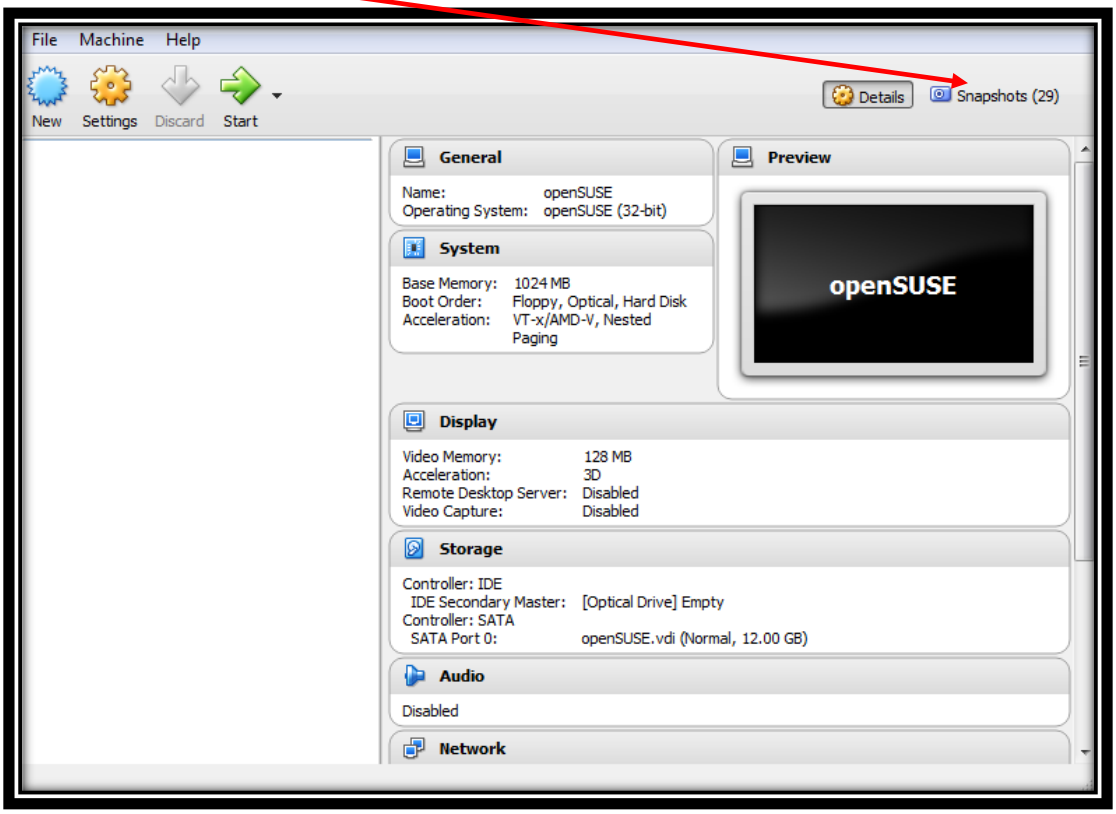
Practical Exercise 11-2: Implementing Network Security Measures on Linux

This Practical Exercise will take students through the creation of rules in chains within the default filter table via the iptables utility.

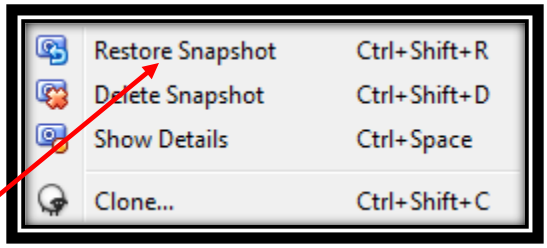
Open VirtualBox and start the openSUSE VM. Run snapshot 17-1 for the correctly configured environment. To run snapshot 17-1:

1. Open the Oracle VM VirtualBox manager by double clicking this icon on your desktop:

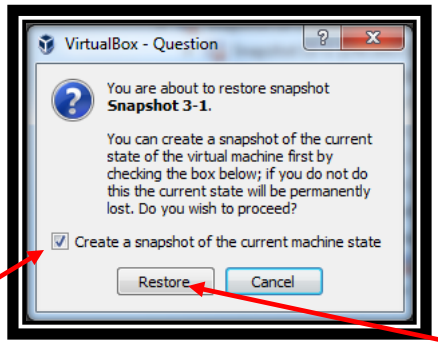
2. Click "Snapshots" in the top right of the Oracle VM Virtualbox Manager.



3. In the right side box populated with snapshots scroll up and find the one titled "Snapshot 17-1" and right click on it. The following box should appear:

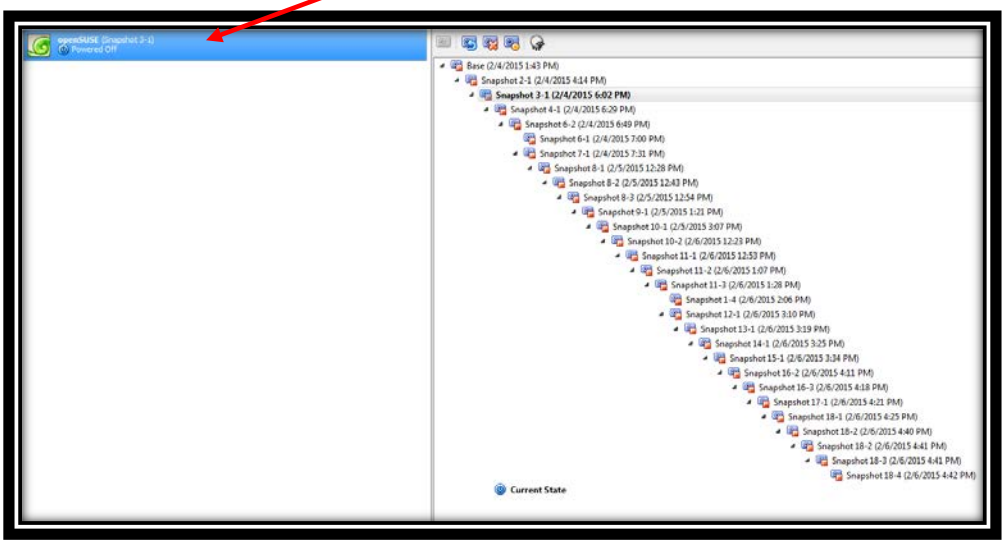


4. Select "Restore Snapshot" and the following pop-up should appear:



5. Uncheck the "Create a Snapshot of the current machine state" box and then click the "Restore" button. If the pop up box does not have the check box, just click "Restore."

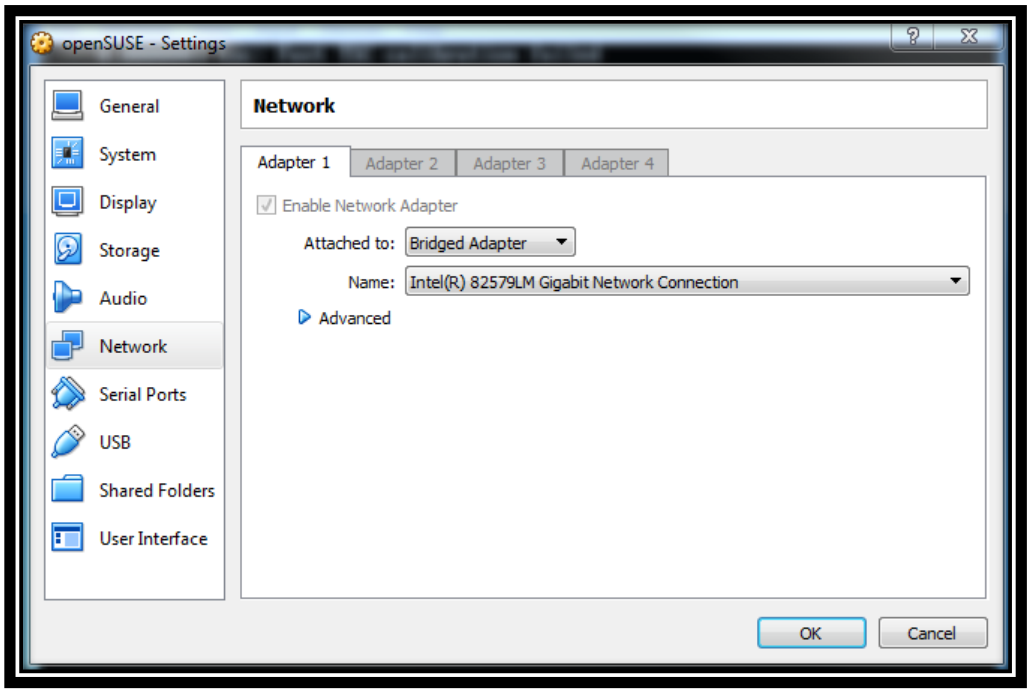
6. You should now see in the left box the openSUSE (Snapshot 17-1) with a status of "Powered Off." Power it on by double clicking it.



7. In this Practical Exercise we will also have to bridge the network adapter for virtual box to the hosts network interface card. To do this at the bottom right of the Virtual Box window find the icon with two computer screens:

8. Right click the icon and select the network settings.

9. Under the Adapter 1 tab ensure the "Enable Network Adapter" box is checked. Set the "Attached to" to Bridged Adapter. Once that is done the Name should auto populate.



10. Press **OK** and the Network Settings window will close.

11. A separate window should open and you should see the openSUSE Linux OS booting.

12. Press **CTRL+ALT+F1** and login with the username: **root** and password: **student**.

13. Enter **sytemctl restart network**.

14. Once the prompt returns we have to download and install nmap as it is not included by default in this distribution.

15. Enter **wget "http://download.opensuse.org/repositories/openSUSE:/13.2/standard/i586/nmap-6.47-2.1.10.i586.rpm"** to download nmap.

16. Enter **rpm -ihv nmap-6.47-2.1.10.i586.rpm** to install nmap.

17. Scan your system for open ports by completing the following steps:

a. At the shell prompt, enter **nmap –sT 127.0.0.1**. What TCP/IP ports are in use on your system?

b. At the shell prompt, enter **nmap –sU 127.0.0.1**. What UDP/IP ports are in use on your system?

18. Configure a simple firewall with iptables by doing the following:

a. Ping the DNS server (**ping xx.xx.xx.xx**) and verify that it responds.

b. If you cannot reach the DNS server try restarting the network by entering **systemctl restart network**.

b. Configure the kernel to use the iptables filter by entering **modprobe iptable_filter** at the shell prompt.

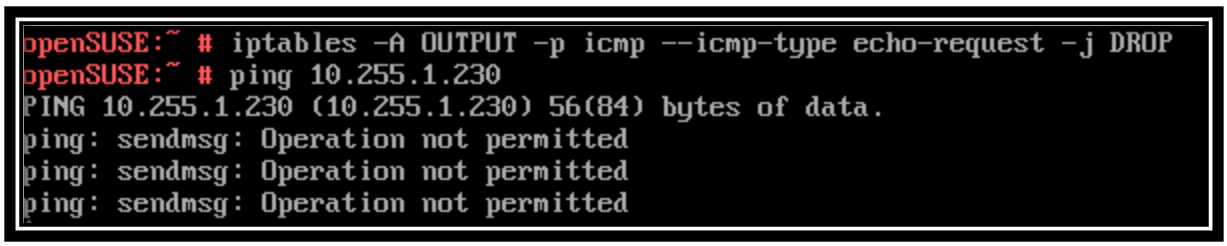
c. List the current rules for the filter table by entering **iptables –t filter –L** at the shell prompt.

d. At the shell prompt, enter **iptables –A OUTPUT -p icmp --icmp-type echo-request -j DROP**. This command creates a rule that will drop all outgoing icmp echo requests to any destination from any source (including this system).

e. View your new rule by entering **iptables –t filter –L** at the shell prompt. You should see the following rule added to your INPUT chain:

DROP icmp -- anywhere anywhere icmp echo-request

f. Ping the DNS servers IP address again (**ping xx.xx.xx.xx**). The packets should be dropped, as shown in this sample output:



g. Enter **iptables –D OUTPUT -p icmp --icmp-type echo-request –j DROP** to remove the rule from the OUTPUT chain.

h. Ping the DNS servers IP address again (**ping xx.xx.xx.xx**). Your requests should reach the DNS server and replies should be received.

i. Enter **dig www.google.com**. Enter the IP address of www.google.com here:_____.

j. Ping the IP address for www.google.com (ping 172.217.7.132). You should be able to ping the IP address and receive packets back.

k. Enter **iptables –A OUTPUT -p icmp --icmp-type echo-request -d 172.217.7.132 –j DROP**.

l. Ping the DNS server (**ping xx.xx.xx.xx**) and you should still receive packets back.

m. Ping www.google.com (**ping 172.217.7.132**) and you should receive a response stating that the operation is not permitted.

n. In step k you added a specific destination to drop icmp packets destined to from anywhere, in this case 172.217.7.132.

--End of Practical Exercise--