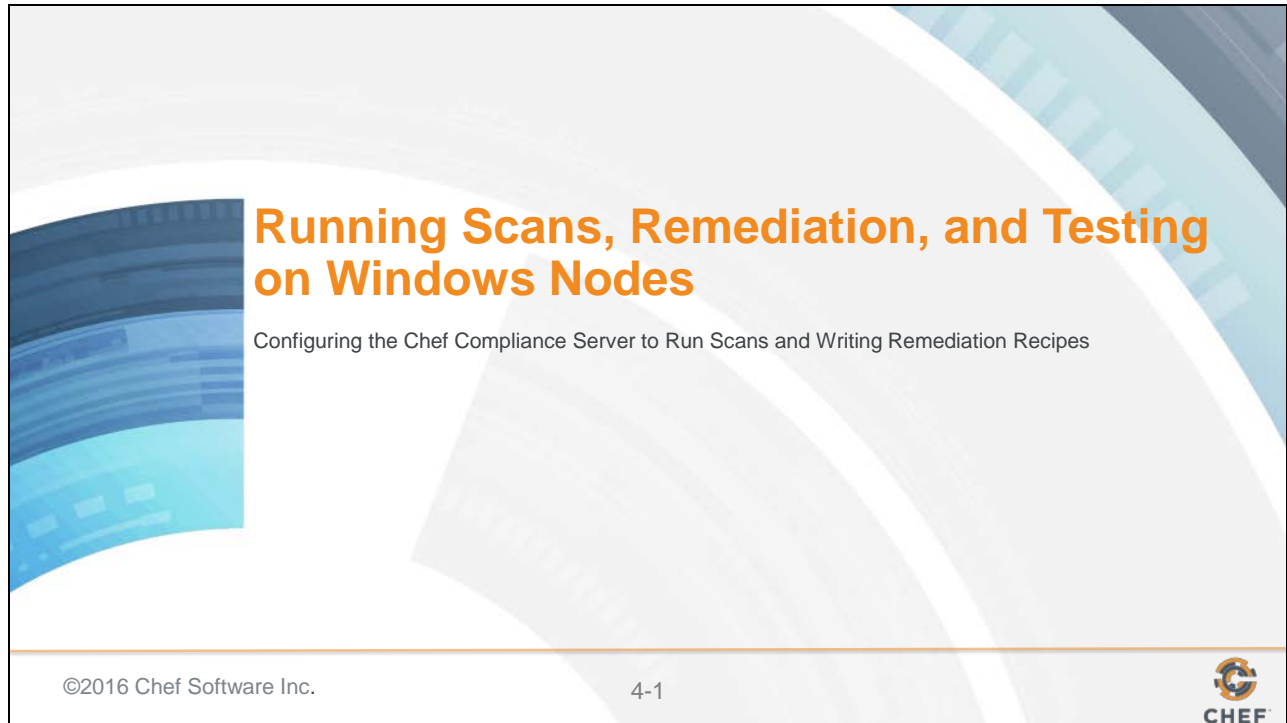


## 4: Running Scans, Remediation, and Testing on Windows Nodes



## Slide 2

## Objectives

After completing this module, you should be able to:

- Add a Windows node to test for compliance.
- Run a Compliance scan.
- Test for compliance with InSpec from the CLI.
- Remediate a compliance issue.
- Use Test Kitchen to test your remediation.
- Rescan the node and ensure compliance.

Slide 3

# EXERCISE



## Group Lab: Adding a Node to Scan

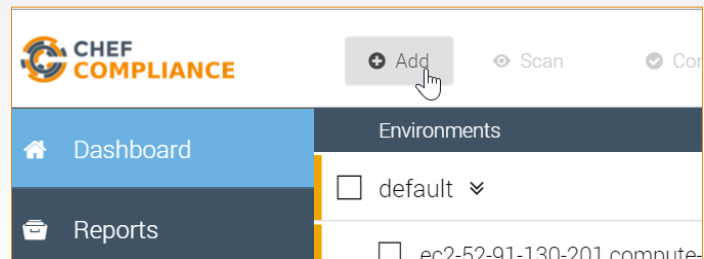
**Objective:**

- ☐ Add a Windows Node to Scan
- ☐ Test connectivity

## Slide 4

## GL: Adding a Node to Scan

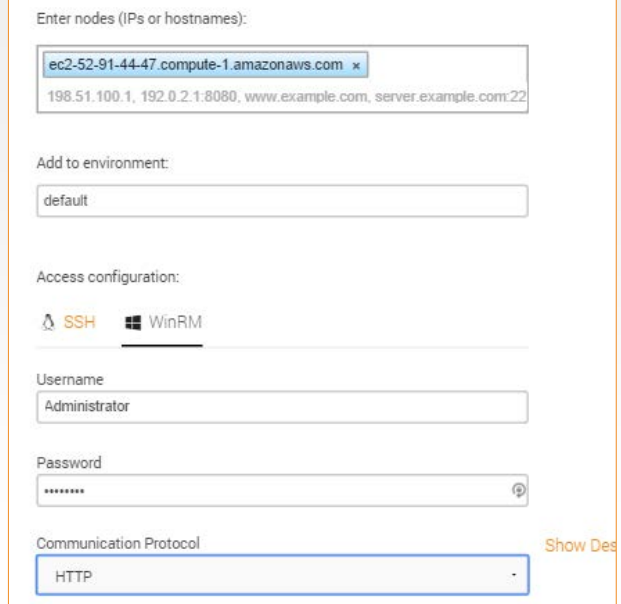
1. From your Chef Compliance Dashboard, click Add Node.



## Slide 5

## GL: Adding a Node

2. From the resulting page, enter the Windows node's FQDN or IP address.
3. Select the **default** environment.
4. Click the **WinRM** Access configuration.
5. Type **Administrator** in the **Username** field.
6. Type the password (**Cod3Can!**) in the password field.



The screenshot shows the 'Add Node' configuration page in Chef. It includes a text area for 'Enter nodes (IPs or hostnames):' with a list of addresses including 'ec2-52-91-44-47.compute-1.amazonaws.com'. Below this is a dropdown for 'Add to environment:' set to 'default'. The 'Access configuration:' section has 'SSH' and 'WinRM' options, with 'WinRM' selected. The 'Username' field contains 'Administrator' and the 'Password' field contains masked characters. The 'Communication Protocol' dropdown is set to 'HTTP'. A 'Show Details' link is visible on the right.

Be sure you are using the hostname of the Windows target node that you noted previously in class.



In the workplace, the target node's username and password will likely be different than shown in this example.

## Slide 6

## GL: Adding a Node to Scan

7. Ensure the **HTTP** Communication Protocol is set.
8. Click the **Add 1 node** button.

Access configuration:

 SSH  WinRM

Username

Password

Communication Protocol

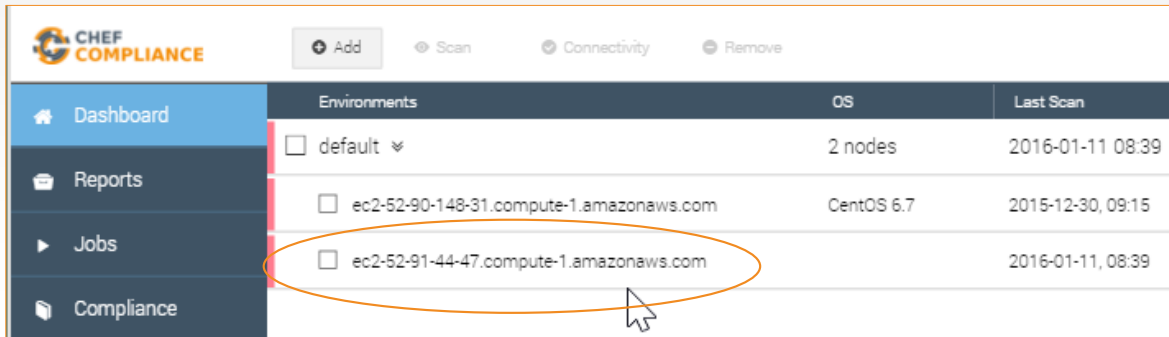
[Show](#)

**Add 1 node**

## Slide 7

## GL: Adding a Node to Scan

At this point your Compliance Dashboard should list the node you just added. In the next step we'll modify the Windows node name to make it easier to differentiate it from your Linux node.



	Environments	OS	Last Scan
<input type="checkbox"/>	default ▾	2 nodes	2016-01-11 08:39
<input type="checkbox"/>	ec2-52-90-148-31.compute-1.amazonaws.com	CentOS 6.7	2015-12-30, 09:15
<input type="checkbox"/>	ec2-52-91-44-47.compute-1.amazonaws.com		2016-01-11, 08:39

## Slide 8

## GL: Modify the Node Name

1. Click the **Windows node**.
2. From the resulting page, click **Configuration**.


Environments	OS
<input type="checkbox"/> default ▾	2 nodes
<input type="checkbox"/> ec2-52-90-148-31.compute-1.amazonaws.com	CentOS 6.7
<input type="checkbox"/> ec2-52-91-44-47.compute-1.amazonaws.com	

default / ec2-52-91-44-47.compute-1.amazonaws.com

Status Compliance Patch Level **Configuration**

Node Status

Scan Connectivity





## Slide 9

## GL: Modify the Node Name

3. Type **Windows** at the beginning of the **Name:** field.

**Important:** Do not change the value in the **IP or Hostname** field because that field is used to connect to your node.


4. Click **Save**.


The screenshot shows the 'Node Configuration' page in the Chef interface. At the top, there are tabs for 'Status', 'Compliance', 'Patch Level', and 'Configuration'. The 'Configuration' tab is active. Below the tabs, the 'Node Configuration' section contains three main fields: 'Name:', 'IP or Hostname:', and 'Access configuration:'. The 'Name:' field is highlighted with a blue border and contains the text 'Windows' followed by 'ec2-52-91-44-47.compute-1.amazonaws.com'. The 'IP or Hostname:' field contains the same IP address. The 'Access configuration:' section has two options: 'SSH' (selected) and 'WinRM'. Below these fields, there is a 'Save' button highlighted with an orange border and a mouse cursor pointing at it.


## Slide 10


## GL: Modify the Node Name


Now you can more easily differentiate your Windows node from your Linux node.





 Add


 Scan


 Connectivity


 Remove

 Dashboard

 Reports

 Jobs

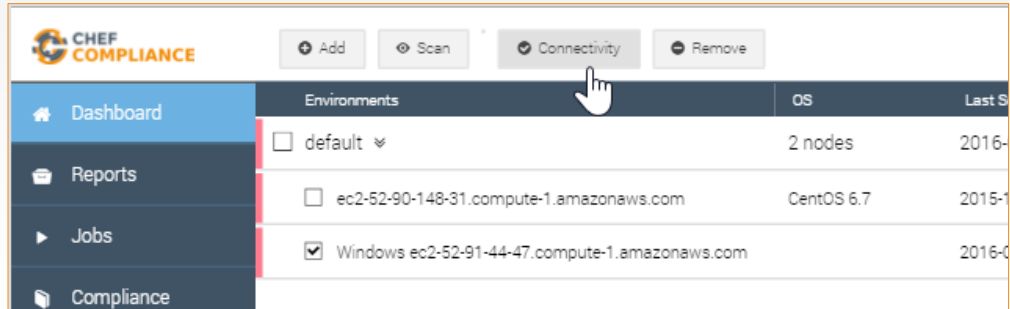
 Compliance

Environments	OS	Last Scan
<input type="checkbox"/> default 	2 nodes	2016-01-11 08:39
<input type="checkbox"/> ec2-52-90-148-31.compute-1.amazonaws.com	CentOS 6.7	2015-12-30, 09:15
<input type="checkbox"/> Windows ec2-52-91-44-47.compute-1.amazonaws.com		2016-01-11, 08:39

## Slide 11

## GL: Testing Connectivity to your Node


1. Click the **check box** next to your Windows node and then click the **Connectivity** button.



## Slide 12

## GL: Testing Connectivity to your Node

The Status column of your node should now indicate **Connection established**.



Dashboard

Reports

Jobs

Compliance

Dashboard / Connectivity Report

Node	Environment	Message	Status
<div><div></div>Windows ec2-52-91-44-47.compute-1.amazonaws.com</div>	default		Connection established

If your Status column does not indicate **Connection established**, please notify the instructor.

Slide 13

# EXERCISE



## Group Lab: Running a Scan

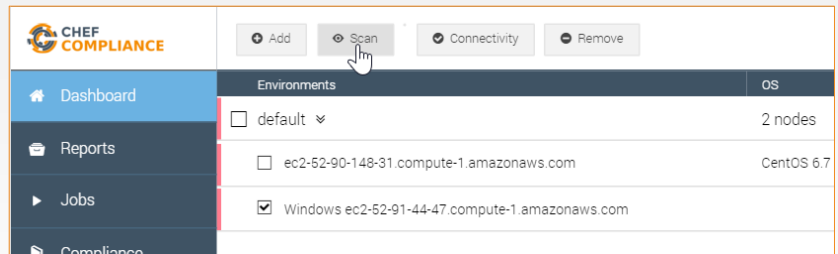
### Objective:

- ☐ Run a Compliance scan.
- ☐ View the output of a scan.

## Slide 14

## GL: Running a Scan

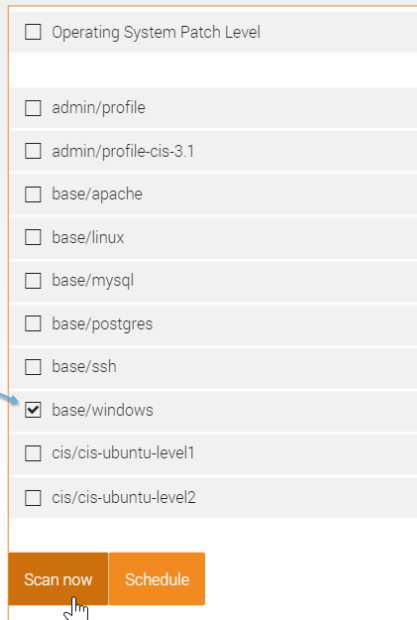
1. Click the **check box** next to your node and then click the **Scan** button.



## Slide 15

## GL: Running a Scan

2. From the resulting page, check the **base/windows** profile and uncheck any other check boxes.
3. Click the **Scan now** button.



<input type="checkbox"/>	Operating System Patch Level
<input type="checkbox"/>	admin/profile
<input type="checkbox"/>	admin/profile-cis-3.1
<input type="checkbox"/>	base/apache
<input type="checkbox"/>	base/linux
<input type="checkbox"/>	base/mysql
<input type="checkbox"/>	base/postgres
<input type="checkbox"/>	base/ssh
<input checked="" type="checkbox"/>	base/windows
<input type="checkbox"/>	cis/cis-ubuntu-level1
<input type="checkbox"/>	cis/cis-ubuntu-level2

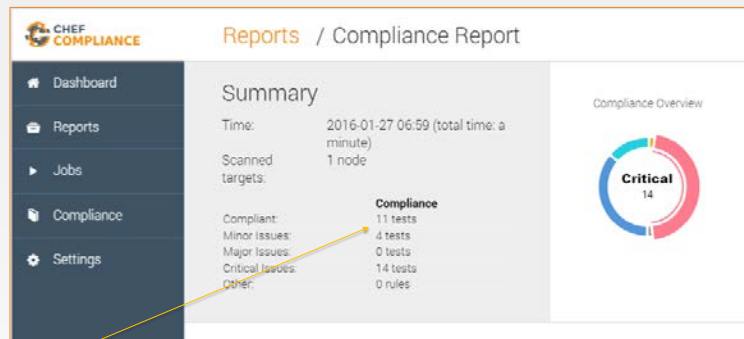
Scan now Schedule

## Slide 16

## Scan Results

A Compliance Report should now display and your scan results should be similar to that shown here.

Notice how in the upper Summary section in this example, 11 tests were compliant and 14 tests show critical issues with ssh.





## Slide 17

## Scan Results

The bottom half of the Compliance Report shown here has a table of details of the scan, similar to what you saw in the Linux example.

Notice how one of the critical issues regards Strong Windows NTLMv2 Authentication Enabled

Ports	Hostname	Compliant	Minor Issues	Major Issues	Critical Issues	Skipped
Ports	Windows ec2-52-91-44-47.compute-1.amazonaws.com	11	4	0	14	0
Compliance	base/windows: Windows Remote Desktop Configured to Only Allow System Administrators Access				Critical Issues	
Windows	base/windows: Minimum Windows Password Length Configured to be at Least 8 Characters				Critical Issues	
	base/windows: Set Windows Account lockout threshold				Critical Issues	
	base/windows: Account Logon Audit Log				Critical Issues	
	base/windows: Audit Application Group Management				Critical Issues	
	base/windows: Audit Distributed Group Management				Critical Issues	
	base/windows: All Shares are Configured to Prevent Anonymous Access				Critical Issues	
	base/windows: Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled				Critical Issues	
	base/windows: Enable Strong Encryption for Windows Network Sessions on Clients				Critical Issues	
	base/windows: Enable Strong Encryption for Windows Network Sessions on Servers				Critical Issues	
	base/windows: IE 64-bit tab				Critical Issues	
	base/windows: Run antimalware programs against ActiveX controls				Critical Issues	
	base/windows: Windows Remote Desktop Configured to Always Prompt for Password				Critical Issues	
	base/windows: Strong Encryption for Windows Remote Desktop Required				Critical Issues	
	base/windows: Configure System Event Log (Application)				Minor Issues	
	base/windows: Audit Application Group Management					
	base/windows: Audit Distributed Group Management					
	base/windows: All Shares are Configured to Prevent Anonymous Access					
	base/windows: Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled					
	Registry Key HKLM\System\CurrentControlSet\Control\Lsa should exist Registry Key HKLM\System\CurrentControlSet\Control\Lsa\CompatibilityLevel should eq 4					
	base/windows: Enable Strong Encryption for Windows Network Sessions on Clients					
	base/windows: Enable Strong Encryption for Windows Network Sessions on Servers					
	base/windows: IE 64-bit tab					
	base/windows: Run antimalware programs against ActiveX controls					
	base/windows: Windows Remote Desktop Configured to Always Prompt for Password					
	base/windows: Strong Encryption for Windows Remote Desktop Required					

The bottom half of the Compliance Report has a table of details of test results.

These are sorted by severity so the critical issues are listed at the top and the compliant items are at the bottom of the list.

If you click an issue as shown here, a bit more information about the issue displays, but that's not really telling us much.

## Slide 18

## GL: Profile

To view the InSpec code that comprises this profile, do the following:

1. Click the **Compliance** button.
2. Click the relevant profile category (**Windows Base ...**).
3. Scroll down and click the **Strong Windows NTLMv2...** profile.

The screenshot shows the Chef Compliance web interface. On the left is a dark sidebar with a menu containing 'Dashboard', 'Reports', 'Jobs', 'Compliance', and 'Settings'. The 'Compliance' item is highlighted. An orange arrow points from the first step of the instructions to this menu. On the right, the 'Reports / Compliance' page is shown. It has a 'Summary' section and a list of profile categories: 'Basic Linux', 'Basic MySQL', 'Basic PostgreSQL', 'Basic SSH', and 'Windows Base Security'. An orange arrow points from the second step of the instructions to the 'Windows Base Security' category. Below this, a detailed view of the 'Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled' profile is shown, including its InSpec code. An orange arrow points from the third step of the instructions to this profile view.

```
rule 'windows-base-201' do
  impact 1.0
  title 'Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled'
  desc '
    @link: http://support.microsoft.com/en-us/kb/823659
  '
  describe registry_key('HKLM\System\CurrentControlSet\Control\Lsa') do
    it { should exist }
    its('lmCompatibilityLevel') { should eq 4 }
  end
end
```

Note that the `rule` designation will be changed to `control` in an upcoming release.

## Slide 19

## Discussion: InSpec Profile Code

You can see in the bottom image where the Registry Key is not set.

In a production environment you'd want to write a Chef recipe to remediate this issue.

The screenshot displays two parts of the InSpec profile code. The top part shows a rule named 'windows-base-201' with a title 'Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled' and a description linking to a Microsoft support article. The code describes a registry key 'HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa' and checks if its 'LmCompatibilityLevel' is set to 4. The bottom part shows the Windows Registry Editor with the path 'Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa' selected, displaying various registry values like 'LsaCfgParameters', 'LsaPolicies', 'LsaSecurity', etc.

```
Force encrypted Windows network passwords
Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled
@link: http://support.microsoft.com/en-us/kb/823659

rule 'windows-base-201' do
  impact 1.0
  title 'Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled'
  desc '
    @link: http://support.microsoft.com/en-us/kb/823659
  '
  describe registry_key('HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa') do
    it { should exist }
    its('LmCompatibilityLevel') { should eq 4 }
  end
end
```

Enable Strong Encryption

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

## Slide 20

# PROBLEM



## Let's Remediate the Issue

Now that we've identified the issue, let's write a recipe on the target node to remediate the issue.

Then we'll run the compliance scan again to see if we successfully remediated the issue.

**Note:** In this course we will write a recipe directly on the node that we're running scans on. Of course in a production environment you will likely write such recipes locally and upload them to Chef Server. Then the nodes would converge the recipes on their next chef-client run.

Slide 21

# EXERCISE



## GL: Remediating the Issue

### Objective:

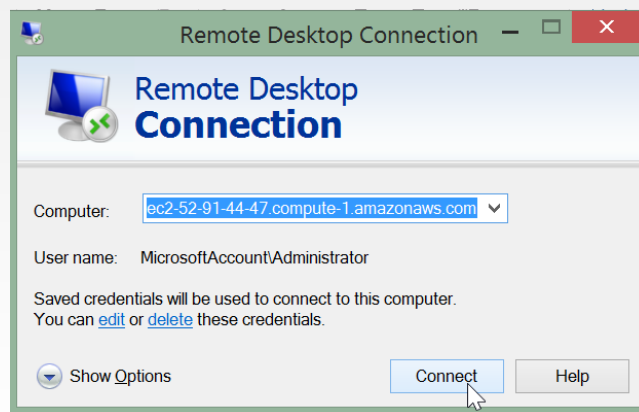
- ☐ Write a remediation recipe on that node
- ☐ Test for compliance with InSpec from the command line interface (CLI)
- ☐ Converge the recipe
- ☐ Rescan the node and ensure compliance

## Slide 22

## GL: Remediating the Issue

Log in to your target node (not your compliance server node) using your RPD client.

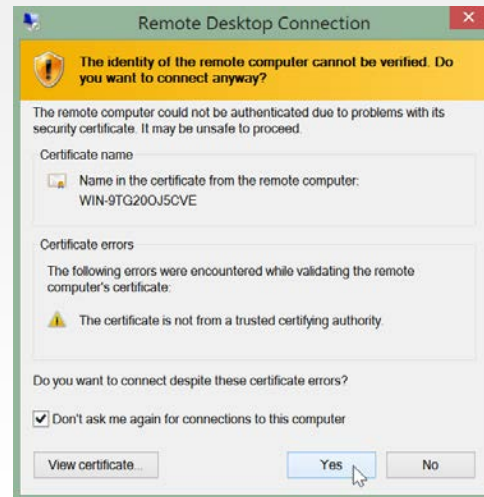
You can use only the IP address instead of the FQDN that this image shows.



## Slide 23

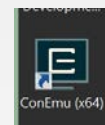
## GL: Remediating the Issue

If you get a warning like this, click **Yes**.



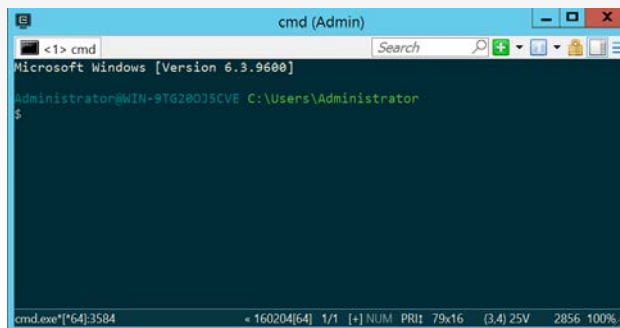
## GL: Remediating the Issue

Double-click the ConEmu(x64) icon on the Windows desktop to start that terminal.



At this point the ConEmu terminal should display and you should be in the home directory.

C:\Users\Administrator





## GL: Create and Change to a 'cookbooks' Directory



```
$ mkdir cookbooks  
$ cd cookbooks
```

From the home directory (C:\Users\Administrator\), create a **`cookbooks`** directory and navigate into it.

## Slide 26

## GL: Create a Windows Access Cookbook



```
$ chef generate cookbook windows_access
```

```
Compiling Cookbooks...
```

```
Recipe: code_generator::cookbook
```

```
  * directory[C:/Users/Administrator/cookbooks/windows_access] action create
    - create new directory C:/Users/Administrator/cookbooks/windows_access
  * template[C:/Users/Administrator/cookbooks/windows_access/metadata.rb] action
  create_if_missing
    - create new file C:/Users/Administrator/cookbooks/windows_access/metadata.rb
    - update content in file C:/Users/Administrator/cookbooks/windows_access/metadata.rb from
  none to 18be67
    (diff output suppressed by config)
  * template[C:/Users/Administrator/cookbooks/windows_access/README.md] action
  create_if_missing
    - create new file C:/Users/Administrator/cookbooks/windows_access/README.md
    - update content in file C:/Users/Administrator/cookbooks/windows_access/README.md from
  none to 481e5e
```

## Slide 27

## GL: Create an Authentication Recipe



```
$ chef generate recipe windows_access authentication
```

```
Compiling Cookbooks...
Recipe: code_generator::recipe
  * directory[./windows_access/spec/unit/recipes] action create (up to date)
  * cookbook_file[./windows_access/spec/spec_helper.rb] action create_if_missing (up to date)
  * template[./windows_access/spec/unit/recipes/authentication_spec.rb] action
  create_if_missing
    - create new file ./windows_access/spec/unit/recipes/authentication_spec.rb
    - update content in file ./windows_access/spec/unit/recipes/authentication_spec.rb from
      none to 021637
      (diff output suppressed by config)
  * template[./windows_access/recipes/authentication.rb] action create
    - create new file ./windows_access/recipes/authentication.rb
    - update content in file ./windows_access/recipes/authentication.rb from none to 11d9b9
      (diff output suppressed by config)
```

## Slide 28

## GL: Write the Authentication Recipe

 ~/cookbooks/windows\_access/recipes/authentication.rb

```
# Cookbook Name:: windows_access
# Recipe:: authentication
# Copyright (c) 2016 The Authors, All Rights Reserved.

lsa_key = 'HKLM\System\CurrentControlSet\Control\Lsa'

registry_key lsa_key do
  values [{
    :name => 'LmCompatibilityLevel',
    :type => :dword,
    :data => 4
  }]
end
```

You can use Atom to edit this file.

# EXERCISE



## GL: Remediating the Issue

### Objective:

- ✓ Write a remediation recipe on that node
- ❑ Test for compliance with InSpec from the command line interface (CLI)
- ❑ Converge the recipe
- ❑ Rescan the node and ensure compliance

Slide 30

## GL: Create the `inspec` Directory



```
$ mkdir windows_access\test\integration\authentication
$ mkdir windows_access\test\integration\authentication\inspec
```

Directory:

C:\Users\Administrator\cookbooks\windows\_access\test\integration\authentica...

Mode	LastWriteTime	Length	Name
----	-----	-----	----
d----	2/9/2016 9:06 PM		inspec

You should still be in the C:\Users\Administrator\cookbooks\ directory prior to running these commands.

## Slide 31

## GL: Create the `auth` Specification File



```
~/cookbooks/windows_access/test/integration/authentication/inspec/auth_spec.rb
```

```
rule 'windows-base-201' do
  impact 1.0
  title 'Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled'
  desc '
    @link: http://support.microsoft.com/en-us/kb/823659
  '
  describe registry_key('HKLM\System\CurrentControlSet\Control\Lsa') do
    it { should exist }
    its('LmCompatibilityLevel') { should eq 4 }
  end
end
```

You can use Atom to create this file.

Slide 32

## GL: Run InSpec from the CLI



```
$ inspec exec  
windows_access\test\integration\authentication\inspec\auth_spec.rb
```

```
.F
```

```
Failures:
```

```
1) Registry Key HKLM\System\CurrentControlSet\Control\Lsa  
LmCompatibilityLevel should eq 4
```

```
Failure/Error: its('LmCompatibilityLevel') { should eq 4 }
```

```
expected: 4  
got: nil
```

This command assumes you are still at C:\Users\Administrator\cookbooks\ when you run it.



Slide 33

# EXERCISE



## GL: Remediating the Issue

### Objective:

- ✓ Write a remediation recipe on that node
- ✓ Test for compliance with InSpec from the command line interface (CLI)
- ❑ Converge the recipe
- ❑ Rescan the node and ensure compliance

## GL: Converge the Recipe



```
$ chef-client --local-mode -r 'recipe[windows_access::authentication]'
```

```
Synchronizing Cookbooks:
```

```
- windows_access (0.1.0)
```

```
Compiling Cookbooks...
```

```
Converging 1 resources
```

```
Recipe: windows_access::authentication
```

```
* registry_key[HKLM\System\CurrentControlSet\Control\Lsa] action create  
- set value {:name=>"LmCompatibilityLevel", :type=>:dword, :data=>4}
```

```
Running handlers:
```

```
Running handlers complete
```

```
Chef Client finished, 1/1 resources updated in 11 seconds
```

This command assumes you are still at C:\Users\Administrator\cookbooks\ when you run it.

Slide 35

## GL: Run InSpec from the CLI



```
$ inspec exec  
windows_access\test\integration\authentication\inspec\auth_spec.rb
```

```
..
```

```
Finished in 2.16 seconds (files took 2.48 seconds to load)
```

```
2 examples, 0 failures
```

This command assumes you are still at C:\Users\Administrator\cookbooks\ when you run it.

Slide 36

# EXERCISE



## GL: Remediating the Issue

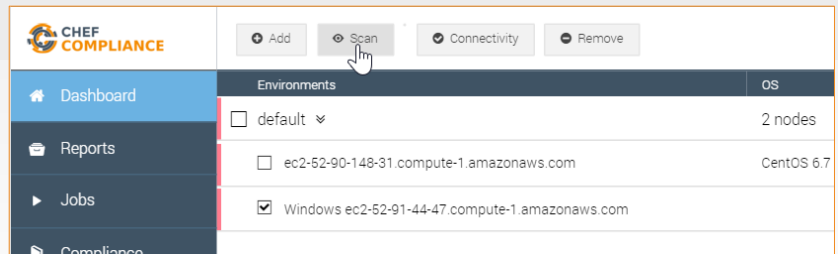
### Objective:

- ✓ Write a remediation recipe on that node
- ✓ Test for compliance with InSpec from the command line interface (CLI)
- ✓ Converge the recipe
- ❑ Rescan the node and ensure compliance

## Slide 37

## GL: Running a Scan

1. Click the **check box** next to your node and then click the **Scan** button.

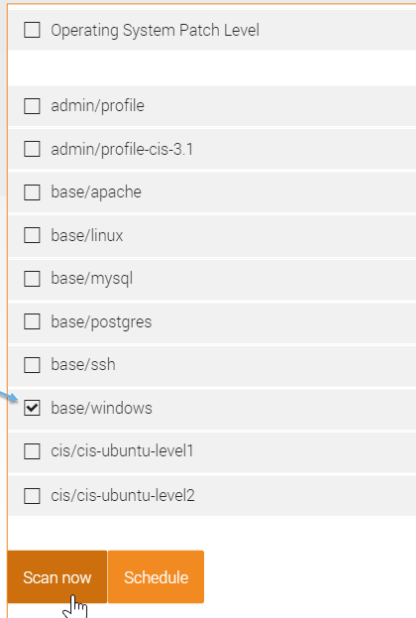


## Slide 38

## GL: Running a Scan

2. From the resulting page, check the **base/windows** profile and uncheck any other check boxes.

3. Click the **Scan now** button.




<input type="checkbox"/>	Operating System Patch Level
<input type="checkbox"/>	admin/profile
<input type="checkbox"/>	admin/profile-cis-3.1
<input type="checkbox"/>	base/apache
<input type="checkbox"/>	base/linux
<input type="checkbox"/>	base/mysql
<input type="checkbox"/>	base/postgres
<input type="checkbox"/>	base/ssh
<input checked="" type="checkbox"/>	base/windows
<input type="checkbox"/>	cis/cis-ubuntu-level1
<input type="checkbox"/>	cis/cis-ubuntu-level2

Scan now Schedule

## Slide 39

## GL: Results of this Exercise

Your scan should show that the **Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled** is now compliant.



base/windows: Strong Encryption for Windows Remote Desktop Required	Critical Issues	■
base/windows: Configure System Event Log (Application)	Minor Issues	■
base/windows: Configure System Event Log (Security)	Minor Issues	■
base/windows: Configure System Event Log (Setup)	Minor Issues	■
base/windows: Configure System Event Log (System)	Minor Issues	■
base/windows: Windows Default Guest Account is Disabled	Compliant	■
base/windows: Windows Password Complexity is Enabled	Compliant	■
base/windows: Windows Account Lockout Counter Configured to Wait at Least 30 Minutes Before Reset	Compliant	■
base/windows: Windows Account Lockout Duration Configured to at Least 30 Minutes	Compliant	■
base/windows: Kerberos Authentication Service Audit Log	Compliant	■
base/windows: Kerberos Service Ticket Operations Audit Log	Compliant	■
base/windows: Audit Computer Account Management	Compliant	■
base/windows: Verify the Windows folder permissions are properly set	Compliant	■
base/windows: Safe DLL Search Mode is Enabled	Compliant	■
base/windows: Anonymous Access to Windows Shares and Named Pipes is Disallowed	Compliant	■
base/windows: Force Encrypted Windows Network Passwords	Compliant	■
base/windows: Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled	Compliant	■

# EXERCISE



## GL: Remediating the Issue

### Objective:

- ✓ Write a remediation recipe on that node.
- ✓ Test for compliance with InSpec from the command line interface (CLI)
- ✓ Converge the recipe.
- ✓ Rescan the node and ensure compliance.



## Slide 41

## Review Questions

1. When adding a node to the Compliance server's dashboard, should you use the node's FQDN or just its IP address?
2. What can `inspec exec` be used for?
3. How are compliance severities defined?
4. Using the image on the right, what section is the actual test?

```
rule 'windows-base-201' do
  impact 1.0
  title 'Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled'
  desc '
    , @link: http://support.microsoft.com/en-us/kb/823659
  '
  describe registry_key('HKLM\System\CurrentControlSet\Control\Lsa') do
    it { should exist }
    its('LmCompatibilityLevel') { should eq 4 }
  end
end
```

Slide 42

## Review Questions

5. If a compliance scan tells you that a node is unreachable, what might you use to troubleshoot the connection?
6. What language is used to define controls?

Slide 43

