# Networking

**Computer Lab Exercises**

**Introduction**

Students should now have a conceptual understanding of network traffic and packet structure, but seeing is believing. Students will use networking tools on a linux machine, Ubuntu 14.04. After completing the labs, they should be able to analyze and deconstruct basic network traffic and packet captures.

**Setup**

Each virtualized computer should already be pre-configured with the required programs and files. Press ‘Ctl+Alt+t’ to open a terminal. Enter the command ‘cd ~/Desktop/Networking; ./check.sh’. Looking at the command output, lines with a program should have a path. An example would be ‘ifconfig: /sbin/ifconfig /usr/share/man/man8/ifconfig.8.gz’. Below the ‘Directory hash’ line, the output should read ‘XX’.

If a program’s directory is blank, or the ‘Directory hash’ doesn’t match, jump to the end of this document to the ‘Machine Reconfigure’ section to fix any errors.

Make sure to close programs from past session before moving onto to the next one to avoid confusion.

**Programs**

* Firefox
  + With ‘Cookies Manager+’ add-on <https://goo.gl/5KpYTo>
* ifconfig
* iptables
* route
* ssh
* wget
* wireshark
* zenmap

**Student Learner Outcomes**

* Understand how network traffic is routed using a GUI topographical representation
* How cookies are persistent when browsing websites
* How firewalls block traffic
* How Network Address Translation changes IP addresses
  + public vs private IP address
* Understand the security difference between telnet and ssh traffic
* How the Domain Name System resolves websites names to and IP address
* See http headers and tcp handshake network traffic
* Understand the security difference between http vs https
  + Extract files from tcp stream/session

**Section 1: Cookies and Firewalls**

1. Click on the ‘Ubuntu’ logo in the top of the launcher on the left of side the desktop
2. In the search bar, type ‘Firefox’ and click the icon to launch it
3. Open the ‘Extras’ menu in the top right of Firefox
4. Click on the ‘Cookies Manager+’ icon
5. In the ‘Cookies Manager+’ window, click the ‘clear all cookies’ button
   1. Image (with extras menu open too)
6. With the ‘Cookies Manager+’ window open, use Firefox to visit the following websites
   1. http://www.facebook.com
   2. http://www.google.com
   3. http://www.imgur.com
   4. http://www.reddit.com
7. **Observe**
   1. You’re able to access the websites
   2. As you visit each website, cookies are added and are persistent
8. Click on the ‘Ubuntu’ logo in the top of the launcher on the left of the desktop
9. In the search bar, type ‘Terminal’’ and click the icon to launch it
10. In the terminal prompt, enter the following commands
    1. sudo iptables -A OUTPUT -p tcp --destination-port 80 -j DROP
    2. sudo iptables -A OUTPUT -p tcp --destination-port 443 -j DROP
       1. Note: enter the user password when prompted for the sudo password
       2. Note: you won’t be able to see the password as it’s entered for security reasons
       3. Image with terminal and commands
11. In Firefox, open a new tab and close all other tabs
12. Using Firefox, visit the following websites
    1. http://www.facebook.com
    2. http://www.google.com
    3. http://www.imgur.com
    4. http://www.reddit.com
13. **Observe**
    1. You’re able to access certain websites
       1. Note: With the created firewall rules, you aren’t able to access websites using HTTP (port 80)
       2. Note: You’re able to access websites using HTTPS (port 443)
14. In the terminal prompt, enter the following commands
    1. sudo iptables -D OUTPUT -p tcp --destination-port 80 -j DROP
    2. sudo iptables -D OUTPUT -p tcp --destination-port 443 -j DROP
    3. Note: enter the user password when prompted for the sudo password
    4. Note: you won’t be able to see the password as it’s entered for security reasons
15. In Firefox, open a new tab and close all other tabs
16. Using Firefox, visit the following websites
    1. facebook.com
    2. google.com
    3. imgur.com
    4. reddit.com
17. **Observe**
    1. You’re able to access the websites
       1. Note: With the firewall rules deleted, you able to access websites again
18. Close all open programs
19. **Conclusion**
    1. Firewalls can prevent certain web traffic while allowing others based on predefined rules
    2. Cookies store user information and keep it after you leave a website

**Section 2: Routing, network address translation, and public vs private IP address**

1. Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.
2. In the search bar, type ‘Terminal’ and click the icon to launch it.
3. In the terminal application, enter the following command
   1. echo “private-ip”;sudo ifconfig ens160 | grep -w inet; echo; echo “public-ip”; wget -qO- http://ipecho.net/plain; echo
      1. Note: enter the user password when prompted for the sudo password
      2. Note: you won’t be able to see the password as it’s entered for security reasons
   2. image
4. **Observe**
   1. You’re shown your ‘private’ IP address in the first line
   2. You’re shown your ‘public’ IP address on the second line
   3. You public IP address is not the same as your internal IP address, this is done by Network Address Translation (NAT)
   4. Remember or write down both for reference later
5. In the terminal application, enter the following command
   1. sudo route -n | head -n 3
      1. Note: enter the user password when prompted for the sudo password
      2. Note: you won’t be able to see the password as it’s entered for security reasons
6. **Observe**
   1. The first line shows your next ‘hop’ to send traffic to
   2. Remember or write down for reference later
7. Close all open programs
8. **Conclusion**
   1. You can see the difference between your public and private ip address
   2. You’re able to get basic networking information using ‘ifconfig’ and ‘route -n’ with the command line

**Section 3: Zenmap**

1. Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.
2. In the search bar, type ‘Terminal’ and click the icon to launch it.
3. In the terminal application, enter the following command
   1. sudo zenmap
      1. Note: enter the user password when prompted for the sudo password
      2. Note: you won’t be able to see the password as it’s entered for security reasons
4. In the ‘Command Field’, enter the following
   1. nmap -T4 -F -n --traceroute scanme.nmap.org www.google.com www.facebook.com www.imgur.com
5. In zenmap, click on the ‘Topology’ tab to see a graphical representation of every device between yours and the others
6. **Observe**
   1. The default gateway i.e. first hop, is closest to you, and should match what you save from earlier
   2. There are areas where packets are routed from a central device
   3. Some are closer or farther away from you
   4. image
7. In zenmap, click on the ‘Ports/Services’ tab
8. Use the hosts list on the left to see what ports are open
9. **Observe**
   1. Some sites have a lot of ports open, some don’t
   2. It’s always safer to have less open than more
   3. Image
10. Close all open programs
11. **Conclusion**
    1. You’re able to get basic networking information using ‘ifconfig’ and ‘route -n’ with the command line
    2. You can use GUI application, like zenmap, to better visualize a network’s topology

**Section 4: Wireshark**

Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.

In the search bar, type ‘Terminal’ and click the icon to launch it.

In the terminal application, enter the following command

sudo wireshark &

Note: enter the user password when prompted for the sudo password

Note: you won’t be able to see the password as it’s entered for security reasons

Image

In the top left of wireshark, select ‘Open’

In the file explorer menu, navigte to the Desktop, open the ‘Networking Folder’, and select the ‘telnet-raw.pcap’ file, and click ‘Open’

In main packet list frame of wireshark, right click on any packet to open the options sub-menu

In the sub menu, hover over the ‘Follow’ option, and select ‘TCP Stream’

Observe

The window show the raw packet network data

At the beginning, in the top, you can clearly see the username and password being entered

This is bad

In the top left of wireshark, select ‘Open’

In the file explorer menu, navigte to the Desktop, open the ‘Networking Folder’, and select the ‘SSHv2.cap’ file, and click ‘Open’

In main packet list frame of wireshark, right click on any packet to open the options sub-menu

In the sub menu, hover over the ‘Follow’ option, and select ‘TCP Stream’

Observe

The window show the raw packet network data

At the beginning, in the top, you can see some data, but the rest is gibberish

This is good

In the top left of wireshark, click on the blue shark fin to start capturing network traffic

In the ‘Display Filter’ field, enter the following

tcp.port == 22

Click the ‘Ubuntu’ logo on the top of the launcher on the left side of the desktop.

In the search bar, type ‘Terminal’ and click the icon to launch it.

In the terminal application, enter the following command

ssh ghost@theshell.xyz

image

In main packet list frame of wireshark, right click on any packet to open the options sub-menu

In the sub menu, hover over the ‘Follow’ option, and select ‘TCP Stream’

Observe

The window show the raw packet network data

The previous command connected to a remote server

At the beginning, in the top, you can see some data, but the rest is gibberish

This is good

--

Explain dns

Look at example

See shit

Go to website

Filter

Observe

--

Example http capture

See header info

Tcp handshake example also

Go to own site

Look at headers

Look for tcp handshake

--

Example http capture with objects in the clear

Extract objects

Go to non tls/https site

Extract objects

Example http traffic

See encrypted data

Go to https stie

See encrypted data

**Procedures**

**Starting Wireshark Capture**

Start Wireshark

Click on the ‘Ubuntu’ icon at the top of the launch bar on the left

In the search bar, type ‘Terminal’ and click to launch it

In the terminal, type ‘sudo wireshark’

Type in the sudo password when prompted

When wireshark opens, click the ‘Ok’ button to dismiss the warning

Start packet capture

In the top menu bar, select ‘Capture’

In the ‘Capture Interfaces’ window, select interface ‘any’

In the bottom of the window near the ‘Capture filter for selected interfaces’ box, click on ‘Managed saved bookmarks’ icon, and select the ‘Ignore VN Traffic’ filter

Click start to start capturing packets

**Iptables**

Sudo iptables -A OUTPUT -p tcp --destination-port 80 -j DROP

Fix shit section

Git clone repo

Cd repo

./fix-me-bitch

If it doesn’t work, gg fam

Tools

Zenmap

Wireshark

Iptables

Ifconfig

Route

wget

Ssh

Firefox

With cookie browser add-on