**Section-2 Security**

**Lesson-02: Add Restore Security Contexts**

First of all we have to confirm that we are entered as a root user. We can check from the file that selinux is enabled or not or we can check it via getenforce utility.

# getenforce (It will tell you about the mode of operation in which selinux is running)

Now if for some reason if selinux is in permissive or disabled mode we can enable it via setenforce utility.

# setenforce 1 (So 1 flag will set the mode operation of selinux to enforcing and for 0 it will set to permissive mode)

If you want to disable selinux it you have to make a change in /etc/selinux/config file and set selinux to disabled.

If selinux is disabled by default, after setting selinux to enforcing we have to restart the linux machine as security context will rewrite for every file in the system.

Now lets have look at security context.

# ls -Z

As you can see the security context against each file

So now lets install apache and elinks

# yum install httpd elinks -y

Now lets make sure that its working

# elinks http://localhost

Now we will goto /var folder and lets have a look at security context of the file that are there and as you can see security context of the www folder.

now we will create a file index.html and store some text in it.

# cd /

# vi index.html

This is the text file

# ls -Z (we can see the admin\_home context to index.html)

lets move that file to /var/www/html/ folder

# mv index.html /var/www/html/

Move to

# cd /var/www/html/

Now lets change the ownership of the file

# chown apache:apache index.html

Also change the permission of the file

# chmod 775 index.html

# ll

now lets have look at it via elinks

# elinks http://localhost/index.html

As you can see we dont have permission to this file and here it shows that apache is the owner of this file and also 775 permission is assigned to it but we still dont have access to it. The reason we cant access to this file is of the security context that the file is in, so what we need to do we need to restore the context. We can do that via restorecon utility.

# restorecon index.html

**Lesson-03: Configuring selinux port labeling to allow services**

Now we will change the port of httpd service

# vi /etc/httpd/conf.d/httpd.conf

Listen 81

Now we will restart the service of httpd, so changes can take effect. Next we will check from elink utility.

# elinks http://localhost

As you can see on port 80 its currently refusing. Now if we specify 81 port on to elinks utility

As you can see that we are able to access apache default page on customized port, so by default selinux has some configuration of httpd service so how can find that, we will simply use semanage utility.

# semanage port -l | grep httpd

And we can see that these ports are allowed for httpd services except 81 port, so what happens if i pick a port that is not listed here so lets pick port 8282 and lets make sure that it is not currently being by any service

# semanage port -l | grep 8282

Now we will goto httpd.conf file and change the port from 81 to 8282, Now what happens if i try to restart the service here well we get a service failure. Now if we get the status of the service it says permission denied. Now how to fix this we have to simply add this port to selinux under http context. So we will find the context name for http port and add that port to it.

# semanage port -l | grep http

# semanage port -a -t http\_port\_t -p tcp 8282

To verify its been added

# semanage port -l | grep http (port 8282 has been added)

and now if we restart the service of httpd it starts successfully and to verify that we will check it with elinks utility

# elinks http://localhost:8282

To know what port are in selinux

# semanage port -l | more

**Lesson-04: Configuring AIDE for intrusion detection**

For configuring AIDE we will lets jump to the terminal first so first of all we will be installing AIDE

# yum install aide -y

Now the configuration file lies in /etc/aide.conf. Now lets have a look at aide.conf file

# vi /etc/aide.conf

As you can see there is an lot of information here, we will use the default configuration for AIDE. But it is good to know that configuration location

Now first we will initialize the database

# /usr/sbin/aide --init (it will take some time)

As you can see that it creates a database in /var/lib/aide/aide.db.new.gz

# cd /var/lib/aide

Now we will rename the database

# cp aide.db.new.gz aide.db.gz

Now we will run the check program against that file

# /usr/sbin/aide --check (this will take some time)

Now we will make a change in some file and run the check command again

# /usr/sbin/aide –check

**Lesson-05: Configuring OSSec for intrusion detection**

Now lets jumb to the terminal

# wget -q -O - http://www.atomicorp.com/installers/atomic | sh

Now we will update the repository

# yum install ossec-hids ossec-hids-server

ossec-hids package is for client, in our case the server and client is the same. Now thats it is installed lets look into its config file.

# vi /var/ossec/etc/ossec.conf

As you can see that its been set to default email address and we will change the smtp server to localhost

Now if you look below there some bunch of rules here. Here is the syscheck execution time which is set to default we will change it to 10minutes i.e 600.

Next we will start the service

# service ossec-hids start

Now type mailq to look for any emails, at the moment there is no email we will wait for 10 minutes and look into the mail

# postcat -vq que-id