Homework 1 - Networking Utilities

- This is an individual assignment, and worth 20 points.
- The due date and time is Tuesday, September 6th, 2:30 (sec01) / 5:30 (sec 76).
- You need to provide your outcomes to the "Homework 1-Outcome.docx." Change the file name following the naming convention. The naming convention is as follows: homework, hypen, last name, first initial, and extension (e.g., Homework1-ImG.docx). If you do not follow the convention, I will deduct 1.
- Focus on the outcomes and zoom in on them.
- YOU ARE NOT ALLOWED TO DO THIS DURING THE CLASS.

- The objective of this assignment is to learn and test basic networking utilities such as ping, traceroute, ipconfig, netstat, and bash commands on Kali.
- **Kali** is a Debian-derived Linux VM. It is used for security training, digital forensics, and penetration testing. Currently, Offensive Security maintains it.
- The instructions are based on **VMware Workstation Player**. Feel free to use **VirtualBox** if you prefer.

Kali Linux Prep

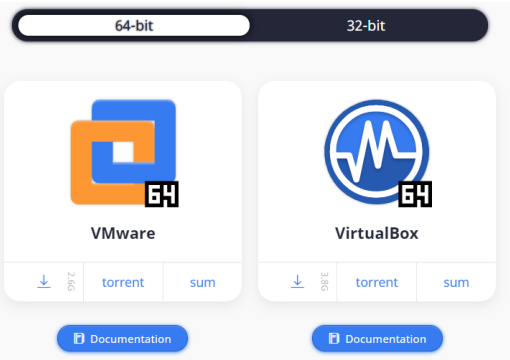
Install VMware

- Install VMware Workstation Player (Windows user) or VMware Fusion Player (MAC user). The VMware site can be accessed from the following link. Install the latest version.
  https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
  https://customerconnect.vmware.com/web/vmware/evalcenter?p=fusion-player-personal

Kali Linux VM Open

- Download a Kali Linux VMware Image. This image is a prebuilt Kali image for VMware.

  https://www.kali.org/get-kali/#kali-virtual-machines



- Select VMware.

- After downloading the Kali 7z file (kali-linux-2022.3-vmware-amd64.7z), you should unzip it with 7z. Mac users can use **Unarchiver** to unzip it (you can get it from the Mac App Store). Create a VM directory and move the extracted directory into it.
- Open Kali with VMware Player.
  - Go to VMware Player > **Open a Virtual Machine** (right side)> Go to the Kali directory (Kali-Linux-2022.3-vmware-amd64.vmwarevm) > Locate " Kali-Linux-2022.3-vmware-amd64.vmx" > Open > Click on **Play virtual machine** (bottom-right).
  - Logon to Kali
    - Username / password = kali / kali
  - **Log Out** button is on top-right.

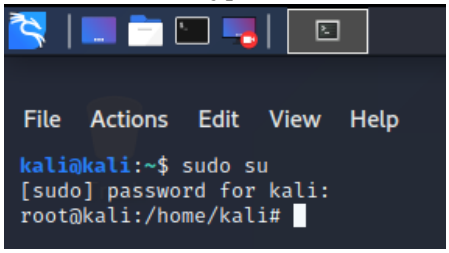
Learn Kali Linux

- What is Kali Linux?
  https://www.youtube.com/watch?v=psyDZ9ytlwc&ab_channel=Simplilearn
- How to use Kali Linux?
  https://www.youtube.com/watch?v=M3JhyWh1HgQ&t=962s&ab_channel=Simplilearn

Tasks

- Login to Kali with the ID and password: **kali/kali**. Launch a Terminal by clicking on the Terminal icon located on the top-left side.

- On the terminal, type **sudo su** to switch into the administrator mode. Type the password **kali**.



Task 1

- Let's identify the IP address of the virtual machine with the **ifconfig** command. The Windows equivalent is ipconfig. The commands you can use are:
  - ifconfig -h (for help)
  - ifconfig (to get the IP address of your system)

- Run a **ifconfig** command to display *the IP address, netmask, broadcast* associated with the VM.
- Take a screenshot of the output.

Task 2

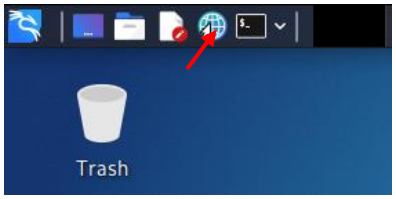
- Let's test the connection to a host with the **ping** command. Run a **ping** command to test the connection to the www.nyt.com server. Send the ECHO REQUEST message *five times only*. You need to use an option to get the requested result. For help, type **ping -h**.
- Take a screenshot of the output.

Task 3

- Let's try **traceroute** to trace the route to the destination by sending TCP packets.
- Run a traceroute command to trace the route to www.louisvilleky.gov *using TCP packets*.
- Take a screenshot of the output.

Task 4

- Let's try **netstat** to display the ports that are open in your system. **netstat** is a networking tool that is used for configuration and troubleshooting. You can monitor network connections of TCP, routing tables, and network interfaces. The state of each port can be *listening*, *waiting*, or *connected*. **netstat** by default does not tell which service is leading a port to be open. For help, type **netstat -h**.
- Launch the Firefox browser and visit a site.



- Run a **netstat** command to display *only TCP and UDP connections*.
- Take a screenshot of the output.

Task 5

- The Secure Shell (SSH) service enables secure access to a computer via a secure, encrypted protocol. This service is TCP-based and listens on port 22 by default.
- We can start or stop the SSH service on Kali by typing the following command: **service ssh start; service ssh stop.**
- Start the SSH service and verify that the SSH service is running on TCP port 22 by using the nestat command. Use the grep command to search the output for sshd.
- Take a screenshot of the output.

Task 6

- Let's use a bash command to find all of the subdomains contained on the index page of a website.
- We first need to download the index page of a website using the **wget** command. Try the following: wget www.louisvilleky.gov.
- To avoid confusion from the different outputs, clear the terminal by running **clear** before trying grep.
- Use the **grep** command on the **index.html** to find all the lines that has the string "href=", showing that these lines contain a link.
  - The first few lines of the output look like the following:

```
└─# grep "href=" index.html
<link rel="canonical" href="https://louisvilleky.gov/" />
<link rel="shortlink" href="https://louisvilleky.gov/" />
<link rel="image_src" href="/themes/custom/louisvilleky/images/footer-logo.png" />
```

- The output shows lots of lines that contain a link. But we notice that each line can be systematically split using the "/" as a delimiter. Clean up further the output of the previous **grep** command using the **cut** command. Use the **cut** command with the "/" as the delimiter and get the data in the **third** field.
- Study the following sites to learn how to specify a delimiter and get the data at the specific field.
  - https://linuxize.com/post/linux-cut-command/
  - https://ww.geeksforgeeks.org/cut-command-linux-examples/
- You must use pipe (|) to send the output of the grep command to the next command (i.e., cut).
  - https://www.youtube.com/watch?v=nCHjYP7kqYU&ab_channel=Hak5
  - http://faculty.winthrop.edu/dannellys/csci208lab/lab09.htm
- Take a screenshot of the first part of the output.