# **LAB REPORT**

NAME: Yousef Jarrar

## **LAB QUESTIONS (40%)**

1. Why we are using Linux?

We use linux because a lot of users have devices that have been built of the Unix or Linux system. By understanding the fundamentals of the system, we can further expand our knowledge of System Information.

1. Why we are using CentOS Linux?

The reason why we use Cent OS Linux is because the system is derived from something called RedHat Enterprise. This system is a major player in many data centers, and server markets. Not only is Cent OS free but it is also compatible with RHEL.

1. Why we want do server virtualization?

Server virtualization technology provides an efficient and available server room and or data center infrastructure. It provides an enormous amount of convenience to system admin. It allows system admins a lot free time by not emulating the same tasks over and over. It can only provide a way to reduce costs in the long run.

1. Why we choose to install text mode instead of graphical mode?

The reason why we choose to install in text mode rather than the GUI is because it provides a more secure way to install the OS rather running it through the graphical interface.

1. What is LVM?

This stands for Logical Volume Management. This includes, allocating disk space, striping, mirroring, and resizing logical volumes to one or more physical volumes.

1. Why we need two network cards? (ens32 and ens33)

We use 2 network cards because it provides and internal NIC for the VM to use, and it also allows a Network to be linked to the internet.

1. Why we use sudo instead of root?

We use sudo because it stands for super user. This allows and grants ultimate access for someone altering the system. It bypasses many protocols that root sometimes does not have. Also, for security reasons.

1. Why you need import rpm gpg keys before update the system?

We import gpg keys to verify that the packages that are being installed in CentOs are verified, and there are no 3rd party packages that are trying to make it’s way into the system. It is also part of yum and the graphical update tools that will verify signatures of a package.

1. What IP address, subnet mask, and broadcast address did you get?

The I.P Address that I did get was the 172.162 number that was assigned to ens33 definition. The subnet was set as 255.255.255.0 and the DNS was left to 0.0.0.0

1. How to update the packages?

Within the lab, we were instructed to udpate the packages that have been imported for rpm-gpg keys. We used the following command: sudo yum -y update || By using this command we are able to update the packages that we previously imported into the VM and in turn allows us to play with the configuration of the machine.

1. Why do I need to reboot system after kernel update?

We rebooted the system to ensure that the updated packages are within the system. By rebooting the VM we can further ensure the installation and update process 100% .

1. What is IP forwarding?

IP Forwarding or IP routing is a process that is used to determine which path a packet will be sent. In this process information becomes distributed based on decisions and rules that have been sent. Sometimes it is over multiple networks.

1. Why we need to enable IP forwarding on hadrian?

We enable port forwarding on the VM because we want to ensure that packets are being sent to the right target. If we do not check then packets of data can be sent to different locations, and we may never know where they will end up.

1. What is masquerade?

This is also known as setting up a NAT. Which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.

1. Why add masquerade on the external zone?

We add masquerade on the external zone because we want to allow internal computers (VM) to be able to communicate to the outside (internet, or machines not within the network) This allows one machine to act on behalf of the other machines.

1. What is NAT (Network Address Translation)?

Which is also known as IP Masquerading. It acts the same way. This allows internal computers within the network with no known address to communicate to machines, or other EU’s on the outside.

## **LINUX COMMANDS (10%)**

List all the UNIX Commands that you used in this lab and explain each command:

1. rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-\*

This allows keys to update the VM to disallow potential attack or system malfunctioning.

2. #vi /etc/selinux/config Type SELINUX=disabled

This is allows the internal defense to be disabled. This allows the network to be compromised.

3. # sudo vi /etc/sysctl.conf

This configures the IP forwarding.

4. # sudo firewall-cmd - -zone=external - -add-interface=ens32 - -permanent

# sudo firewall-cmd - -zone=internal - -add-interface=ens33 - -permanent

This configures the firewall settings.

5. # sudo firewall-cmd - -zone-external - -add-masquerade - -permanent

This creates a NAT or masquerade on the network config.

6.]# sudo firewall-cmd - -permanent - -zone=internal - -add-service=dhcp

[sysadmin@hadrian ~]# sudo firewall-cmd - -permanent - -zone=internal - -add-service=tftp [sysadmin@hadrian ~]# sudo firewall-cmd - -permanent - -zone=internal - -add-service=dns [sysadmin@hadrian ~]# sudo firewall-cmd - -permanent - -zone=internal - -add-service=http [sysadmin@hadrian ~]# sudo firewall-cmd - -permanent - -zone=internal - -add-service=https [sysadmin@hadrian ~]# sudo firewall-cmd - -permanent - -zone=internal - -add-service=nfs

this configures the network tunnels to be enabled for the different ports that are associated with it.

## **TROUBLESHOOTING (50%)**

From this lab what troubles did you have?

Problem 1:

Solution:

Identify the problem: The biggest issue I ran into with this Lab was being able to enable ens32. In the beginning I did not know how to identify why I was not able to ping a simple URL. But after the hint that was given to us by the professor, and discussion with my classmates. I was able to figure out that the issue lied in the VM Network configuration. Originally ens32 had been disabled internally and the only way we were able to enable it was to find the config file that was buried deep within the system. After much trial and error I was able to deduce where the file was located and enable ens32 to be turned on.