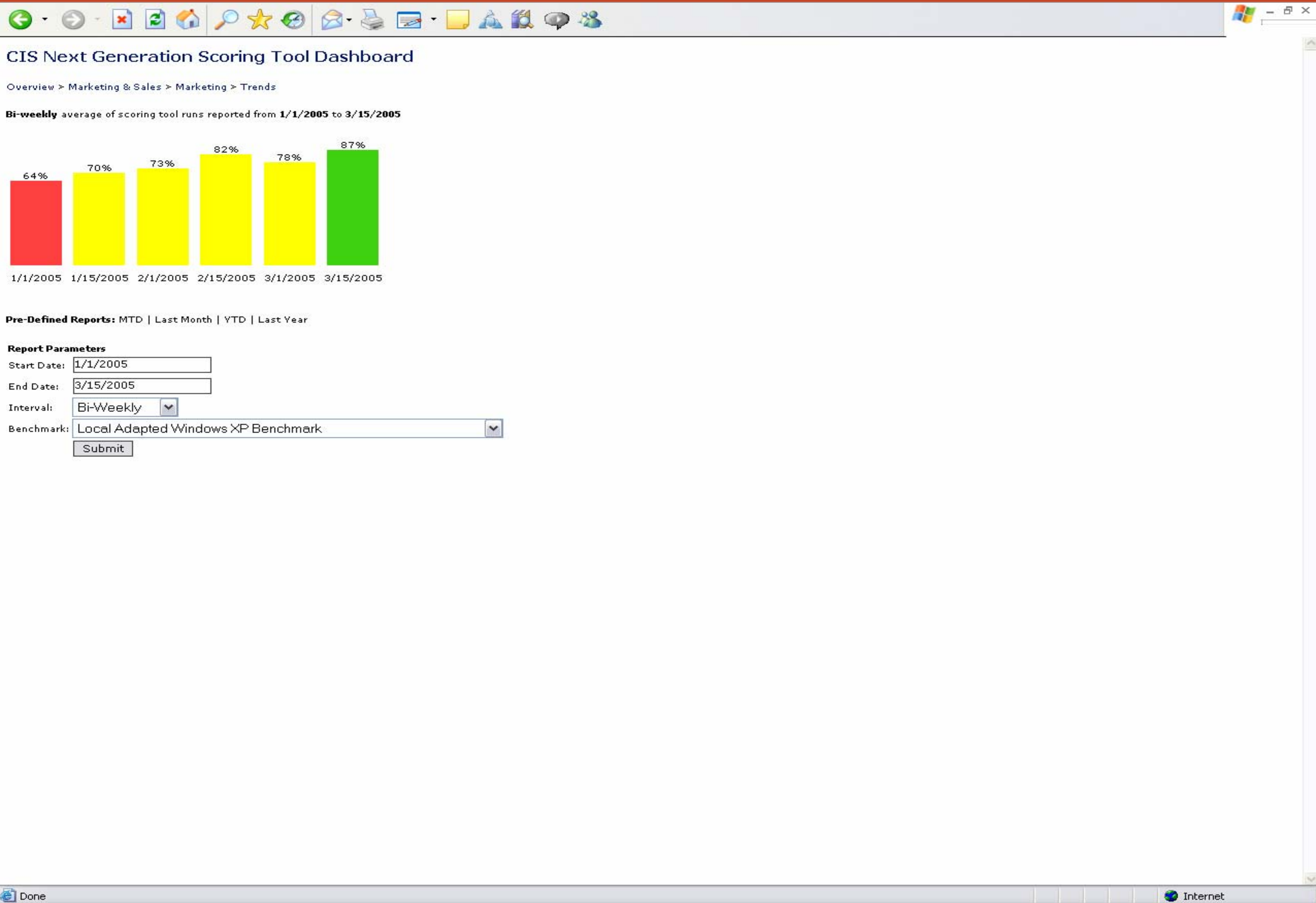
2218 Audit Process Tracking

Status:

Not Tested

Description

When this option is enabled, an event is generated each time an application or a user starts, stops, or otherwise changes a process. This creates a very large event log very quickly, and the information is not normally exceptionally useful, unless you are tracking a very specific behavior. As such, auditing process tracking is not required, and is only recommended when absolutely necessary.



CIS Next Generation Scoring Tool Dashboard

Overview > Marketing & Sales > Marketing > Trends

Bi-weekly average of scoring tool runs reported from **1/1/2005** to **3/15/2005**

Pre-Defined Reports: MTD | Last Month | YTD | Last Year

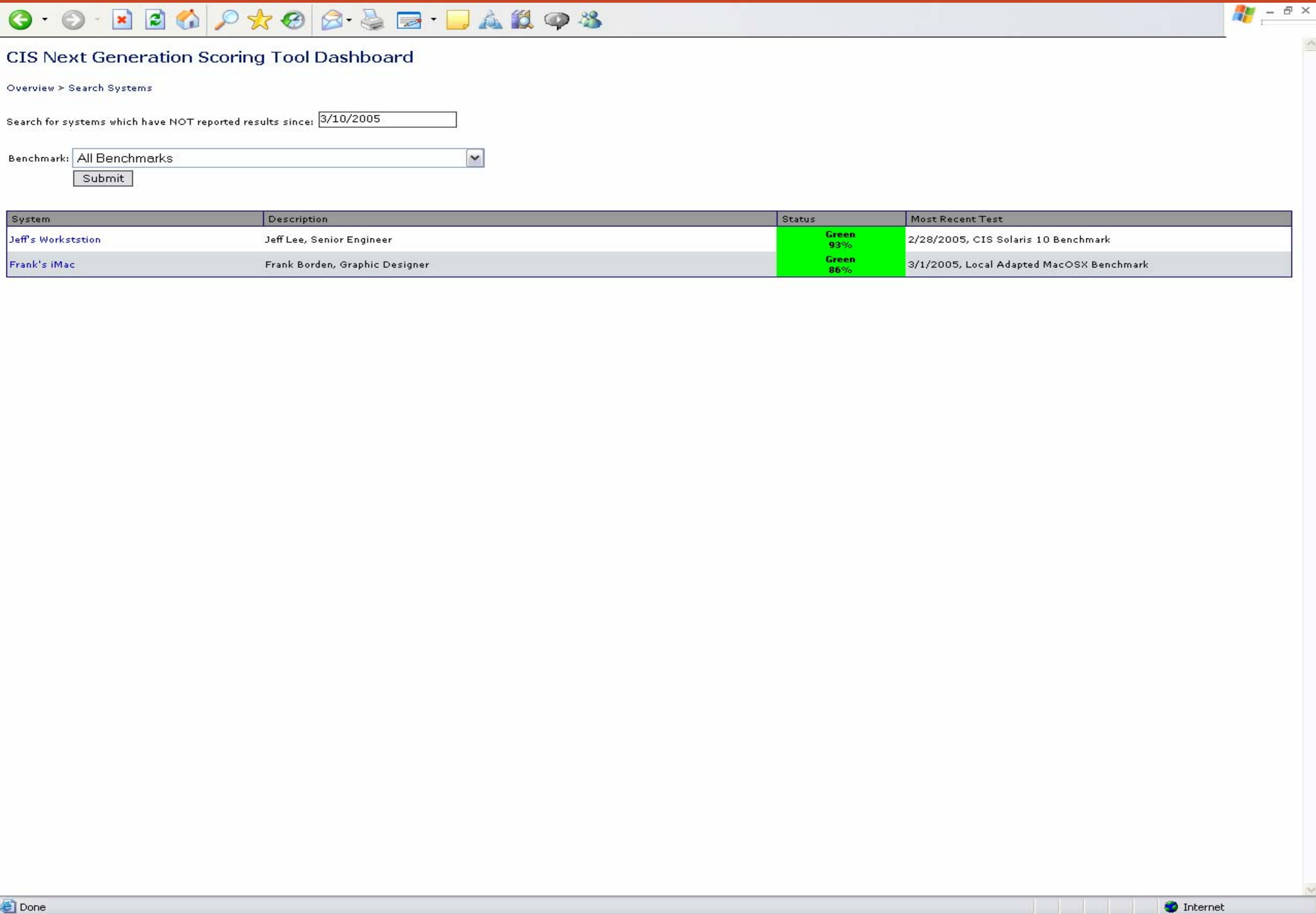
Report Parameters

Start Date: 1/1/2005

End Date: 3/15/2005

Interval: Bi-Weekly

Benchmark: Local Adapted Windows XP Benchmark



CIS Next Generation Scoring Tool Dashboard

Overview > Search Systems

Search for systems which have NOT reported results since: 3/10/2005

Benchmark: All Benchmarks

System	Description	Status	Most Recent Test
Jeff's Workststion	Jeff Lee, Senior Engineer	Green 93%	2/28/2005, CIS Solaris 10 Benchmark
Frank's iMac	Frank Borden, Graphic Designer	Green 86%	3/1/2005, Local Adapted MacOSX Benchmark

Questions we're often asked about XCCDF

- What technical expertise is needed to create and modify configuration benchmarks in XCCDF?
- Is an XCCDF editor available?
- What human readable formats can an XCCDF benchmark be translated into?
- Does XCCDF help tool vendors?

http//:www.cisecurity.org
ckreitner@cisecurity.org
dwaltermire@cisecurity.org

»