



Center for
Internet Security®

Security
Benchmarks™

“Measurably reducing risk through collaboration, consensus & practical security management”

Content of this Presentation:

- ▶ Background
- ▶ State of Idaho'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

CIS Security Benchmarks

- ▶ 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

State of Idaho's Rights & Benefits of Membership

Benefits of CIS

Security Benchmarks Membership:

Unlimited Number of State of Idaho Employees

- ▶ The right to distribute and use the CIS resources throughout State of Idaho
- ▶ 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
 - ▶ User's Guide and XML/XCCDF Policy Customization Guide
 - ▶ **Remediation Content** (AIXPERT XML IBM AIX 5.3-6.1 & 7.1, RHEL 6 & CentOS Linux 6 Puppet Modules, GPOS for MS Windows XP, 7, 8 & 8.1, MS Windows Server 2008, 2008 R2, Server 2012 and Server 2012 R2, MS Internet Explorer 9 & 10, MS Outlook 2010 - Hardened Virtual Images MS Windows Server 2008 SP2, MS Windows Server 2012, SLES 11, RHEL 5, 6, & 7, CentOS Linux 6 & 7, Ubuntu 12.04 & 14.04 LTS Server)
 - ▶ Tutorials/Webcasts
 - ▶ Participation on the Member only discussion areas
 - ▶ Register for access <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>
- ▶ **Support** – As Members, State of Idaho employees receive **free** Benchmark/CIS–CAT implementation support. Submit requests at support@cisecurity.org
- ▶ To view complete list of benefits, please visit: <http://benchmarks.cisecurity.org/membership>



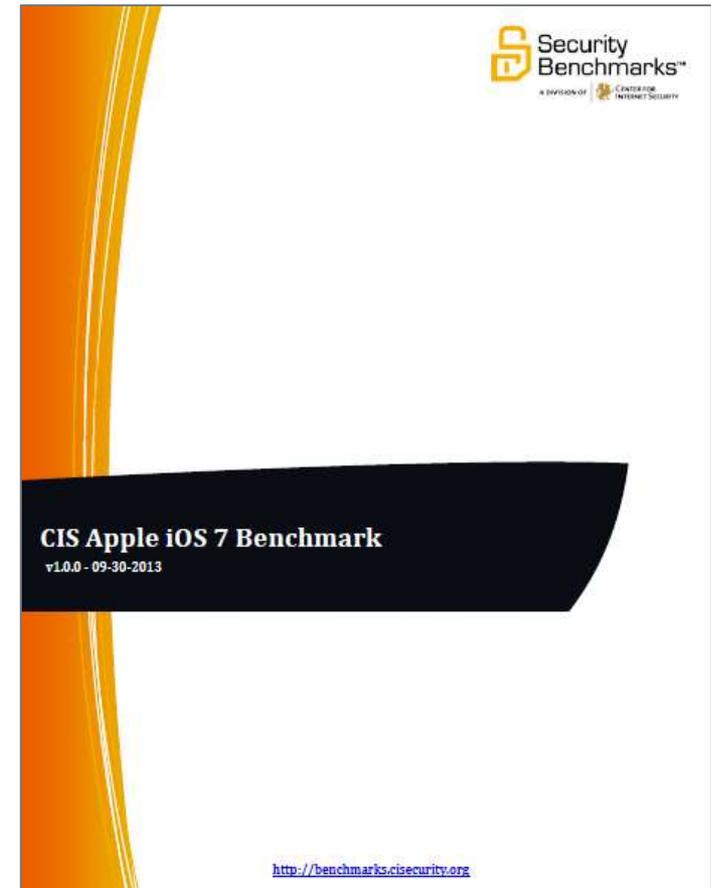
Security Benchmarks

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?

▶ What it applies to... 

Overview

This document, *Security Configuration Benchmark for Apple iOS 7*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS version 7.0.2. This guide was tested against the Apple iOS 7.0.2 and the iPhone Configuration Utility (iPCU) v3.6.2.300. This benchmark covers the Apple iOS 7.0.2 and all hardware devices on which this iOS is supported. As of the publication of this guidance, mobile devices supported by iOS 7.0.2 include the following:

- iPhone 5S
- iPhone 5C
- iPhone 5
- iPhone 4S
- iPhone 4
- iPad with Retina display
- iPad Mini
- iPad 2
- iPod Touch (5th Generation)

In determining recommendations, the current guidance treats all iOS mobile device platforms as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform; for the few cases where variation exists, the benchmark notes the difference within the respective section. To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at 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 7.0.2.

Consensus Guidance

This benchmark was created using a consensus review process comprised 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.

What's inside?

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



Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author

David Skrdla

Contributors

Adrian Sanabria

Brian Reilly

Joe Wulf RHCSA(RHEL6), FITSP-D, CISSP, VCP3, CPO(USN RET), *U.S. National Security Agency*

Richard Tychansky

Roland Grefer

Shawn Geddis

Toon Mordijck

Blake Frantz, *Center for Internet Security*

Jonathan Zeolla

Mark Andersen

Editors

David Skrdla

Mike de Libero, *MDE Development, Inc.*

What's inside?

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



Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Apple iOS 7**

Items in this profile apply to Apple iOS 7 and intend to:

- Be practical and prudent.
- Provide a clear security benefit.
- Not inhibit the utility of the technology beyond acceptable means.

- **Level 2 - Apple iOS 7**

This profile extends the "Level 1 - Apple iOS 7" profile. Items in this profile exhibit one or more of the following characteristics:

- Intended for environments or use cases where security is paramount.
- Act as defense in depth measures.
- May negatively inhibit the utility or performance of the technology.

What's inside?

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

▶ What to do...



▶ Why to do it...



▶ How to audit...



▶ How to fix...



2.2 Passcode Settings

This section provides guidance on the secure configuration of passcode settings.

2.2.1 Require passcode on device (Scored)

Profile Applicability:

- Level 1 - Apple iOS 7

Description:

This control determines whether a password is required before allowing access to the device via the touch screen.

Rationale:

Requiring a password to unlock the device helps prevent unauthorized access to the device and increases the effort required to use the device or access data stored on it.

Audit:

1. Open the configuration profile XML file.
2. Search for `<key>forcePIN</key>`.
3. Observe if the next line is `<true/>`.

Remediation:

1. Open iPCU.
2. Click on Configuration Profiles in the left windowpane.
3. Click on the Passcode tab in the lower right windowpane.
4. If a passcode is not currently required, you will be prompted to Configure Passcode Policy. Click on the Configure button in the prompt.
5. Install the configuration profile on the device.

Over 100 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 R2/2012/2014
 - ▶ MySQL Database Server 4.1/5.0/5.1/5.6
 - ▶ Oracle Database Server 8i/9i/10g/11g R2/12c
 - ▶ 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**
 - ▶ Microsoft Exchange 2003/2007/2010/2013
- ▶ **Mobile Platforms**
 - ▶ Apple Mobile Platform iOS 5/6/7
 - ▶ 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 10.4/10.5/10.6/10.8/10.9
 - ▶ Microsoft Windows Desktop XP/NT/7/8.1
- ▶ **Virtualization Platforms**
 - ▶ VMware Server 3.5/4.1/5.1/5.5, 5.5 Update 2
 - ▶ Xen Server 3.2
 - ▶ Agnostic VM Server
 - ▶ Docker 1.6
- ▶ **Operating Systems – Servers**
 - ▶ CentOS 6 / 7
 - ▶ 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/2008 R2 DC & MS/ 2012 R2 DC & MS/ 2012 DC & MS
 - ▶ Novell Netware
 - ▶ Oracle Solaris Server 2.5.1–11.1/ 10 updates 3–8
 - ▶ Red Hat Linux Server 4/5/6/7
 - ▶ Slackware Linux Server 10.2
 - ▶ SUSE Linux Enterprise Server 9/10/11
 - ▶ Ubuntu LTS Server 12.04/14.04
 - ▶ Amazon Linux 2014.09
 - ▶ Oracle Linux 7
- ▶ **Web Browsers**
 - ▶ Apple Safari Browser 4.x
 - ▶ Microsoft Internet Explorer 9/10
 - ▶ Mozilla Firefox Browser 3.6/24 ESR
 - ▶ Opera Browser 10
- ▶ **Web Servers**
 - ▶ Apache HTTP Server 2.2/2.4
 - ▶ Apache Tomcat Server 5.5/6.0
 - ▶ Microsoft IIS Server 5/6/7/7.5/8

Benchmarks Planned for 2015

- ▶ **Big Data**
 - ▶ Apache Hadoop 2.6
- ▶ **Database Platforms**
 - ▶ IBM DB2 10
 - ▶ MySQL Server 5.6 – RELEASED
 - ▶ MySQL Server 5.7
 - ▶ Mongo DB 2.6
 - ▶ Oracle 12c – RELEASED
 - ▶ PostgreSQL 9.4
- ▶ **Mail Servers**
 - ▶ Microsoft Exchange 2015
 - ▶ Microsoft Outlook 2013
- ▶ **Network Devices**
 - ▶ Checkpoint Firewall
 - ▶ Cisco ASA
 - ▶ Cisco NX-OS
 - ▶ Juniper Firewall
- ▶ **Operating Systems – Desktop**
 - ▶ Apple OSX 10.10
- ▶ **Operating Systems – Servers**
 - ▶ Amazon Linux – RELEASED
 - ▶ Debian Linux 7
 - ▶ IBM AIX
 - ▶ Oracle Linux 7 – RELEASED
 - ▶ Oracle Solaris 11.2
 - ▶ SUSE Linux Enterprise Server 12
 - ▶ Ubuntu Server 14.04 LTS – RELEASED
- ▶ **Productivity Software**
 - ▶ Microsoft Excel 2013
 - ▶ Microsoft Word 2013
- ▶ **Virtualization Platforms**
 - ▶ VMware ESXi 5.5 Update 2 – RELEASED
 - ▶ Docker 1.6 – RELEASED
- ▶ **Web Servers**
 - ▶ Apache Tomcat 7
 - ▶ Apache Tomcat 8
 - ▶ IBM Websphere Application Server 8.5
 - ▶ NginX 1.2
- ▶ **Web Browsers**
 - ▶ Google Chrome
 - ▶ Mozilla Firefox 31.3 ESR

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

```
▶ while(tickets.Count > 0)
{
    discussTickets();
}
```

Discussions		
Dashboard > Projects > CIS IBM AIX Benchmar... > Discussions > List		
Discussion	Replies	Last Reply
 Updated AIX 5.3 - 6.1 Benchmark Draft Available Started by Blake Frantz	5	4 days ago by Huibert K.
 Query regarding Trusted Execution (TE) flags Started by Shailesh Athalye	8	On Tue, May 25. 2010 by Steve P.
 Security Benchmark for AIX 6.1 Started by Shailesh Athalye	5	On Mon, May 3. 2010 by Shailesh A.
 Custom level AIX Security Expert Policy Started by Shailesh Athalye	2	On Tue, Apr 6. 2010 by Paul S.
 Rationale @ Item 1.1.16 - text mismatch Started by Christiane Cuculo	0	
 CIS AIX Benchmark Review Started by Blake Frantz	1	On Thu, Mar 18. 2010 by Boris K.

Tickets	
Dashboard > Projects > CIS IBM AIX Benchmar... > Tickets > All Open Tickets	
CIS AIX IBM 5.3-6.1 Benchmark v1.0.0 Released Add Ticket	
 - #1	Fix document title (5.1 - 6.3 -> 5.3 - 6.1) 
 - #2	No recommendation for SNMP community string 
 - #3	Possibly missing two more legacy recommendations 
 - #4	Remove reference to XML TAR file 

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>
 - ▶ Click Profile
 - ▶ Click Manage Communities
 - ▶ Add yourself to the community
- ▶ 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



The screenshot shows the Security Benchmarks website interface. At the top left is the logo for Security Benchmarks. To the right of the logo is a navigation bar with several tabs: People, Areas, Help, Downloads (which is highlighted in green), Search, Starred, Trash, and Quick Add. Below the navigation bar is a section titled 'Downloads' with buttons for 'New Text Download', 'Upload File', and a printer icon. Below this is a breadcrumb trail: 'Dashboard > Downloads > List'. There is a pagination control showing 'Page: (1), 2, 3, ... 8 | Next >>'. The main content area displays a list of downloaded files:

File Name	Size	Upload Date	Uploader	Category
ciscat-full-bundle-2011-10-31.zip	10.77MB	Mon, Oct 31, 2011	Mike de Libero	Tools: CIS-CAT
CIS Apache Tomcat Benchmark v1.0.0.pdf	1.25MB	Fri, Sep 30, 2011	Blake Frantz	Servers: Web
CIS Apple iOS Benchmark v1.3.0.pdf	1.20MB			

On the right side of the page, there is a sidebar with a section titled 'All Downloads' and several sub-sections: Archive, Desktop: Office, Desktop: Web Browsers, and Devices: Mobile.

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>
- ▶ How:
 - ▶ Subscribe to our Download RSS Feed
 - ▶ <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
- ▶ Remediation Content
 - ▶ Hardened Virtual Images – Amazon Machine Images (AMIs) for
 - ▶ Microsoft Windows Server 2008 SP2
 - ▶ Microsoft Windows Server 2012
 - ▶ RHEL 5 & 6
 - ▶ CentOS Linux 6 & 7
 - ▶ Ubuntu 12.04 & 14.04 LTS Server
 - ▶ SLES 11
 - ▶ Group Policy Objects (GPO)
 - ▶ MS Windows XP, 7, 8 & 8.1
 - ▶ MS Windows Server 2003, 2008, 2008 R2, 2012 & 2012 R2 and
 - ▶ MS Internet Explorer 9 & 10,
 - ▶ MS Outlook 2010
 - ▶ AIXPert XML
 - ▶ IBM AIX 5.3, 6.1 and 7.1
 - ▶ Puppet Modules
 - ▶ RHEL 6
 - ▶ CentOS Linux 6
 - ▶ 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) v1.6 or later
- ▶ Has graphical (GUI) and command line (CLI) user interfaces
- ▶ Reads XML policy that can be customized
- ▶ SCAP Validation as an Authenticated Configuration 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.
- ▶ **Vulnerability Assessment** (MS Windows XP, 7, 8, 8.1 Server 2008, 2008 R2, 2012, 2012 R2 and RHEL 4, 5, 6, 7)

What benchmarks does it assess?

▶ Authentication Servers

- ▶ MIT Kerberos 1.10*

▶ Database Platforms

- ▶ Oracle Database 12c
- ▶ Oracle Database 11g
- ▶ Oracle Database 9i-10g
- ▶ Microsoft SQL Server 2008 R2 Database Engine*
- ▶ Microsoft SQL Server 2014
- ▶ Microsoft SQL 2012 Database Engine*
- ▶ MySQL Server 5.6*

▶ Operating Systems – Desktop

- ▶ Apple OSX 10.5
- ▶ Apple OSX 10.6
- ▶ Apple OSX 10.8
- ▶ Apple OSX 10.9
- ▶ Apple OSX 10.10
- ▶ Microsoft Windows 7 (domain joined)*
- ▶ Microsoft Windows Desktop 8 (domain joined)*
- ▶ Microsoft Windows 8.1*
- ▶ Microsoft XP*

▶ Operating Systems – Servers

- ▶ Amazon Linux 2014.09
- ▶ CentOS Linux 6
- ▶ CentOS Linux 7
- ▶ Debian Linux
- ▶ FreeBSD Server 4.1.0
- ▶ HP-UX 11i
- ▶ IBM AIX 4.3-5.1
- ▶ IBM AIX 5.3-6.1
- ▶ IBM AIX 7.1
- ▶ Microsoft Windows 2003 MS DC
- ▶ Microsoft Windows 2008 Server (domain joined)*
- ▶ Microsoft Windows 2008 R2 Server*
- ▶ Microsoft Windows Server 2012 (domain joined)*
- ▶ Microsoft Windows Server 2012 R2
- ▶ Oracle Linux 7
- ▶ Oracle Solaris Server 2.5.1- 9
- ▶ Oracle Solaris 10
- ▶ Oracle Solaris 11
- ▶ Oracle Solaris 11.1 Benchmark
- ▶ Red Hat Enterprise Linux Server 4
- ▶ Red Hat Enterprise Linux Server 5
- ▶ Red Hat Enterprise Linux Server 6
- ▶ Red Hat Enterprise Linux Server 7
- ▶ Slackware Linux10.2
- ▶ SUSE Linux Enterprise Server 9
- ▶ SUSE Linux Enterprise Server 10
- ▶ SUSE Linux Enterprise Server 11
- ▶ Ubuntu 12.04 LTS Server
- ▶ Ubuntu 14.04 LTS Server

▶ Virtualization Platforms

- ▶ VMware ESX 3.5
- ▶ VMware ESX 4.1
- ▶ VMware ESX 5.5

▶ Web Browsers

- ▶ Mozilla Firefox
- ▶ Mozilla Firefox ESR 24
- ▶ Microsoft Internet Explorer 10*

▶ Web Servers

- ▶ Apache Tomcat
- ▶ Microsoft IIS 7/7.5
- ▶ Microsoft IIS 8/8.5

What's coming out this year?

▶ Databases

- ▶ IBM DB2 10*
- ▶ Microsoft SQL Server 2014* – RELEASED
- ▶ MySQL Server 5.6* – RELEASED
- ▶ MySQL Server 5.7*
- ▶ Mongo DB 2.6*
- ▶ Oracle 12c* – RELEASED
- ▶ PostgreSQL 9.4*

▶ Mail Servers

- ▶ Microsoft Outlook 2013*

▶ Network Devices

- ▶ Cisco IOS*
- ▶ Cisco ASA*
- ▶ Cisco NX-OS*

▶ Operating Systems – Desktop

- ▶ Apple Desktop OSX 10.10 – RELEASED

▶ Operating Systems – Servers

- ▶ Amazon Linux 2014.09 – RELEASED
- ▶ Debian Linux 7*
- ▶ Oracle Solaris 11.2
- ▶ Oracle Linux 7 – RELEASED
- ▶ SUSE Linux Enterprise Server 12
- ▶ Ubuntu Server 14.04 LTS – RELEASED

▶ Productivity Software

- ▶ Microsoft Excel 2013*
- ▶ Microsoft Word 2013*

▶ Web Server

- ▶ Apache Tomcat 7*
- ▶ Apache Tomcat 8*
- ▶ IIS 7/7.5 – RELEASED
- ▶ NginX 1.7*

▶ Web Browsers

- ▶ Mozilla Firefox 31.3ESR*
- ▶ Google Chrome

▶ Virtualization Platforms

- ▶ VMware ESXi 5.5 Update 2 – RELEASED

*indicates XCCDF+OVAL coverage

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

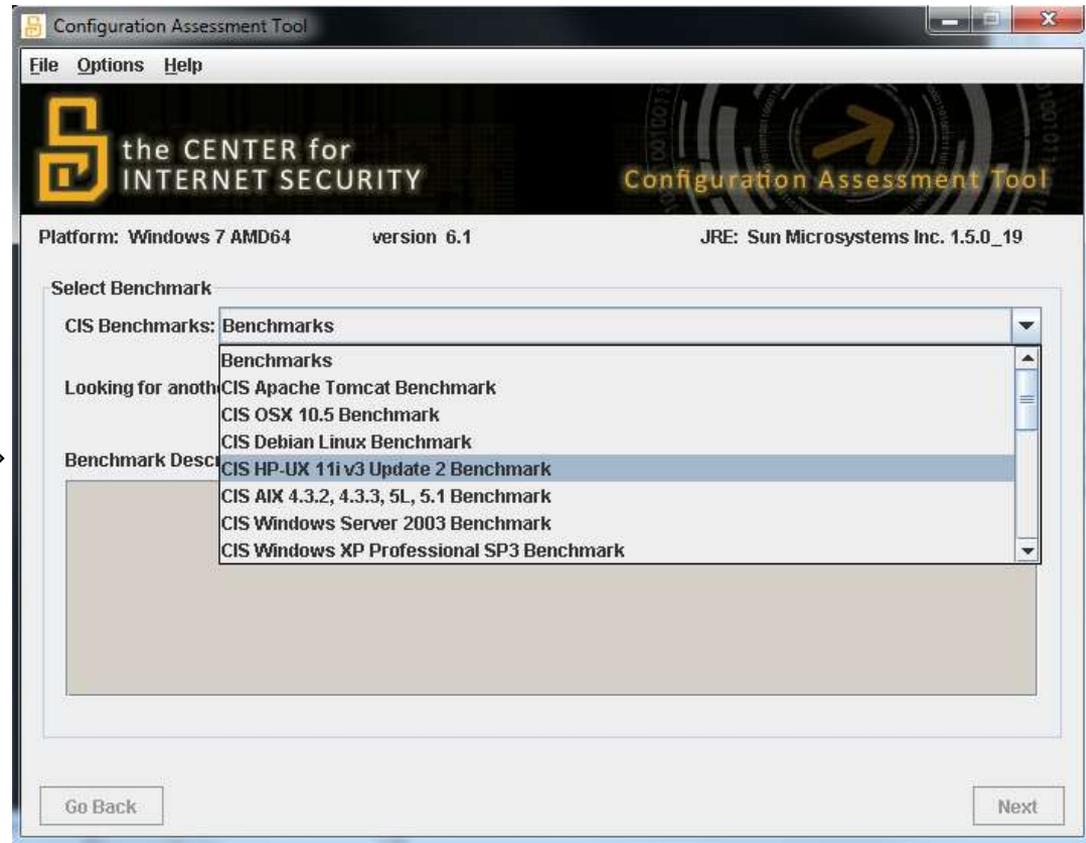
What's it take to get CIS-CAT running?

I 
RUNNING

Just a few steps...

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

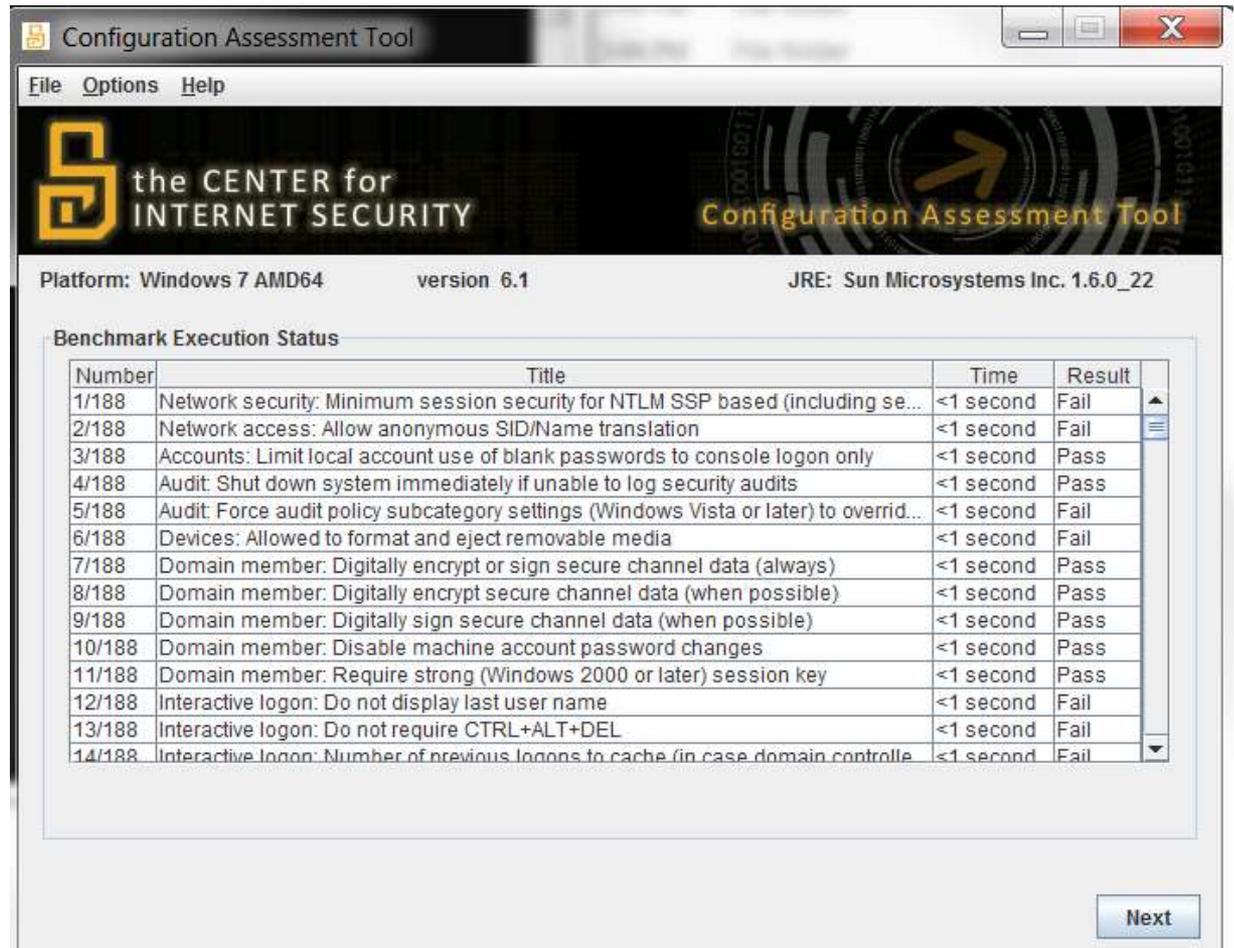
*P.S. – Unzip CIS-CAT on a network drive and invoke it via Group Policy for +10 scalability points.



5. Select a Profile



6. Scan



The screenshot shows the Configuration Assessment Tool interface. At the top, there is a menu bar with 'File', 'Options', and 'Help'. Below the menu bar is a banner for 'the CENTER for INTERNET SECURITY' and 'Configuration Assessment Tool'. The main area displays the following information:

Platform: Windows 7 AMD64 version 6.1 JRE: Sun Microsystems Inc. 1.6.0_22

Benchmark Execution Status

Number	Title	Time	Result
1/188	Network security: Minimum session security for NTLM SSP based (including se...	<1 second	Fail
2/188	Network access: Allow anonymous SID/Name translation	<1 second	Fail
3/188	Accounts: Limit local account use of blank passwords to console logon only	<1 second	Pass
4/188	Audit: Shut down system immediately if unable to log security audits	<1 second	Pass
5/188	Audit: Force audit policy subcategory settings (Windows Vista or later) to overrid...	<1 second	Fail
6/188	Devices: Allowed to format and eject removable media	<1 second	Fail
7/188	Domain member: Digitally encrypt or sign secure channel data (always)	<1 second	Pass
8/188	Domain member: Digitally encrypt secure channel data (when possible)	<1 second	Pass
9/188	Domain member: Digitally sign secure channel data (when possible)	<1 second	Pass
10/188	Domain member: Disable machine account password changes	<1 second	Pass
11/188	Domain member: Require strong (Windows 2000 or later) session key	<1 second	Pass
12/188	Interactive logon: Do not display last user name	<1 second	Fail
13/188	Interactive logon: Do not require CTRL+ALT+DEL	<1 second	Fail
14/188	Interactive logon: Number of previous logons to cache (in case domain controlle	<1 second	Fail

At the bottom right of the window, there is a 'Next' button.

(WEEEEEE!!!)

7. “Find The Fail ”™® © ☺

Summary



Description	Tests			Scoring		
	Pass	Fail	Error	Score	Max	Percent
1 Recommendations	7	21	0	7.0	28.0	25%
1.1 Preinstallation	0	0	0	0.0	0.0	0%
1.2 Installation	0	0	0	0.0	0.0	0%
1.3 Remove Extraneous Resources	0	0	0	0.0	0.0	0%
1.4 Limit Server Platform Information Leaks	1	1	0	1.0	2.0	50%
1.5 Protect the Shutdown Port	1	0	0	1.0	1.0	100%
1.6 Protect Tomcat Configurations	0	14	0	0.0	14.0	0%
1.7 Secure Realms	0	0	0	0.0	0.0	0%
1.8 Connector Security	1	2	0	1.0	3.0	33%
1.9 Establish and Protect Logging Facilities	0	1	0	0.0	1.0	0%
1.10 Configure Catalina Policy	0	0	0	0.0	0.0	0%
1.11 Application Deployment	0	1	0	0.0	1.0	0%
1.12 Miscellaneous Configuration Settings	4	2	0	4.0	6.0	67%
Total	7	21	0	7.0	28.0	25%

1.4 Limit Server Platform Information Leaks		
1.0	1.4.5 Disable client facing Stack Traces	Fail
1.0	1.4.6 Turn off TRACE	Pass
1.5 Protect the Shutdown Port		
1.0	1.5.1 Set a nondeterministic Shutdown command value	Pass

8. “Confirm the Fail”™® © ☺

1.1.1.2.1.72 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled' Fail

Description:

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment. The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to 1.
`Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares`

Impact:

It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

Assessment:

Check that 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is configured to 'Enabled' -- [Less](#)



Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
Registry Value:	RestrictAnonymous
CIS-CAT Expected...	CIS-CAT Collected...
the registry key's type to be set to reg_dword	reg_dword
the registry key's value to be set to 1	0

[Show Rule Result XML](#)

References:

- CCE-IDv5: [CCE-10557-7](#) -- [More](#)

[Back to Summary](#)

9. “Fix The Fail”™® © ☺



1.1.1.2.1.72 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled' Fail

Description:

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment. The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to 1. `Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares`

Impact:

It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

Assessment:

Check that 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is configured to 'Enabled' -- [Less](#)

Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
Registry Value:	RestrictAnonymous
CIS-CAT Expected...	CIS-CAT Collected...
the registry key's type to be set to reg_dword	reg_dword
the registry key's value to be set to 1	0

[Show](#) Rule Result XML

References:

- [CCE-IDv5: CCE-10557-7](#) -- [More](#)

[Back to Summary](#)

10. Monitor Progress



11. Measure Configuration Change Management using the CIS Security Metrics



The screenshot displays the 'Downloads' section of the Security Benchmarks application. At the top left is the 'Security Benchmarks' logo. A navigation bar contains icons for 'People', 'Areas', 'Help', 'Downloads', 'Search', 'Starred', 'Trash', and 'Quick Add'. Below the navigation bar, the 'Downloads' title is followed by buttons for 'New Text Download', 'Upload File', and a printer icon. A breadcrumb trail reads 'Dashboard > Downloads > Security Metrics > List'. The main content area shows a list of two PDF files:

File Name	Size	Upload Date	Uploader	Actions
CIS_Security_Metrics_v1.1.0.pdf	1.90MB	Thu, Apr 28, 2011	Michelle Vogeler	View, Download
CIS_Security_Metrics-Quick_Start_Guide_v1.0.0.pdf	1.37MB	Thu, Apr 28, 2011	Michelle Vogeler	View, Download

On the right side of the file list, there are three buttons: 'All Downloads', 'Archive', and 'Desktop: Office'.

Questions about CIS-CAT?

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>
- ▶ 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

Security Metrics Initiative

- ▶ 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>
(Downloads Tab ->Security Metrics Category)

Member Support, Contact & Additional Information

Member Support for State of Idaho

- ▶ As a benefit of membership, State of Idaho 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 Peterson, Member Services Manager, Michelle.Peterson@cisecurity.org

Q&A