Linux TCP/IP Utilities

Contents

Time required: 60 minutes

How to Create Screenshots: Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

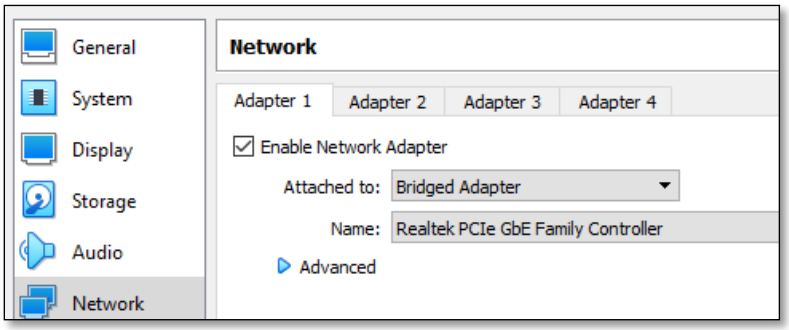
Lab Description

Windows is by far the most popular operating system in the world. However, in your career, you will likely encounter other operating systems such as Linux and MacOS. It is important for you to understand that these operating systems have similar diagnostic tools built into them. In this lab, you use commands available in Linux to explore these diagnostic tools.

VirtualBox Local Network Access

The labs in this class require our VirtualBox virtual machines to directly access our local network. The default network access is NAT (Network Address Translation). This is a bit like a firewall and does not allow direct access to your local network.

1. In the VirtualBox Manager → **Right Click** your Kali Linux virtual machine. Click **Settings**.
2. Click **Network** → Change **NAT** to **Bridged Adapter**. Pick the adapter that connects to your local network. Click **OK**.



Use GUI TCP/IP Utility

The GUI has intuitive access to IP configuration.

1. Log on to the Linux desktop.
2. In the upper right corner, there is a network Icon.
3. Right Click this icon.
4. Click **Connection Information**.
5. Insert a screenshot.

Click or tap here to enter text.

Use Terminal TCP/IP Utilities

The Linux Terminal is a command-line interface shell that can be used with the Linux Desktop. Follow these steps to use the Linux Terminal:

1. Launch and logon to Linux.
2. On the desktop, click the **Launcher** button in the top-left corner of the screen, type **terminal** in the search box and click **Terminal**. The Terminal window appears.

One of the most used network troubleshooting tools is **ping**. Ping confirms connectivity between your computer and a remote host.

3. At a terminal type: **ping www.google.com**
4. Press **CTRL-C** to stop the ping command.
5. Insert a screenshot.
6. Click or tap here to enter text.

Let's explore the traceroute command, which is like the tracert command in Windows. This command traces the route from your computer to the destination.

7. Enter this command:
   traceroute www.google.com
8. If Linux reports that traceroute has not been installed, install it using the method suggested on screen.
   sudo apt install traceroute
9. Try the command again.
10. Insert a screenshot.

Click or tap here to enter text.

11. Open a Windows command prompt and enter this command:
    tracert www.google.com
12. Were the results the same? If they were different, how were they different?

Click or tap here to enter text.

13. Insert a screenshot.

    Click or tap here to enter text.

14. Run the command **man traceroute.** This brings up the manual file with directions on how to use traceroute.
15. Run the command **traceroute --help**. How are these results different from the man page? Which is more useful?

Click or tap here to enter text.

16. The Linux **mtr** command combines traceroute and ping commands into a single network troubleshooting tool and is like the Windows pathping command. This command provides a real time traceroute in a much nicer format.

17. Run the command **mtr www.google.com**
18. If Linux reports that mtr has not been installed, install it using the method suggested on screen.
    sudo apt update
    sudo apt install mtr
19. Insert a screenshot.

Click or tap here to enter text.

20. To quit **mtr** → Click quit.
21. Did you get the same results from each method of tracing routes? How did they differ?

Click or tap here to enter text.

Linux IP Configuration Information

Linux has GUI network information utilities where all the IP addressing is shown at once. At the command line, it takes three different commands.

1. **DNS Configuration:** Run the command **cat /etc/resolv.conf**
2. Insert a screenshot.

   Click or tap here to enter text.

3. **Default Gateway:** Run the **ip r** command.
4. Insert a screenshot.

   Click or tap here to enter text.

5. **IP Address:** Run the command **ip a**
6. Write down the IP address of your Linux system.
7. Insert a screenshot.

Click or tap here to enter text.

Part 2: Use a Remote Terminal

The Linux Terminal is used for many functions to execute shell commands. Often, a network administrator will need to access the Linux system from a remote location to enter shell commands. In later labs in this course, you learn to use Secure Shell (SSH) to make a

remote connection to a Linux system. In this section, we access the Linux secure shell remotely by using PuTTY installed in Windows. PuTTY is open source software and can be used on any Windows computer to remote into the shell on any Linux system.

Follow these steps to install PuTTY in Windows and remote into your Linux Desktop secure shell:

1. In Terminal, enter **sudo apt update**
2. **Insert a screenshot.**

Click or tap here to enter text.

3. In Terminal, enter **sudo apt upgrade**

Click or tap here to enter text.

Your Linux system needs OpenSSH Server installed to allow remote control from another networked computer.

4. In your Terminal window, to make sure that the OpenSSH Server is installed, run these commands one at a time at the terminal:

```
sudo apt install openssh-server
sudo systemctl enable ssh.service
sudo systemctl start ssh.service
```

5. On your Windows computer, go to **www.putty.org** and download the PuTTY install package. If putty.org doesn't work, do a search for putty Windows. It will be somewhere.
6. Follow the onscreen directions to install PuTTY and then launch PuTTY.
7. By default, PuTTY uses SSH for the remote connection. What port is SSH using?

   Click or tap here to enter text.

8. In the HostName (or IP address) field, enter the IP address of your Linux system and click **Open**. If the PuTTY Security Alert dialog box appears, click **Yes** to continue.
9. When prompted, enter your Linux login and password. The Linux shell prompt appears. You now have remote access to your Linux shell.
10. Insert a screenshot of PuTTY connected to your Linux VM

Click or tap here to enter text.

Let's continue exploring some Linux commands used to diagnose and troubleshoot network connections. The tcpdump is a command line packet sniffer that command displays the contents of packets on a network interface.

1. Use PuTTY to run the following commands.
2. Enter the command: **sudo tcpdump**
3. Insert a screenshot.

Click or tap here to enter text.

4. Use the key combination **CTRL+C** to exit **tcpdump**
5. Insert a screenshot.

Click or tap here to enter text.

6. Return to the Linux terminal and enter the **sudo tcpdump** command.
7. Why do you think the amount of network traffic reported by tcpdump is more from the PuTTY remote connection than from the Linux Terminal?

Click or tap here to enter text.

Using your PuTTY remote terminal in Windows, you will perform a network scan with nmap. The nmap (network mapper) command tests for network vulnerabilities by port scanning, network mapping and other vulnerability tests.

1. Use PuTTY for the following commands
2. In your PuTTY window, enter the command:
   sudo nmap x.x.x.1/24
   (Where x.x.x is your local network.)
3. Look through the list. Try to identify the devices. Please list the devices you can identify.

   Click or tap here to enter text.

4. Insert a screenshot.

Click or tap here to enter text.

5. In Windows, the nslookup command is used to query DNS servers for information about IP addresses and domain names. Under Linux, you can use the dig command, which gives you more information.

6. At a Windows Command Prompt window, enter this command:
   nslookup www.google.com
7. Insert a screenshot.

Click or tap here to enter text.

8. In your PuTTY remote terminal window, enter this command:
   dig www.google.com
9. What is the IP address for www.google.com?

   Click or tap here to enter text.

10. What information did the dig command give you that nslookup did not?

Click or tap here to enter text.

Address Resolution Protocol (ARP) is the protocol that computers and routers use to find other devices on the network. The Linux arp command tells you what devices the OS has resolved.

11. In your PuTTY remote terminal, enter the **arp** command.
12. Explain the information you received?

Click or tap here to enter text.

13. Insert a screenshot.

Click or tap here to enter text.

14. The arp command only supports IPv4. IPv6 doesn't use ARP, but rather uses Neighbor Discovery Protocol (NDP). In IPv6, the ARP table is called the neighbor table.
15. Use the **ip neigh** command to view the table.
16. Enter this command: **ip -6 neigh show**
17. What IPv6 devices are in the neighbor table? How many devices did you get? (You may not have any.)

Click or tap here to enter text.

18. Insert a screenshot.

Click or tap here to enter text.

Assignment Submission

Attach this completed document to the assignment in Blackboard.