6: Applying Compliance Frameworks Using InSpec

Useful references for this module:

https://docs.chef.io/release/compliance_1-0/dsl_compliance.html

https://docs.chef.io/inspec_reference.html

Slide 2

Objectives

After completing this module, you should be able to:

- Translate CIS (Center for Internet Security) specifications into InSpec tests.
- Translate DoD (Department of Defense) specifications into InSpec tests.

Slide 3

CONCEPT

CIS Compliance Frameworks

The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security.

Resources include secure configuration benchmarks, automated configuration assessment tools and content, security metrics and security software product certifications.

https://benchmarks.cisecurity.org/

CHEF

Slide 4

EXERCISE

Group Lab:
Compliance Frameworks - CIS Linux

Translating a CIS benchmark into an InSpec control and Compliance profile.

Objective:

- ❑ Download the benchmark PDF for the platform of your scanning target
- ❑ Implement Section 3 - Specialty Purpose Services as InSpec controls.

CHEF

Slide 5

GL: Downloading the CIS Benchmarks for Linux

1. Go to: https://benchmarks.cisecurity.org/
2. Click the **Products & Services** tab.
3. Click **Benchmarks**.

Slide 6

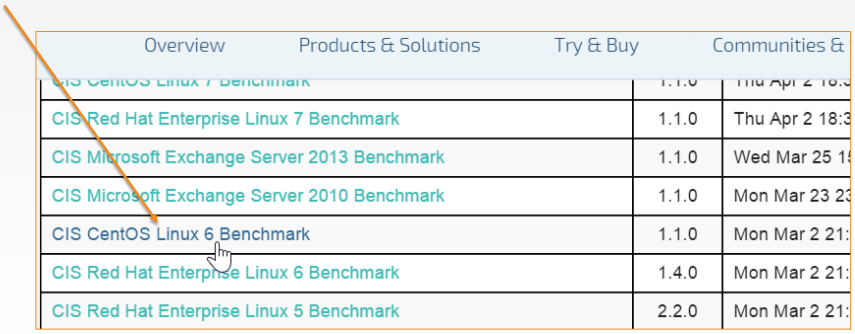
GL: Downloading the CIS Benchmarks

Scroll down to the **Available Free of Charge** section and then click **Current version of CIS Benchmarks.**

Slide 7

GL: Downloading the CIS Linux Benchmarks

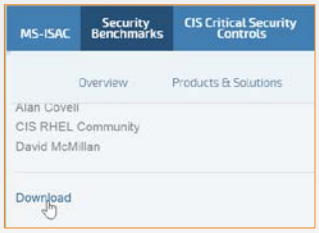
Scroll down to the benchmark for the system you're running. In our case, click the **CIS CentOS Linux 6 Benchmark** link.



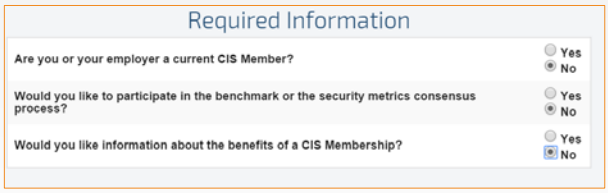
Slide 8

GL: Downloading the PDF

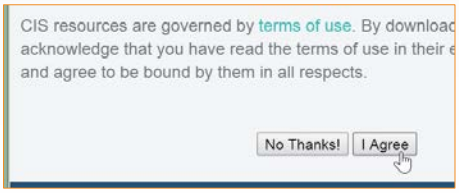
1. Scroll down to the bottom of the page and click **Download**.



2. On the resulting page, click the **Required Information** radio buttons.



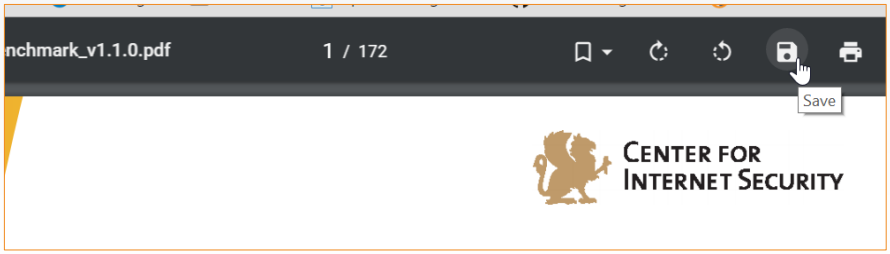
3. Then scroll down and click the **I Agree** button.



Slide 9

GL: Downloading the CIS Benchmarks

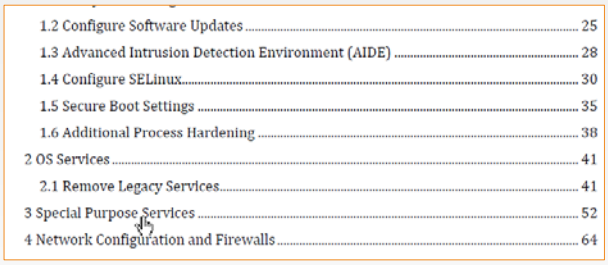
Save the PDF to your laptop. If a Save icon is not obvious, you should be able to save the PDF by right-clicking it.



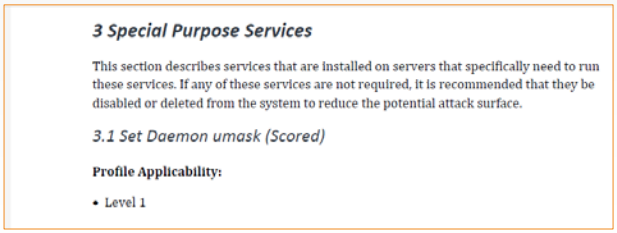
Slide 10

GL: CIS Benchmarks

Open the PDF and then from the Table of Contents, click the **Special Purpose Services** bookmark or otherwise go to that section.

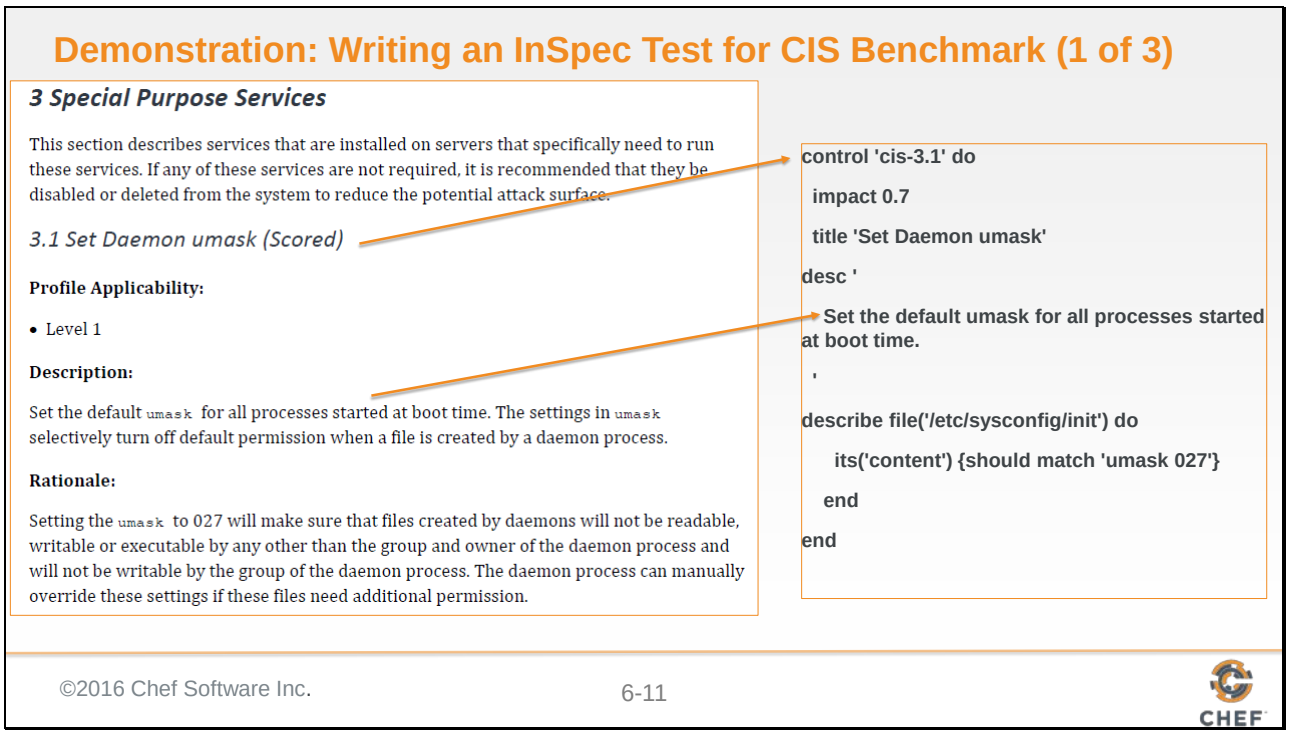


Go to Section 3.1.



CHEF

Slide 11



The text in the example on the left can be used to create a Compliance Profile control (on the right).

In this example, you can name the control the same as the section in the CIS document:
control 'cis-3.1'
The Description text from the CIS document can be used to write the `desc` section.

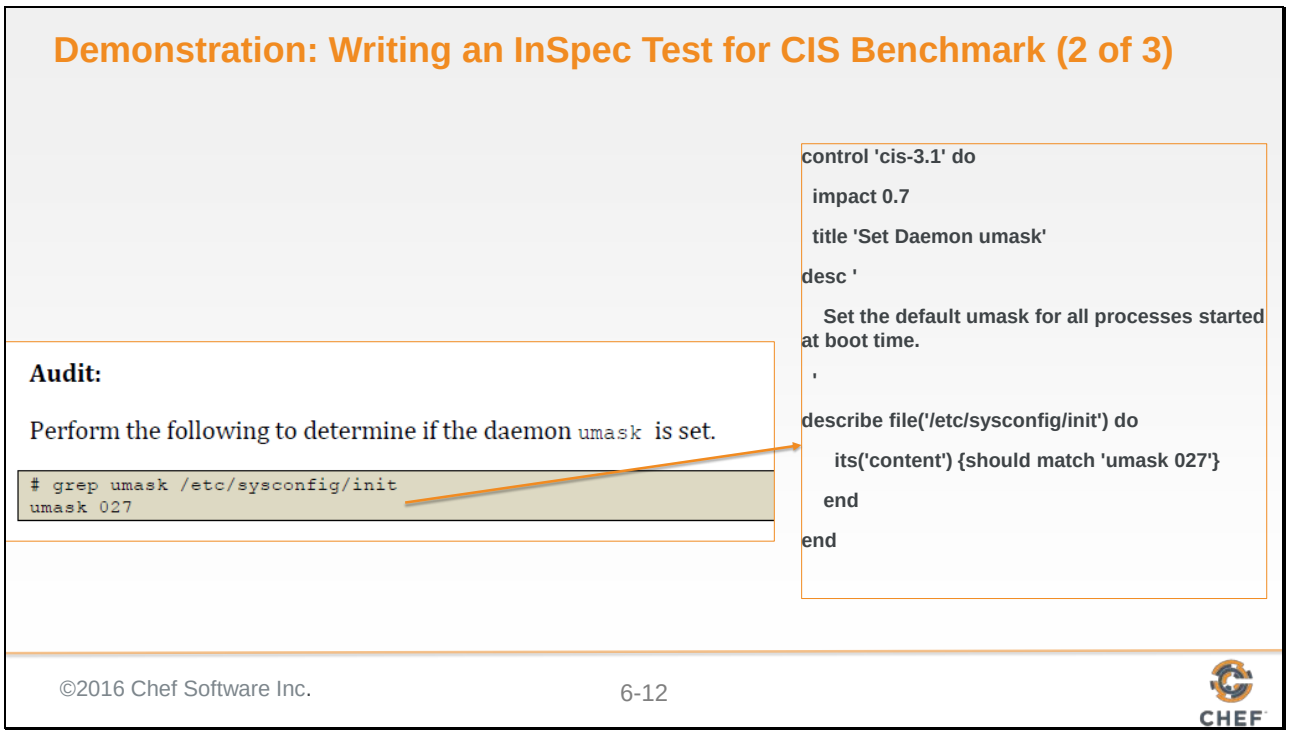
As you can see on that page, the *3.1 Set Daemon umask (Scored)* section says:

Description:

Set the default umask for all processes started at boot time. The settings in umask selectively turn off default permission when a file is created by a daemon process.

Rationale:
Setting the umask to 027 will make sure that files created by daemons will not be readable, writable or executable by any other than the group and owner of the daemon process and will not be writable by the group of the daemon process. The daemon process can manually override these settings if these files need additional permission.

Slide 12



If you scrolled down in that section, you will see an Audit example.

So based on the Audit example on the left, you could write an InSpec test as shown on the right. In this way you can subsequently use this custom profile to scan nodes for umask compliance.

https://docs.chef.io/release/compliance_1-0/dsl_compliance.html

https://docs.chef.io/inspec_reference.html

Slide 13

Demonstration: Writing an InSpec Test for CIS Benchmark (3 of 3)

```
control 'cis-3.1' do
 impact 0.7
 title 'Set Daemon umask'
desc '
   Set the default umask for all processes started
at boot time.
 '
describe file('/etc/sysconfig/init') do
     its('content') {should match 'umask 027'}
   end
end
```

After writing the test, in the workplace you should:

- Use 'inspec exec' to test the control.
- Package the custom compliance profile and upload it to your Compliance server.

After writing the test, in the workplace you should:

Use 'inspec exec' to test the control.
Package the custom compliance profile and upload it to your Compliance server.

Slide 14

EXERCISE

Group Lab:
Compliance Frameworks - CIS Windows

Translating a CIS benchmark into an InSpec control and Compliance profile.

Objective:

- ❑ Download the benchmark PDF for the platform of your scanning target
- ❑ Implement Section 3 - Specialty Purpose Services as InSpec controls.

CHEF

Slide 15

GL: Downloading the CIS Benchmarks for Windows

1. Go to: https://benchmarks.cisecurity.org/
2. Click the **Products & Services** tab.
3. Click **Benchmarks**.

Slide 16

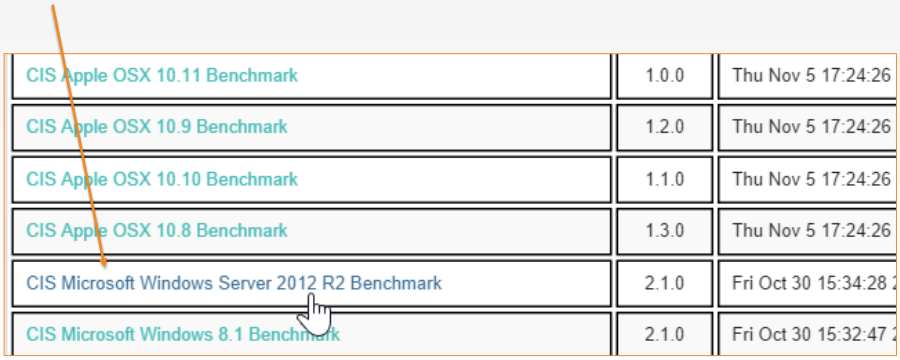
GL: Downloading the CIS Benchmarks for Windows

Scroll down to the **Available Free of Charge** section and then click **Current version of CIS Benchmarks.**

Slide 17

GL: Downloading the CIS Benchmarks for Windows

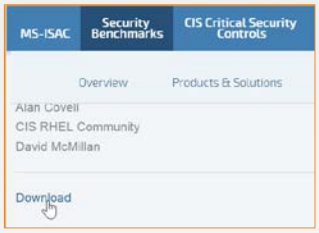
Scroll down to the benchmark for the system you're running. In our case, click the **CIS Microsoft Windows Server 2012 R2 Benchmark** link.



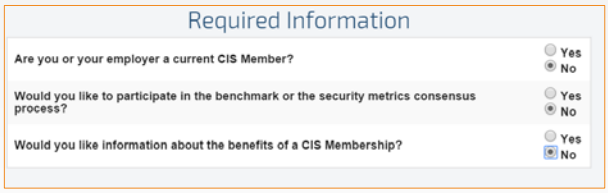
Slide 18

GL: Downloading the PDF

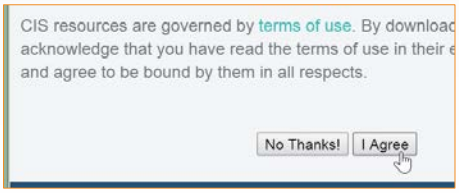
1. Scroll down to the bottom of the page and click **Download**.



2. On the resulting page, click the **Required Information** radio buttons.



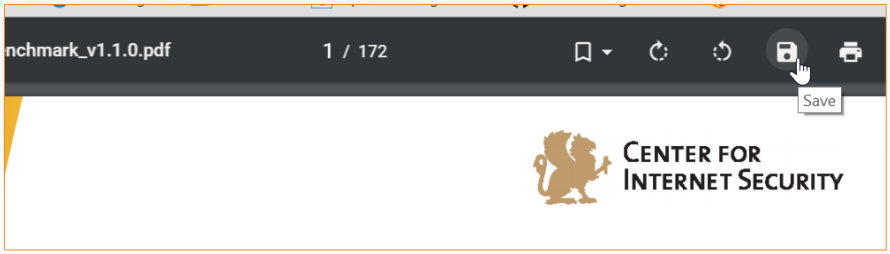
3. Then scroll down and click the **I Agree** button.



Slide 19

GL: Downloading the CIS Benchmarks for Windows

Save the PDF to your laptop. If a Save icon is not obvious, you should be able to save the PDF by right-clicking it.

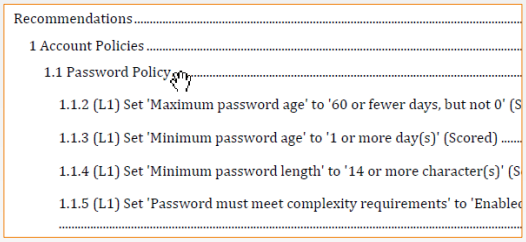


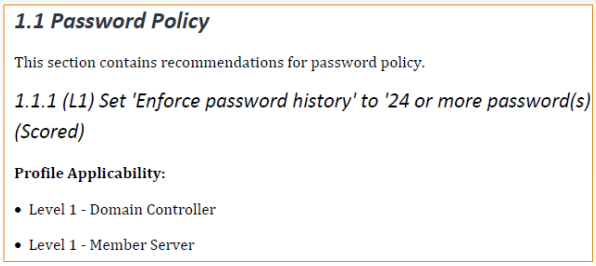
GL: CIS Benchmarks for Windows

Implement Section 1.1 - Password Policy as InSpec controls with the profile of Level 1 - Member Server.

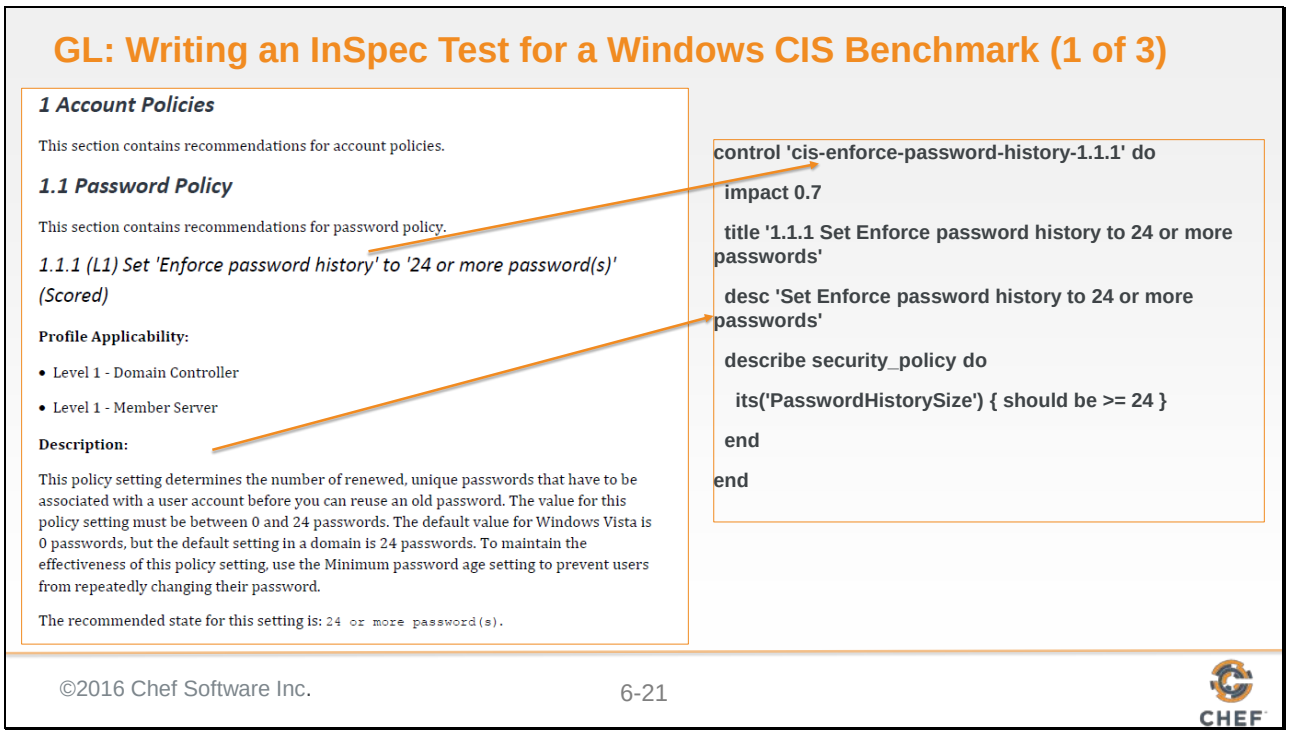
Use 'inspec exec' to test the control.

Package profile and upload to your Compliance server.





Slide 21



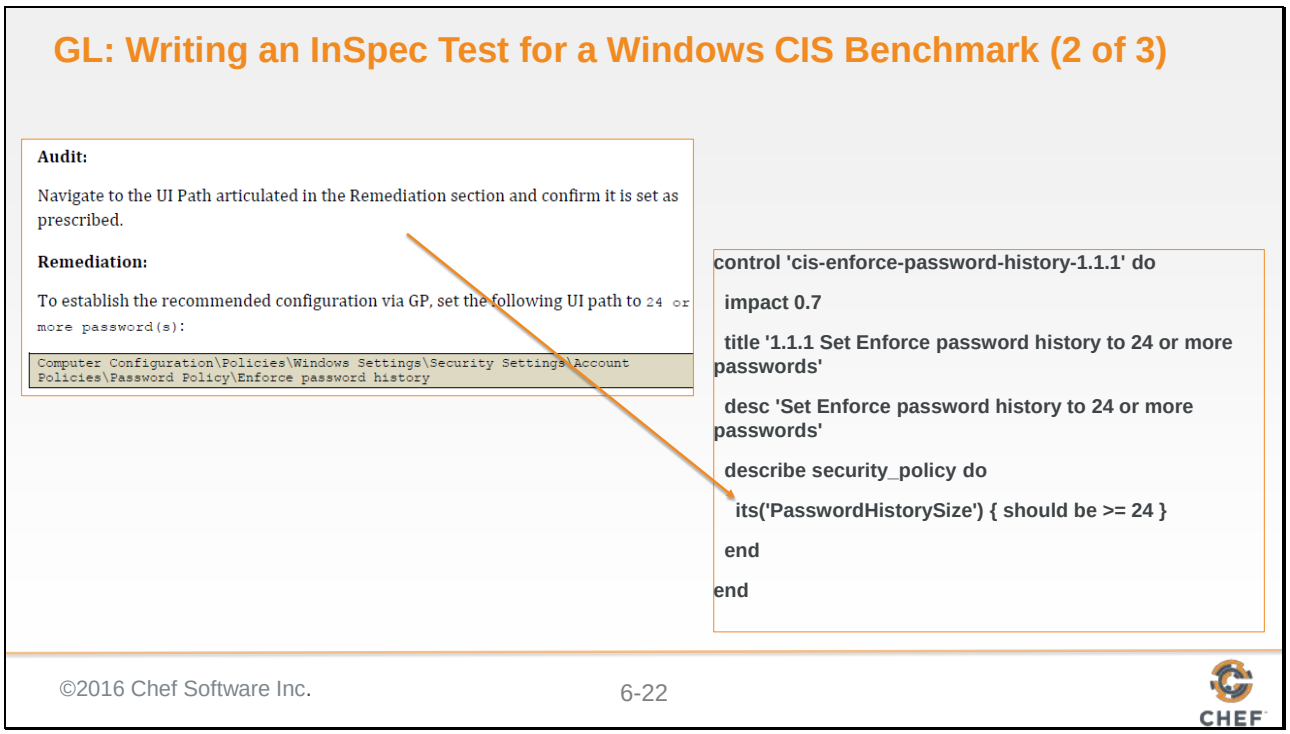
Scroll down to the *1.1 Password Policy* section,

The text in the example on the left can be used to create a Compliance Profile control (on the right).

In this example, you can name the control the same as the section in the CIS document: **cis-enforce-password-history-1.1.1**

The Description text from the CIS document can be used to write the `desc` section.

Slide 22



If you scrolled down in that section, you will see an Audit example.

So based on the Audit example on the left, you could write an InSpec test as shown on the right. In this way you can subsequently use this custom profile to scan nodes for umask compliance.

The path shown in this example could be used if you wanted to manually navigate on the Windows node to see how password history parameter is set. However, when the Compliance Server scans the node, the Compliance server's inspec will use cmd = inspec.command('secedit /export /cfg win_secpol.cfg') to locate the parameter.

https://github.com/chef/inspec/blob/master/lib/resources/security_policy.rb

Slide 23

GL: Writing an InSpec Test for a Windows CIS Benchmark (3 of 3)

This inspec code below shows how inspec can scan for security policy compliance by parsing **`secedit /export /cfg win_secpol.cfg`**.

```
# load security content
  def load
    # export the security policy
    cmd = inspec.command('secedit /export /cfg win_secpol.cfg')
    return nil if cmd.exit_status.to_i != 0
```

```
control 'cis-enforce-password-history-1.1.1' do
 impact 0.7
 title '1.1.1 Set Enforce password history to 24 or more passwords'
 desc 'Set Enforce password history to 24 or more passwords'
 describe security_policy do
  its('PasswordHistorySize') { should be >= 24 }
 end
end
```

https://github.com/chef/inspec/blob/master/lib/resources/security_policy.rb

The Compliance server's inspec will parse cmd = inspec.command('secedit /export /cfg win_secpol.cfg') to locate the parameter.

The following URL shows the full inspec/lib/resources/security_policy.rb code.

https://github.com/chef/inspec/blob/master/lib/resources/security_policy.rb

Slide 24

GL: CIS Benchmarks for Windows

After writing such a Compliance policy, in a production environment you would use 'inspec exec' to test the control.

Then you could package the profile and upload it to your Compliance server.

```
control 'cis-enforce-password-history-1.1.1' do
  impact 0.7
  title '1.1.1 Set Enforce password history to 24 or more passwords'
  desc 'Set Enforce password history to 24 or more passwords'
  describe security_policy do
    its('PasswordHistorySize') { should be >= 24 }
  end
end
```

Slide 25

CONCEPT

DoD Compliance Frameworks

Department of Defense (DoD) STIGs

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems.

CHEF

Slide 26

CONCEPT

DoD Compliance Frameworks

Department of Defense (DoD) STIGs

Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs).

The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

http://iase.disa.mil/stigs/Pages/index.aspx

CHEF

Slide 27

EXERCISE

GL: Compliance Frameworks - DoD

Translating a CIS benchmark into an InSpec control and Compliance profile.

Objective:

- ❑ Download STIGViewer2.
- ❑ Download DoD Security Rules for RHEL 6 and Windows 2012 MS (Member Server).
- ❑ Explain how to translate the DoD Security Rule into a Chaf Compliance profile control.

CHEF

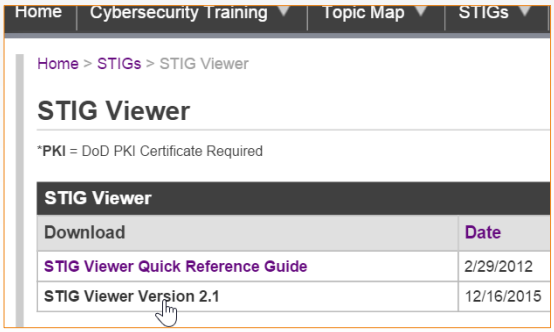
Slide 28

GL: Download STIGViewer2.x

From your local laptop, go to this site...

http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

...and download the latest version of the STIG Viewer



CHEF

Go to this site...
http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

...and download the latest version of the STIG Viewer. In this example we are downloading Version 2.1.

Slide 29

GL: Launch STIGViewer2.x

Click the STIGViewer_2.1 shortcut or otherwise launch the STIGViewer_2.1 viewer.

If it doesn't launch, you may need to install the latest Java Runtime Environment (JRE) as indicated on the next slide.

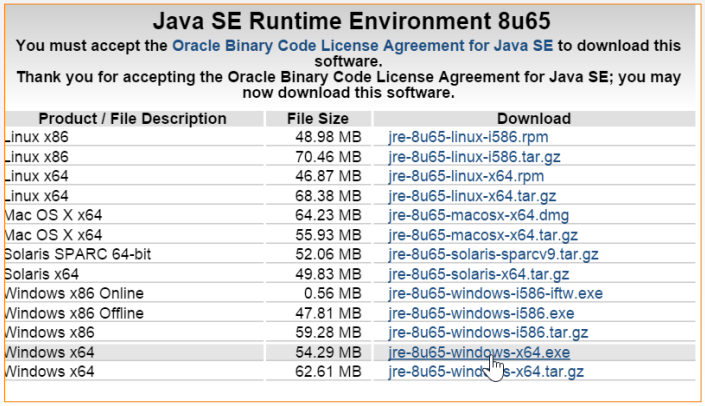
Try to run the STIG Viewer. If it fails due to a Java error, you may need to install the latest Java Runtime Environment (JRE) as indicated on the next slide.

Slide 30

GL: Download Java JRE if Necessary

You may need to install the latest Java Runtime Environment (JRE) if your STIG Viewer doesn't launch when clicked.

http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html



Java SE Runtime Environment 8u65

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.
Thank you for accepting the Oracle Binary Code License Agreement for Java SE; you may now download this software.

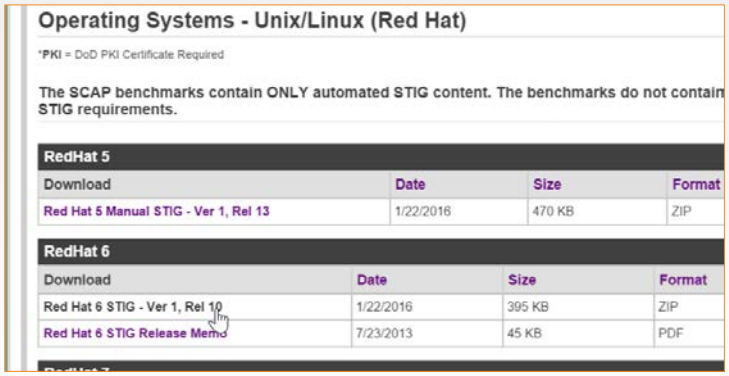
Product / File Description	File Size	Download
Linux x86	48.98 MB	jre-8u65-linux-i586.rpm
Linux x86	70.46 MB	jre-8u65-linux-i586.tar.gz
Linux x64	46.87 MB	jre-8u65-linux-x64.rpm
Linux x64	68.38 MB	jre-8u65-linux-x64.tar.gz
Mac OS X x64	64.23 MB	jre-8u65-macosx-x64.dmg
Mac OS X x64	55.93 MB	jre-8u65-macosx-x64.tar.gz
Solaris SPARC 64-bit	52.06 MB	jre-8u65-solaris-sparcv9.tar.gz
Solaris x64	49.83 MB	jre-8u65-solaris-x64.tar.gz
Windows x86 Online	0.56 MB	jre-8u65-windows-i586-iftw.exe
Windows x86 Offline	47.81 MB	jre-8u65-windows-i586.exe
Windows x86	59.28 MB	jre-8u65-windows-i586.tar.gz
Windows x64	54.29 MB	jre-8u65-windows-x64.exe
Windows x64	62.61 MB	jre-8u65-windows-x64.tar.gz

Slide 31

GL: Download STIG Profiles for Red Hat 6

Download the STIG profiles for RHEL 6 from this site and remember the location to where you downloaded onto your laptop.

http://iase.disa.mil/stigs/os/unix-linux/Pages/red-hat.aspx



Operating Systems - Unix/Linux (Red Hat)

*PKI = DoD PKI Certificate Required

The SCAP benchmarks contain ONLY automated STIG content. The benchmarks do not contain STIG requirements.

RedHat 5			
Download	Date	Size	Format
Red Hat 5 Manual STIG - Ver 1, Rel 13	1/22/2016	470 KB	ZIP

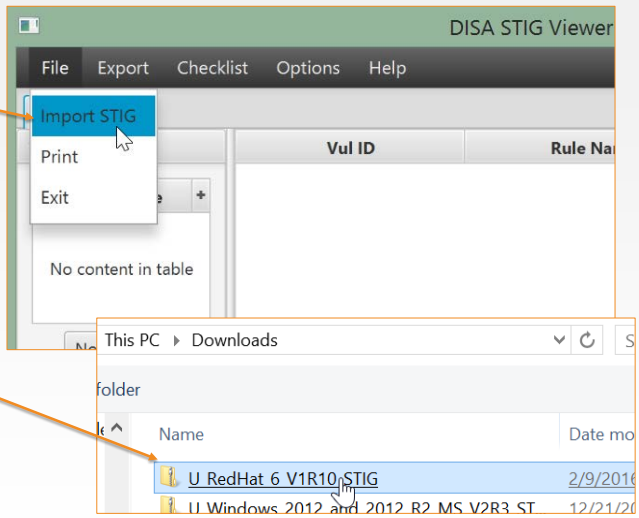
RedHat 6			
Download	Date	Size	Format
Red Hat 6 STIG - Ver 1, Rel 10	1/22/2016	395 KB	ZIP
Red Hat 6 STIG Release Memo	7/23/2013	45 KB	PDF

Slide 32

GL: Import STIG Profiles for Red Hat 6

Click **File > Import STIG**.

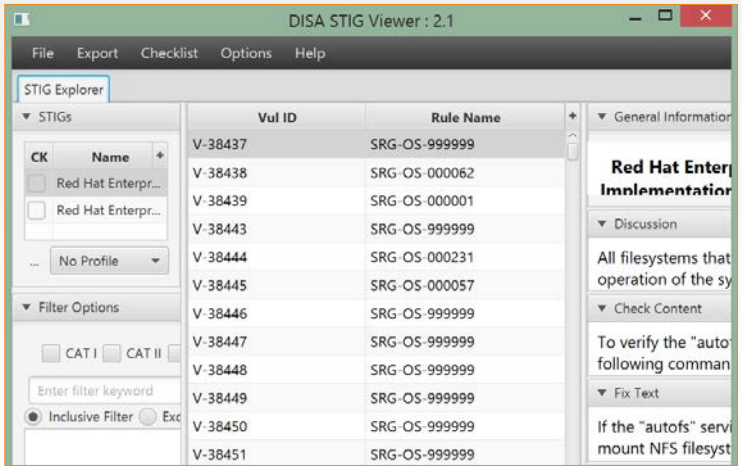
Navigate to the STIG profiles file you just downloaded and click the file.



Slide 33

GL: STIG Profiles for Red Hat 6

Your STIG viewer should now be populated with DoD Security Rule profiles.

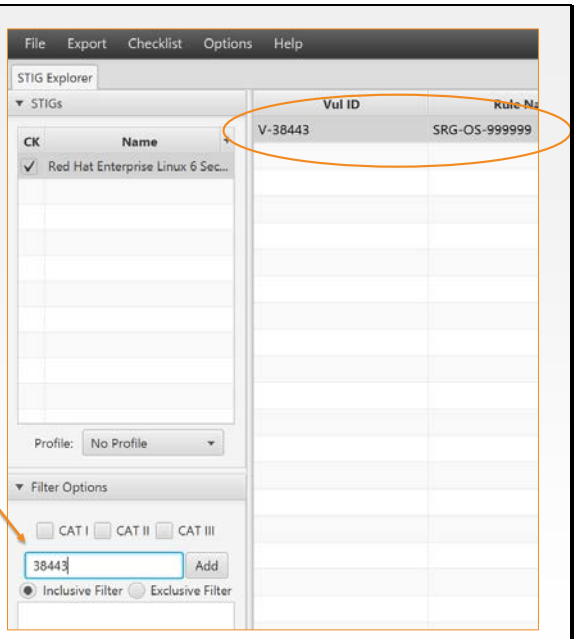


Slide 34

GL: Filter STIG Profiles

Type **38443** in the filter field.

Notice how the center pane now lists only one DoD Security Rule.



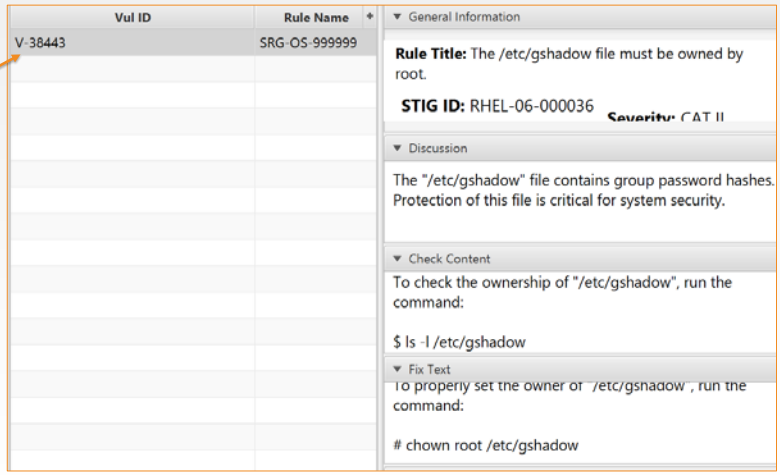
CHEF

TBD SCAP Roadmap.

Slide 35

GL: Writing Compliance Profiles from DoD Rules

```
#The /etc/gshadow file must be owned by
root.

#Severity: Medium

#The "/etc/gshadow" file contains group
password hashes. Protection of this

#file is critical for system security.


control 'v-38443-gshadow' do

  impact 0.5

  title 'v-38443: verify gshadow is
owned by root'

  describe file('/etc/gshadow') do

    it { should be_owned_by 'root' }

  end

end
```



The image on the right shows the right-side pane of the STIG viewer including the details of this DoD Security rule. This rule states that /etc/gshadow must be owned by root.

The image on the left shows a Chef Compliance Profile that was written based on the details of this DoD Security rule. Notice how the Chef Compliance Profile control name reflects the DoD Security rule name. This is a best practice that you should follow when writing Chef Compliance Profiles for DoD Security rules.

Slide 36

GL: Writing Compliance Profiles from DoD Rules

If you have permissions you can access a list of predefined DoD controls at this link:

https://github.com/chef/compliance-profiles/tree/DOD-STIG/stig/rhel6/test

```
#The /etc/gshadow file must be owned by
root.

#Severity: Medium

#The "/etc/gshadow" file contains group
password hashes. Protection of this

#file is critical for system security.


control 'v-38443-gshadow' do

  impact 0.5

  title 'v-38443: verify gshadow is
owned by root'

  describe file('/etc/gshadow') do

    it { should be_owned_by 'root' }

  end

end
```


CHEF

Slide 37

DoD STIG References

Windows 2012 - http://iase.disa.mil/stigs/os/windows/Pages/2012.aspx

Unix/Linux (Red Hat) - http://iase.disa.mil/stigs/os/unix-linux/Pages/red-hat.aspx

All Operating Systems - http://iase.disa.mil/stigs/os/Pages/index.aspx

Slide 38

Compliance Profiles for Compliance Premium

Chef Compliance Premium customers can download all CIS profiles in a package that can be directly uploaded to the Chef Compliance server.

In the near future, NIST Security Standards/DoD profiles will be available for Chef Compliance Premium customers in a package that can be directly uploaded to the Chef Compliance server.

Slide 39