IA 313 Labs Part II

Lab 1- Installing CentOS in a Virtual Environment

Step 1. Go to https://wiki.centos.org/Download and click the mirrors link for the ISO images:

Step 2. Click on a mirror site of your choosing and then click on the CentOS-7-x86_64-Everything-1708.iso link to download the file. It takes some time for the file to download.

Step 3. Start Oracle VirtualBox and then click the New button.

Step 4. Enter CENTOS 7 - for class in the Name box.

Step 5. Change the memory size to 4196 MB and click the Create button.

Step 6. Change the file size to 10.00 GB.

Step 7. Change the storage on physical hard disk to Fixed Size and click the Create button.

Step 8. When you are returned to the main Oracle VirtualBox screen, click on the Start button.

Step 9. Click on the small folder icon next to the dropdown list and navigate to the location where you downloaded the CentOS ISO file. Select that file and then click the Open button.

Step 10. Click the Start button.

Step 11. Click in the installation window and then at the CentOS 7 screen, either press the Enter key to start the installation or wait for the timer to run down and the installation to begin automatically.

Note

You can press the Esc key to avoid the lengthy media check. In addition, to “get out of” the virtual machine, press your right Ctrl key (the Ctrl key on the right side of your keyboard).

Step 12. At the Welcome to CENTOS 7 screen, click the Continue button to accept the default installation language, English.

Step 13. Click the Installation Destination button.

Step 14. Under Local Standard Disks, click on the icon of the 10 GiB disk multiple times until it is mark as selected. It is marked as selected when a checkmark appears next to the disk icon.

Step 15. Click the Done button in the upper-left area of the window.

Step 16. Click the Network & Host Name button.

Step 17. Click the icon next to Ethernet (enp0s3) to change the value from OFF to ON.

Step 18. Click the Done button to return to the INSTALLATION SUMMARY screen.

Step 19. Click the SOFTWARE SELECTION button.

Step 20. Click GNOME Desktop and then click the Done button.

Step 21. Click the Begin Installation button.

Step 22. While the installation is running, click on the ROOT PASSWORD button and set a password for the root account that is easy for you to remember. You may need to click the Done button twice if your password isn't very strong.

Step 23. While the installation is running, click on the USER CREATION button.

Step 24. For both full name and user name, enter student. Enter a password of your choosing and then click the Done button. You may need to click the Done button twice if your password isn't very strong. Do not make this account an administrator.

Step 25. When the installation is complete, click the Reboot button.

Step 26. After the system boots, when the INITIAL SETUP screen appears, click the LICENSE INFORMATION button.

Step 27. Click the box next to I accept the license agreement and then click the Done button in the upper-left corner of the screen.

Step 28. Click the FINISH CONFIGURATION button.

Step 29. At the login screen, log in as the student user.

Step 30. After logging in, click the Next button at the Welcome screen.

Step 31. Click the Next button at the Typing screen.

Step 32. Turn off Location Services and then click the Next button.

Step 33. Click the Skip button at the Online Accounts screen.

Step 34. Click the Start using CentOS Linux button.

Step 35. If you are interested, you can view the help videos for using GNOME on the Getting Started screen. Close this window when finished.

Step 36. For the next lab, you need to suspend the CentOS operating system. By suspending, you can start again quickly from the Oracle VirtualBox manager. To suspend, click the close box (the X) in the upper-right corner.

Make sure Save the machine state is selected and then click the OK button. When you want to use CentOS again, just double-click the CENTOS 7 - for class (Saved) icon in the Oracle VM VirtualBox Manager window.

Lab 2 - Securing User Accounts

Scenario: Create a user account named sue with the following restrictions:

• The account should have a strong, randomly generated password (consider using https://passwordsgenerator.net or a similar site to create the password).

• The user should be a secondary member of the games group.

• The user's home directory should be explicitly set as /home/sue.

• The user should be forced to change her password every 60 days.

• The user should not be allowed to change her password for 2 days after it has been set.

• The password warning field should be set to 10.

• The password inactivity period should be set to 60.

• The account should be set to expire on January 1, 2025.

• This user (and all others) should have a minimum password length of 12 characters.

Steps:

Step 1. Enter the following:

useradd -d /home/sue -m -f 60 -e 2025-01-01 -G games -K PASS_MAX_DAYS=60 -K PASS_MIN_DAYS=2 -K PASS_WARN_AGE=10 sue

Step 2. Enter the following:

passwd sue #provide the password you created here

Step 3. Enter the following:

vim /etc/pam.d/common-password

Step 4. In the common-password file, change the minlen= value on the pam_cracklib.so line to 12, as in this example:

password requisite pam_cracklib.so retry=3 minlen=12 difok=3

Lab 3 - Enabling Access Control Lists

Step 1. Open a terminal window by clicking the Applications in the menu bar and then Terminal.

Step 2. Copy the /etc/hosts file to the student user's home directory using the following command:

cp /etc/hosts ~

Step 3. Set an access control list (ACL) for the games group (create the group first if it does not exist) that allows read and write permissions for that group on the hosts file:

setfacl -m group:games:rw- hosts

Or

setfacl -m group:games:6 hosts

Step 4. Display the ACLs for the hosts file:

getfacl hosts

Step 5. Change the ACL mask value to read-only forthe hosts file:

setfacl -m mask:r-- hosts

Or

setfacl -m mask:4 hosts

Step 6. Display the ACLs for the hosts file to verify the ACL mask:

getfacl hosts

Step 7. Create a directory called test_acl:

mkdir test_acl

Step 8. Create a default ACL for the test_acl directory so the adm user (add the user first) has read and write permissions for all new files and directories created in the test_acl directory:

setfacl -m default:user:adm:rw- test_acl

Or

setfacl -m default:user:adm:6 test_acl

Step 9. Use the touch command to create a new file named test_file in the test_acl directory:

touch test_acl/test_file

Step 10. Verify the default ACLs by viewing the ACLs for the test_file file:

getfacl test_acl/test_file

Lab 4 - Monitoring Security Issues with SElinux

Step 1. Open a terminal window by clicking the Applications in the menu bar and then Terminal.

Step 2. Use the su command to switch to the root account as follows:

su -

Step 3. Execute the correct command to determine what mode (enforcing or permissive) SELinux is currently in:

getenforce

Note

CentOS normally defaults to enforcing mode.

Step 4. Change the current mode to permissive:

setenforce 0

Step 5. Display any log entries related to SELinux:

journalctl | grep SELinux

Step 6. Change the current mode to enforcing:

setenforce 1

Note

SELinux prevents access to files, so it is somewhat similar to permissions and file attributes. However, it is normally used in conjunction with servers, such as FTP and web servers.

Lab 5 - Backing up a File system

Step 1. Open a terminal window.

Step 2. Use the su command to switch to the root user.

Step 3. Back up the contents of the /etc/X11 directory into a tar file named /tmp/X11.tar:

tar -cf /tmp/X11.tar /etc/X11

Step 4. List the contents of the /tmp/X11.tar file, including details about the files (such as using verbose mode):

tar -tvf /tmp/X11.tar

Step 5. Move to the /tmp directory:

cd /tmp

Step 6. Extract the contents of the X11.tar file into the current directory:

tar -xf X11.tar

Step 7. Back up the contents of the /etc/X11 directory into a compressed tar file named /tmp/X11.tar.gz, using the gzip compression option:

tar -czf /tmp/X11.tar /etc/X11.gz

Step 8. Execute the correct command so that you can see and compare the sizes of the two tar files:

ls -l /tmp/X11.tar*

Lab 6 - Configuring a Proxy Server

Scenario: Configure your local system to act as a proxy server. By default, Squid is configured as a forward proxy server on port 3128. After installing Squid, start the service and use Firefox to test the proxy server.

As the root user, follow these steps:

Step 1. Enter the following:

yum -y install squid

Step 2. Enter the following:

systemctl enable squid

Step 3. Enter the following:

systemctl start squid

Step 4. Start Firefox.

Step 5. Access the menu options for the browser by clicking the icon that looks like three horizontal bars.

Step 6. Click the Preferences button.

Step 7. Click Advanced on the left-hand menu and then select Network from the menu that appears.

Step 8. Click the Settings button next to Configure How Firefox Connects to the Internet.

Step 9. Click the Manual Proxy Configuration radio button and fill in the IP address 127.0.0.1 in the box next to HTTP Proxy. Enter 3128 for the port number. Click the OK button and restart Firefox.

Step 10. Go to onecoursesource.com and test your proxy server.

Lab 7 - Administering Kernel Security Parameters

Scenario: Implement the following kernel parameter changes so they are persistent across reboots:

• Ignore all ping requests.

• Ignore all broadcast requests.

• Enable TCP SYN protection.

• Disable IP source routing.

Steps:

Add the following lines to the /etc/sysctl.conf file:

net.ipv4.icmp_echo_ignore_all = 1

net.ipv4.icmp_echo_ignore_broadcasts = 1

net.ipv4.tcp_syncookies = 1

net.ipv4.conf.eth0.accept_source_route = 0

Lab 8 - Securing a System with TCP Wrappers

Scenario: Implement the following TCP Wrappers rules:

• Allow SSH connections from all hosts.

• Allow connections to the Very Security FTP server from hosts in your local network.

• Allow connections to the xinetd server for any clients that can be resolved via the hostname resolver tool.

• Block access to all other services that use TCP Wrappers from all systems.

Steps:

Step 1. Add the following lines to the /etc/hosts.allow file (replacing 192.168.0. with your local network, which can be determined by using the ifconfig command):

sshd: ALL

vsftpd: 192.168.0.

xindtd: KNOWN

Step 2. Add the following lines to the /etc/hosts.deny file:

ALL: ALL

Lab 9 - Managing Log Files

Scenario: Modify the CentOS system so the following log events take place:

• All cron messages of debug level only should be sent to the /var/log/cron.debug file.

• All messages from the local3 service should be sent to the root user's terminal.

Verify that these changes have taken place correctly.

Steps:

Step 1. Click Applications in the menu bar, then Utilities, then Terminal.

Step 2. Switch to the root account.

Step 3. Edit the /etc/rsyslog.conf file by adding the following entries:

cron.=debug /var/log/cron.debug

local3.* root

Step 4. After saving the changes and quitting the editor, execute the following command:

systemtcl restart rsyslog

Step 5. Execute the following commands to test the changes to the rsyslog.conf file:

logger -p cron.debug "test"

logger -p local3.warn "test"

Note: The second command should produce a message to the root terminal window.

Step 6. View the contents of /var/log/cron.debug and verify that the logger entry was made.

Lab 10 - Configuring Grub Security

Scenario: You need to configure the current system so it is more secure because it will be located in a public area. Configure the GRUB boot so the following features are enabled:

• The GRUB menu should not appear. Instead, the default image should be automatically booted.

• Create a superuser GRUB account named super with the encrypted password noaccess.

• Create a regular GRUB account named user with the encrypted password secured.

Steps:

Step 1. As the root user, edit the /etc/default/grub file and change the GRUB_TIMEOUT value to 0.

Step 2. Execute the grub2-mkpasswd-pbkdf2 command to create the encrypted password noaccess and then execute the grub2-mkpasswd-pbkdf2 command again to create the encrypted password secured.

Step 3. Modify the /etc/grub.d/01_users file and add the following (replacing the grub.pbdkf2* value with the encrypted passwords from step 2):

cat <<EOF

set superusers="super"

password_ pbkdf2 super

grub.pbkdf2.sha512.10000.19074739ED80F115963D984BDCB35AA671C24325755377C3E9B014D862DA6ACC77BC110EED41822800A87FD3700C037320E51E9326188D53247EC0722DDF15FC.C56EC0738911AD86CEA55546139FEBC366A393DF9785A8F44D3E51BF09DB980BAFEF85281CBBC56778D8B19DC94833EA8342F7D73E3A1AA30B205091F1015A85

password_ pbkdf2 user

grub.pbkdf2.sha512.10000.19074739ED80F115963D984BDCB35AA671C24325755377C3E9B014D862DA6ACC77BC110EED41822800A87FD3700C037320E51E9326188D53247EC0722DDF15FC.C56EC0738911AD86CEA55546139FEBC366A393DF9785A8F44D3E51BF09DB980BAFEF85281CBBC56778D8B19DC94833EA8342F7D73E3A1AA30B205091F1015A85

EOF

Step 4. Execute the grub2-mkconfig command.

Lab 11 - Creating a Firewall to Protect a System

Scenario: Using the iptables command, create a firewall for the local system that meets the following objectives:

• Allows incoming connections for the SSH and FTP ports from any system

• Allows incoming connections for the telnet port for any system in the 192.168.1.0/24 network

• Logs all other incoming connections

• Drops all other incoming connections by changing the default policy

Note:

Do not save the changes you make during this lab exercise.

Stepsr: As the root user, execute the following commands:

iptables -F INPUT

iptables -A INPUT -m tcp -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -m tcp -p tcp --dport 21 -j ACCEPT

iptables -A INPUT -m tcp -p tcp --dport 20 -j ACCEPT

iptables -A INPUT -m tcp -p tcp --dport 22 -s 192.168.1.0/24 -j ACCEPT

iptables -A INPUT -j LOG

iptables -P INPUT DROP

Lab 12 – installing Snort on CentOS

Follow these steps to install Snort on CentOS:

1. On the Snort home page, just scroll down a bit, and you'll see the guide on how to download and install Snort. Click on the Centos tab and follow the steps. The commands in Step 1 will download and install Snort all in one smooth operation

2. Step 2 and Step 3 involve signing up for your Oinkcode so that you can download the official Snort detection rules, and then installing PulledPork so that you can keep the rules updated automatically

Bear in mind though that the free-of-charge detection rules that the Snort folk provide are about a month behind the ones that paid subscribers get. For learning purposes, though, they're all that you need. Also, if you choose to not get the Oinkcode, you can just use the Community rules, which are a subset of the official Snort rules.

3. Step 4 is just to read the documentation:

And that's it. You now have a working copy of Snort. The only catch is that all you have so far is just the command-line interface, which might not be what you want.

Lab 13 - Create an Inbound Firewall Rule

In this lab, you will verify that the Windows Firewall is enabled on a server and then create an inbound firewall rule that blocks file and printer sharing.

This lab requires access to a system running Windows Server 2012 or Windows Server 2012 R2.

Part A: Verify that Windows Firewall is enabled

1. Open the Control Panel for your Windows Server.

2. Choose System And Security.

3. Under Windows Firewall, click Check Firewall Status.

4. Verify that the Windows Firewall state is set to On for Private networks. If it is not on, enable the firewall by using the "Turn Windows Firewall on or off" link on the left side of the window.

Part B: Create an inbound firewall rule that blocks file and printer sharing

1. On the left side of the Windows Firewall control panel, click "Allow an app or feature through Windows Firewall."

2. Scroll down the list of applications and find File And Printer Sharing.

3. Uncheck the box to the left of that entry to block connections related to File And Printer Sharing.

4. Click OK to apply the setting.

Note: You should perform this lab on a test system. Disabling file and printer sharing on a production system may have undesired consequences.

Lab 14 - Create a Group Policy Object

In this lab, you will create a Group Policy Object and edit its contents to enforce an organization's password policy.

This lab requires access to a system running Windows Server 2012 or Windows Server 2012 R2 that is configured as a domain controller.

1. Open the Group Policy Management Console. (If you do not find this console on your Windows 2012 Server, it is likely that it is not configured as a domain controller.)

2. Expand the folder corresponding to your Active Directory forest

3. Expand the Domains folder.

4. Expand the folder corresponding to your domain.

5. Right-click the Group Policy Objects folder and click New on the pop-up menu.

6. Name your new GPO Password Policy and click OK.

7. Right-click the new Password Policy GPO and choose Edit from the pop-up menu.

8. When Group Policy Editor opens, expand the Computer Configuration folder.

9. Expand the Policies folder.

10. Expand the Windows Settings folder.

11. Expand the Security Settings folder.

12. Expand the Account Policies folder.

13. Click on Password Policy.

14. Double-click Maximum password age.

15. In the pop-up window, select the Define This Policy Setting check box and set the expiration value to 90 days.

16. Click OK to close the window.

17. Click OK to accept the suggested change to the minimum password age.

18. Double-click the Minimum Password Length option.

19. As in the prior step, click the box to define the policy setting and set the minimum password length to 12 characters.

20. Click OK to close the window.

21. Double-click the Password Must Meet Complexity Requirements option.

22. Click the box to define the policy setting and change the value to Enabled.

23. Click OK to close the window.

24. Click the X to exit Group Policy Editor

You have now successfully created a Group Policy Object that enforces the organization's password policy. You may apply this GPO to users and/or groups as needed.