**ITSM**

OS Admin

SELinux Narrative Exercises

© FDM Group Ltd 2011. All Rights Reserved.

Any unauthorised reproduction or distribution in part  
or in whole will constitute an infringement of copyright.

|  |
| --- |
| Page left intentionally blank |

## SELinux Exercises

### Observing SELinux in action.

Run the ‘getenforce’ command. Which mode is the system in? – Enforcing

Run the ‘sestatus command’. Has the system been switched from permissive to enforcing, or did the system boot into the enforcing mode? What tells you this? – The system booted into enforcing mode, the line in the output ‘mode from config file:’ indicates the system is configured to boot into enforcing mode.

Run ‘getsebool –a | grep http | wc –l’. How many http related Booleans are listed?

44 Your figure may slightly differ from this.

What would the following command do?

ps –eZ

It produces a list of every process with its SELinux security context, the operative field is the type field, so it produces a list of each process and its domain.

The following command produces a unique list of all the domains in currently associated with processes running on the system.

ps –eZ| awk –F: ‘{print $3}’ | sort | uniq

How many are there?

ps –eZ| awk –F: ‘{print $3}’ | sort | uniq| wc –l There are 46. Your own answer may differ slightly from this figure.

The following command produces a unique list of type fields currently in use in the SELinux security labels within the whole filesystem tree.

ls –RZ | awk –F: ‘$3~/\_t/ {print $3}’

How many are there?

ls –RZ | awk –F: ‘$3~/\_t/ {print $3}’| wc –l … 647 (your figure may differ from this slightly).

Are there more domains or more ‘types’?

There are more types.

What does this tell you about the make up of SELinux policies?

It means each policy is likely to allow a process to access more than one type label.

Use the command semodule to list and count all currently load SELinux policy modules.

semodule –l | wc –l …. 405 approx

Run the command ‘sesearch –allow’ to show all the allow rules in the current policy. How many are there?

sesearch –allow | wc –l … 102104 approx

The following command shows the allow rules for the httpd\_t domain.

sesearch –allow| grep ‘^ \*allow httpd\_t’

This next command shows which types the httpd\_t domain process is allowed to access.

sesearch –allow| awk ‘/^ \*allow httpd\_t / {print $3}’ | sort | uniq

How many are there?

sesearch –allow| awk ‘/^ \*allow httpd\_t / {print $3}’ | sort | uniq | wc –l … 372 approx

### Getting a web service running

Run the script /scenariolabs/resetweb.sh. This provides a simple website within /web. Actually, the site is very simple. Two pages. Just the index.html file and a script cgi-bin/myscript.sh. The httpd daemon is configured to use the /web directory.

Take a quick look in /web. Who owns the files? Which group?

ls –l /web

apache and apache

This ensures the webserver is able to access the files using unix standard permissions.

The following command starts the web service.

systemctl start httpd

Now, on the windows server, point IE at the ip address of your Linux system.

<http://10.0.10.xxx>

You will see a message indicating the apache server is alive but NOT showing the website. Look at the last few lines of /var/log/audit/audit.log. What is the last error message about?

tail /var/log/audit/audit.log

There is an AVC message about access to /web/index.html being denied.

Run the command

setenforce 0

Reload the web page. Any difference? Why?

Yes! It now works. The system has entered permissive mode, so SELinux access denials cease to take effect.

Now it is working, lets run a script.

<http://10.0.10.xxx/cgi-bin/myscript.sh>

This executes a bash shell script which produces html output using echo statements. The html is rendered by the browser. What is the timezone in the date output?

UTC

Run the command

setenforce 1

Now reload <http://10.0.10.xxx>. This confirms the site can no longer be accessed.

Run the commands

semanage fcontext –a –t http\_sys\_content\_t “/web(/.\*)?”

restorecon /web/\*

Reload <http://10.0.10.xxx>. Does it work? What is missing?

The web page loads but the image is missing.

Run the commands

semanage fcontext –a –t http\_sys\_content\_t “/web/images(/.\*)?”

restorecon /web/images/\*

Reload the page. What changes?

The image now appears.

Now load the page

<http://10.0.10.xxx/cgi-bin/myscript.sh>. Any luck?

No luck at all.

Run the commands

Semanage fcontext –a –t httpd\_sys\_script\_exec\_t “/web/cgi-bin(/.\*)?”

restorecon /web/cgi-bin/\*

Any improvement?

Yes the script now runs.