“Measurably reducing risk through collaboration, consensus & practical security management”
Content of this Presentation:

- Background
- George Mason University’s Rights and Benefits as a CIS Security Benchmarks Member
- Consensus Benchmarks
  - their value for system and network security
- Assessment Tools – Primarily CIS–CAT
  - use cases & features
  - specs & system requirements
- Security Software Certification
- Consensus Security Metrics
- Member Support & Contact Information
- Q & A
Background
Formed in October 2000

A not-for-profit consortium of users, security consultants, and vendors of security software (Members)

Convenes and facilitates teams developing consensus CIS Benchmarks for system & network security configuration and definitions for information security metrics

Developed, maintains and distributes the Configuration Assessment Tool (CIS-CAT) to its members
George Mason University’s Rights & Benefits of Membership
Benefits of CIS Security Benchmarks Membership: Unlimited Number of George Mason University Employees

- The right to distribute and use the CIS resources throughout George Mason University
- Access to Member Only Resources via the CIS Community Site including but not limited to:
  - Configuration Assessment Tool (CIS–CAT) Bundle
    - CIS–CAT Application
    - XML/XCCDF Benchmark versions
  - Remediation Kits (IBM AIX 5.3–6.1, RHEL Puppet Modules, MS Windows 7 & 8, MS Windows Server 2008 & 2012, MS Internet Explorer 9 &10, MS Outlook 2010)
  - Tutorials/Webcasts
  - Participation on the Member only discussion areas
  - Register for access [http://benchmarks.cisecurity.org/register](http://benchmarks.cisecurity.org/register)
Additional Benefits

- **Member Updates** – timely notification of new releases & updates
- **CIS Member Logo** – use of the CIS Member Logo to show your membership support. Learn more here: [http://benchmarks.cisecurity.org/trademarks](http://benchmarks.cisecurity.org/trademarks)
- **Support** – As Members, George Mason University employees receive **free** Benchmark/CIS-CAT implementation support. Submit requests at [support@cisecurity.org](mailto:support@cisecurity.org)
- To view complete list of benefits, please visit: [http://benchmarks.cisecurity.org/membership](http://benchmarks.cisecurity.org/membership)
Use of CIS resources in the classroom environment for educational purposes.

Redistribution of CIS resources to enrolled students for use on students’ laptops and desktops. A university may not redistribute CIS resources on its public-facing web site, but may redistribute CIS resources to enrolled students by means which require students to receive and accept the CIS Terms of Use as defined at http://benchmarks.cisecurity.org/downloads.
What are you working on?

- What’s in your environment?
  - Databases, Mail, WWW
  - Server OSs
  - Network Gear
  - Endpoint Software

- Which Benchmarks have you looked at? Any feedback?
- Which Benchmarks do you plan to leverage next?
What are Benchmarks?

- Consensus Configuration Recommendations for Security IT Resources
  - Examples:
    - Ensure Firewall is Enabled
    - Disallow SSH Protocol 1
    - Ensure `echo` Service is Disabled
  - Specifically called out by FISMA and PCI for securing systems.
What’s inside?

Overview
This document, Security Configuration Benchmark for Apple iOS 4.1.0, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS version 4.1.0. This guide was tested against the Apple iOS 4.1.0 and the iPhone Configuration Utility (iPCU) v3.1.0.256. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance
This guide was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience
This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that incorporate the Apple iOS 4.1.0.
What’s inside?

- What it applies to ...
- Who helped make it...

Acknowledgements

The Center for Internet Security would recognize the individuals that significantly contributed to creation of this guide.

Authors
Robert Fritz
Michael Louie
Chris Calabrese (v1.4.2)

Contributors and Reviews
Alex Noordergraaf
Anders Thulin
Andre Carrington
Andrew Gilmore
Aurobindo Sundaram
Bill Barto
Blake Frantz
Buck Keith
Calabrese Christopher
Carlisle Childress
James A. Finegan
James B. Horwath
James Finegan
James G. McIntyre
James Philip
Jay Beale
Jeff Pike
Jennifer Friend
Jim Becher
Jim Finegan
Randy Bowie
Randy Marchany
Randy Young
Ratan Nalumasu
Richard Bejtlich
Rich Murphey
Robert W. Maloy
Rodney McKee
Ronald Luman
Ron Colvin
What’s inside?

- What it applies to...
- Who helped make it...
- How to interpret...

<table>
<thead>
<tr>
<th>Configuration Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.</td>
</tr>
</tbody>
</table>

**Level-I Benchmark settings/actions**
Level-I Benchmark recommendations are intended to:
- be practical and prudent;
- provide a clear security benefit; and
- not negatively inhibit the utility of the technology beyond acceptable means

**Level-II Benchmark settings/actions**
Level-II Benchmark recommendations exhibit one or more of the following characteristics:
- may negatively inhibit the utility or performance of the technology
- acts as defense in depth measure

**Scoring Status**
This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

**Scorable**
The platform’s compliance with the given recommendation can be determined via automated means.

**Not Scorable**
The platform’s compliance with the given recommendation cannot be determined via automated means.
What’s inside?

- What it applies to...
- Who helped make it...
- How to interpret...
- What to do...

Why to do it...

How to do it...

How do you know you did it...

1.5 Protect the Shutdown Port

1.5.1 Set a nondeterministic Shutdown command value (Level 1, Scorabble)

Description:
Tomcat listens on TCP port 8005 to accept shutdown requests. By connecting to this port and sending the SHUTDOWN command, all applications within Tomcat are halted. The shutdown port is not exposed to the network as it is bound to the loopback interface. It is recommended that a nondeterministic value be set for the shutdown attribute in $CATALINA_HOME/conf/server.xml.

Rationale:
Setting the shutdown attribute to a nondeterministic value will prevent malicious local users from shutting down Tomcat.

Remediation:
Perform the following to set a nondeterministic value for the shutdown attribute.

1. Update the shutdown attribute in $CATALINA_HOME/conf/server.xml as follows:

   ```xml
   <Server port="8005" shutdown="NONDETERMINISTICVALUE"/>
   ```

   Note: NONDETERMINISTICVALUE should be replaced with a sequence of random characters.

Audit:
Perform the following to determine if the shutdown port is configured to use the default shutdown command:

1. Ensure the shutdown attribute in $CATALINA_HOME/conf/server.xml is not set to SHUTDOWN.

   ```
   $ cd $CATALINA_HOME/conf
   $ grep "shutdown[[:space:]]*=[:space:]*"SHUTDOWN" server.xml
   ```

Default Value:
The default value for the shutdown attribute is SHUTDOWN.

References:
1. http://tomcat.apache.org/tomcat-5.5-doc/config/server.html
Over 70 Benchmarks Covering 14 Technology Groups

- **Authentication Servers**
  - FreeRADIUS 1.1.3
  - MIT Kerberos 1.0

- **Collaboration Servers**
  - Microsoft SharePoint Server 2007

- **Database Platforms**
  - IBM DB2 Server 8/9/9.5
  - Microsoft SQL Server 2000/2005/2008 R2
  - MySQL Database Server 4.1/5.0/5.1
  - Oracle Database Server 8i/9i/10g/11g R2
  - Sybase Database Server 15

- **Directory Servers**
  - Novell eDirectory 8.7
  - OpenLDAP Server 2.3.39/2.4.6

- **DNS Servers**
  - BIND DNS Server 9.0–9.5

- **Mail Servers**

- **Mobile Platforms**
  - Apple Mobile Platform iOS 5.0.x
  - Google Mobile Platform

- **Network Devices**
  - Checkpoint Firewall
  - Cisco Firewall Devices
  - Cisco Routers/Switches IOS 12.x
  - Cisco Wireless LAN Controller 7
  - Juniper Routers/Switches JunOS 8/9/10
  - Agnostic Print Devices

- **Productivity Software**
  - Microsoft Office 2007
  - Microsoft Outlook 2010

- **Operating Systems – Desktop**
  - Apple Desktop OSX 10.4/10.5
  - Microsoft Windows Desktop XP/NT/7/8

- **Operating Systems – Servers**
  - Debian Linux Server
  - FreeBSD Server 4.1.0
  - HP–UX Server 11iv2/3 Update 4
  - IBM AIX Server 4.3.2/4.3.3/5L/5.1/5.3/6.1/7.1
  - Microsoft Windows Server 2000 Pro/2003 DC & MS/2008 DC & MS/2012 DC & MS
  - Novell Netware
  - Oracle Solaris Server 2.5.1–11/10 updates 3–8
  - Red Hat Linux Server 4/5/6
  - Slackware Linux Server 10.2
  - SUSE Linux Enterprise Server 9/10

- **Virtualization Platforms**
  - VMware Server 3.5/4.1
  - Xen Server 3.2
  - Agnostic VM Server

- **Web Browsers**
  - Apple Safari Browser 4.x
  - Microsoft Internet Explorer 9/10
  - Mozilla Firefox Browser 3.6
  - Opera Browser 10

- **Web Servers**
  - Apache HTTP Server 2.2/2.4
  - Apache Tomcat Server 5.5/6.0
  - Microsoft IIS Server 5/6/7/7.5

©2013 CIS Security Benchmarks
Benchmarks Planned for 2013

- **Database Platforms**
  - Microsoft SQL Server 2012

- **Network Devices**
  - Agnostic Wireless Devices

- **Mail Servers**
  - Microsoft Exchange 2010

- **Productivity Software**
  - Microsoft Outlook 2010 – RELEASED

- **Virtualization Platforms**
  - VMware Server vSphere 5

- **Web Browsers**
  - Microsoft Internet Explorer 10 – RELEASED

- **Operating Systems – Desktop**
  - Apple Desktop OSX 10.7 & 10.8
  - Microsoft Windows Desktop 8 – RELEASED

- **Operating Systems – Servers**
  - Linux Agnostic
  - IBM AIX Server 7.1 – RELEASED
  - Microsoft Windows Server 2012 – RELEASED
  - SUSE Linux Enterprise Server 11
How are the Benchmarks created?

- Decide what to make
  - Ask CIS members
  - Survey community
- Build a consensus team
  - CIS Members
  - Subject Matter Experts
  - Public security community
  - Technology vendors
  - .com, .edu, .gov, .org, .tld
How does the consensus process work?

- Define scope
- Contractors and volunteers write recommendations
- Recommendations are reviewed by consensus team
- Tickets are created for issues

```csharp
while(tickets.Count > 0)
{
    discussTickets();
}
```
How are the benchmarks maintained?

- After a Benchmark release, a new milestone is created 3+ months out.
- Benchmark adopters filter feedback to CIS via:
  - support@cisecurity.org (members)
  - feedback@cisecurity.org (non member)
  - Web site bug report form
  - Open ticket in consensus platform
- Tickets are assigned to a release milestone.
- Technology point releases are accounted for.
- Maintainer teams work/close tickets with consensus group.
- Where no maintainer team exists, staff and/or contractors work tickets.
Who contributes and why do they?

- Technology Vendors
  - Many don’t have their own security guides
  - They want to ensure guidance does not introduce unsupported state

- Individuals
  - Earn CPE credits for ISC2/ISACA certs
  - Learn from other SMEs/skill building

- Members
  - They’ve bought in to the model
  - It’s in their best interest
  - RFP bid fodder for security consultancies

- Attribution
- Some just want to help
How can I get involved?

- Join a Consensus Team
  - Log in to the member community site:
    [https://community.cisecurity.org](https://community.cisecurity.org)
  - Click Profile
  - Click Manage Projects
  - Add yourself to the project(s)
- Begin Participation
  - Review Drafts
  - Answer Questions
  - Test Configurations
  - Report Bugs/Suggestions
Where do I download the resources?

- All downloads can be found under the Downloads Tab
When is a benchmark scheduled for release?
How can I be notified when it has been released?

- **When:**
  - Roadmap is Updated Automatically from Project Milestones
    - [https://benchmarks.cisecurity.org/projects](https://benchmarks.cisecurity.org/projects)

- **How:**
  - Subscribe to our Download RSS Feed
    - [http://benchmarks.cisecurity.org/rss](http://benchmarks.cisecurity.org/rss)

- **Member Updates**
  - Via email
    - Update your ‘receive newsletter’ setting on the community site
    - Profile → Update Profile
What formats are the benchmarks in?

- All
  - Portable Document Format (PDF)
- Select
  - Microsoft Word
  - Microsoft Excel
  - eXtensible Configuration Checklist Description Format (XCCDF)
    - OVAL and ECL
- Automated Remediation Formats
  - Group Policy Objects (GPO)
    - MS Windows 7 & 8 and MS Windows Server 2008 & 2012 and MS Internet Explorer 9 & 10, MS Outlook 2010
  - AIXPert XML
    - IBM AIX 5.3 – AIX 6.1
  - RedHat Linux Enterprise
    - RHEL 6 Puppet Modules
  - Bastille Configuration
    - HP–UX 11i
Questions about the Benchmarks?
CIS Configuration Assessment Tool (CIS–CAT)
What is CIS–CAT?

- Host based, configuration assessment tool
- Assesses a target system against recommendations made in CIS benchmarks
- Requires Java Runtime Environment (JRE) v1.5 or later
- Has graphical (GUI) and command line (CLI) user interfaces
- Reads XML policy that can be customized
- NIST FDCC Validated Scanner
- Available to CIS members only
How is it used?

- Server admins/operations teams use CIS–CAT to perform self assessments.
- Build teams use CIS–CAT to validate a system before production rollout.
- Security teams use CIS–CAT as part of their assessment process.
- Auditors use CIS–CAT as part of compliance and governance processes.
- Run CIS–CAT via Group Policy to assess Microsoft Windows environment on reoccurring basis.
What benchmarks does it assess?

- **Authentication Servers**
  - MIT Kerberos 1.10 Benchmark v1.0.0

- **Database Platforms**
  - Oracle Database 11g Benchmark v1.0.1
  - Oracle Database 9i–10g Benchmark v2.0.1

- **Virtualization Platforms**
  - VMware ESX 3.5 Benchmark v1.2.0
  - VMware ESX 4.1 Benchmark v1.0.0

- **Web Browsers**
  - Mozilla Firefox Benchmark v1.0.0
  - Microsoft Internet Explorer 10 Benchmark v1.0.0

- **Web Servers**
  - Apache Tomcat Benchmark v1.0.0

- **Operating Systems – Desktop**
  - Apple OSX 10.5 Benchmark v1.1.0
  - Apple OSX 10.6 Benchmark v1.0.0
  - Microsoft Windows 7 Benchmark v1.2.0 (domain joined/oval)
  - Microsoft XP Benchmark v2.0.1

- **Operating Systems – Servers**
  - Debian Linux Benchmark v1.0.0
  - FreeBSD Server 4.1.0
  - HP-UX 11i Benchmark v1.4.2
  - IBM AIX 4.3–5.1 Benchmark v1.0.1
  - IBM AIX 5.3–6.1 Benchmark v1.1.0
  - IBM AIX 7.1 Benchmark v1.0.0
  - Microsoft Windows 2003 MS DC Benchmark v2.0.0
  - Microsoft Windows 2008 Server Benchmark v1.2.0 (domain joined/oval)
  - Oracle Solaris Server 2.5.1–11/10 updates 3–8
  - Red Hat Enterprise Linux Server 4 Benchmark v1.0.5
  - Red Hat Enterprise Linux Server 5 Benchmark v2.0.0
  - Red Hat Enterprise Linux Server 6 Benchmark v1.2.0
  - Slackware Linux 10.2 Benchmark v1.1.0
  - Solaris 10 Benchmark v5.1.0
  - Solaris 11 Benchmark v1.0.0
  - SUSE Linux Enterprise Server 10 Benchmark v2.0.0
  - SUSE Linux Enterprise Server 9 Benchmark v1.0.0
What’s coming out this year?

- **Databases**
  - Microsoft SQL 2008

- **Network Devices**
  - Cisco coverage

- **Operating Systems – Desktop**
  - Apple Desktop OSX 10.8
  - Microsoft Windows Desktop 8

- **Operating Systems – Servers**
  - Microsoft Windows Server 2012
  - Oracle Database 11gR2
  - SUSE Linux Enterprise Server 11

- **Productivity Software**
  - Microsoft Outlook 2010

- **Virtualization Platforms**
  - VMware Server vSphere 5

- **Web Browsers**
  - Microsoft Internet Explorer 10 – RELEASED
What kind of docs does it come with?

- CIS–CAT Users Guide
  - Executing CIS–CAT via GUI and CLI
  - Understanding CIS–CAT Reports & Customization of Reports
  - Using the CIS–CAT Dashboard
- CIS–CAT XML Adaptation Guide
  - How to add/remove/modify checks
What’s it take to get CIS–CAT running?
Ten Easy Steps

1. Download
2. Unzip*
3. Double Click
4. Select a Benchmark

*P.S. – Unzip CIS–CAT on a network drive and invoke it via Group Policy for +10 scalability points.
5. Select a Profile

The image shows a window from a Configuration Assessment Tool. It displays an interface for selecting profiles with options such as "Enterprise Member Server," "Profiles," "Enterprise Domain Controller," and "SSLF Domain Controller." Instructions for selecting a profile are visible in the window.
6. Scan

![Configuration Assessment Tool](image.png)

**Benchmark Execution Status**

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Time</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/188</td>
<td>Network security: Minimum session security for NTLM SSP based (including se...</td>
<td>&lt;1 second</td>
<td>Fail</td>
</tr>
<tr>
<td>2/188</td>
<td>Network access: Allow anonymous SID/Name translation</td>
<td>&lt;1 second</td>
<td>Fail</td>
</tr>
<tr>
<td>3/188</td>
<td>Accounts: Limit local account use of blank passwords to console logon only</td>
<td>&lt;1 second</td>
<td>Pass</td>
</tr>
<tr>
<td>4/188</td>
<td>Audit: Shut down system immediately if unable to log security audits</td>
<td>&lt;1 second</td>
<td>Pass</td>
</tr>
<tr>
<td>5/188</td>
<td>Audit: Force audit policy subcategory settings (Windows Vista or later) to overrid...</td>
<td>&lt;1 second</td>
<td>Fail</td>
</tr>
<tr>
<td>5/188</td>
<td>Devices: Allowed to format and eject removable media</td>
<td>&lt;1 second</td>
<td>Fail</td>
</tr>
<tr>
<td>7/188</td>
<td>Domain member: Digitally encrypt or sign secure channel data (always)</td>
<td>&lt;1 second</td>
<td>Pass</td>
</tr>
<tr>
<td>7/188</td>
<td>Domain member: Digitally encrypt secure channel data (when possible)</td>
<td>&lt;1 second</td>
<td>Pass</td>
</tr>
<tr>
<td>9/188</td>
<td>Domain member: Digitally sign secure channel data (when possible)</td>
<td>&lt;1 second</td>
<td>Pass</td>
</tr>
<tr>
<td>10/188</td>
<td>Domain member: Disable machine account password changes</td>
<td>&lt;1 second</td>
<td>Pass</td>
</tr>
<tr>
<td>11/188</td>
<td>Domain member: Require strong (Windows 2000 or later) session key</td>
<td>&lt;1 second</td>
<td>Pass</td>
</tr>
<tr>
<td>12/188</td>
<td>Interactive logon: Do not display last user name</td>
<td>&lt;1 second</td>
<td>Fail</td>
</tr>
<tr>
<td>13/188</td>
<td>Interactive logon: Do not require CTRL+ALT+DEL</td>
<td>&lt;1 second</td>
<td>Fail</td>
</tr>
<tr>
<td>14/188</td>
<td>Interactive logon: Number of previous logons to cache (in case domain controller)</td>
<td>&lt;1 second</td>
<td>Fail</td>
</tr>
</tbody>
</table>

©2013 CIS Security Benchmarks
7. “Find The Fail”™® © 😊

<table>
<thead>
<tr>
<th>Description</th>
<th>Pass</th>
<th>Fail</th>
<th>Info</th>
<th>Not Selected</th>
<th>Score</th>
<th>Max</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Patches and Additional Software</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0.0</td>
<td>0.0</td>
<td>0%</td>
</tr>
<tr>
<td>2. Restrict Services</td>
<td>0</td>
<td>22</td>
<td>0</td>
<td>1</td>
<td>0.0</td>
<td>22.0</td>
<td>0%</td>
</tr>
<tr>
<td>2.2 Disable Unnecessary Local Services</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>7.0</td>
<td>0%</td>
</tr>
<tr>
<td>2.3 Disable Other Services</td>
<td>0</td>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>14.0</td>
<td>0%</td>
</tr>
<tr>
<td>3. Kernel Tuning</td>
<td>0</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>21.0</td>
<td>0%</td>
</tr>
<tr>
<td>3.4 Modify Network Parameters</td>
<td>0</td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>17.0</td>
<td>0%</td>
</tr>
<tr>
<td>4. Logging</td>
<td>0</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>9.0</td>
<td>0%</td>
</tr>
<tr>
<td>5. File/Directory Permissions/Access</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0.0</td>
<td>2.0</td>
<td>0%</td>
</tr>
<tr>
<td>6. System Access, Authentication, and Authorization</td>
<td>2</td>
<td>18</td>
<td>0</td>
<td>2</td>
<td>2.0</td>
<td>20.0</td>
<td>10%</td>
</tr>
<tr>
<td>6.3 Configure SSH</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>10.0</td>
<td>0%</td>
</tr>
<tr>
<td>7. User Accounts and Environment</td>
<td>2</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
<td>9.0</td>
<td>22%</td>
</tr>
<tr>
<td>8. Warning Banners</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
<td>5.0</td>
<td>0%</td>
</tr>
<tr>
<td>9. System Maintenance</td>
<td>14</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>14.0</td>
<td>17.0</td>
<td>82%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>18</td>
<td>87</td>
<td>0</td>
<td>9</td>
<td><strong>18.0</strong></td>
<td><strong>105.0</strong></td>
<td><strong>17%</strong></td>
</tr>
</tbody>
</table>

©2013 CIS Security Benchmarks
8. “Fix The Fail”™® ☺

3.4.5 Disable Response to ICMP Netmask Requests

Description:
The `ip_respond_to_address_mask_broadcast` parameter controls whether or not to respond to ICMP netmask requests, typically sent by diskless clients when booting.

Rationale:
An attacker could use the netmask information to determine network topology. The default value is 0.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `nadm` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# nadm -set /dev/Ip ip_respond_to_address_mask_broadcast 0
```

Note:
This setting will NOT persist between reboots.
Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svcfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# nadm -get /dev/Ip ip_respond_to_address_mask_broadcast
0
```
9. Monitor Progress
10. Measure Configuration Change Management using the CIS Security Metrics
Other Assessment Tools Currently Available

- Router Audit Tool (RAT Tool)
  - PERL based tool
  - Assesses Cisco ASA, FWSM, PIX and IOS devices against CIS Cisco benchmarks.

- Apache Benchmark Tool
  - PERL based tool
  - Assesses Apache HTTP Server instances against the CIS Apache HTTP Server benchmark.
Questions about the Tools?
Security Software Certification
Certification Overview

- CIS Certified Security Software
  - Tested to accurately measure and report system status against recommendation in CIS Benchmarks
  - [http://benchmarks.cisecurity.org/certified](http://benchmarks.cisecurity.org/certified)

- Why use Certified Security Software?
  - Independently validated to accurately audit systems
  - CIS Benchmark content integrated into software
  - Enterprise scale security auditing
  - Leverage deployed management tools
Consensus Security Metrics
Organizations struggle to make cost-effective security investment decisions;

Information Security Professionals lack widely accepted and unambiguous metrics for decision support.

To address this need, established a consensus team of over 120 industry experts from leading commercial, government and academic organizations of varying sizes.

The result was a set of unambiguous, user originated, consensus-based standard metrics and data definitions that can be used across organizations to define, collect and analyze data on security process benefits and outcomes.
Consensus Security Metrics

- Set of 28 metrics definitions designed to help security professionals in analyzing security process performance and outcome data.

- Metrics cover 7 important business functions:
  - Incident Management
  - Vulnerability Management
  - Patch Management
  - Application Security
  - Configuration Management
  - Change Management
  - Financial Metrics

- CIS Security Metrics Quick Start Guide v1.0.0

- Download: [http://community.cisecurity.org](http://community.cisecurity.org)
  (Downloads Tab → Security Metrics Category)
Member Support, Contact & Additional Information
As a benefit of membership, George Mason University employees are eligible to receive support service, at no charge, from staff:

- Email: support@cisecurity.org
- Telephone, after initial email contact
- Discussion areas on Community Member site

Primary Membership Contact – Michelle Vogeler, Member Representative, mvogeler@cisecurity.org
Q&A