

# Practical 1

**Objectives:** Understand the skills and knowledge required for an Ethical Hacker  
 Set up Kali Linux  
 Set up Windows VM  
 Install Wireshark for Windows

## Exercise 1. Explore Security Certifications

1. Go to [www.eccouncil.org](http://www.eccouncil.org). Look for information on the Certified Ethical Hacker training.
2. Still in [www.eccouncil.org](http://www.eccouncil.org), go to “About EC-Council”. Click on Code of Ethics. Look through the Code of Ethics expected of Ethical Hackers.
3. Go to [www.isc2.org/Certifications/CISSP](http://www.isc2.org/Certifications/CISSP). Click on “2. Register and Prepare for the Exam” to see the 8 CISSP Domains covered in the CISSP certification.

## Exercise 2. Explore SANS website







1. Go to [www.sans.org](http://www.sans.org). Under Resources, click on The Critical Security Controls. Click on the CIS Critical Security Controls (<http://www.cisecurity.org/critical-controls>).

These are a recommended set of actions that companies can follow to protect their networks.

2. Browse through the CIS Controls.

The following are some screenshots extracted from the CIS Controls, for reference.

### CIS Control 2: Inventory and Control of Software Assets

| Sub-Control | Asset Type   | Security Function | Control Title                             | Control Descriptions  | Implementation Groups   |   |   |
|-------------|--------------|-------------------|---|---|---|---|---|
|             |              |                   |   |   | 1   | 2   | 3   |
| 2.1         | Applications | Identify          | Maintain Inventory of Authorized Software | Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.  |  |  |  |
| 2.2         | Applications | Identify          | Ensure Software Is Supported by Vendor    | Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system. |  |  |  |

**CIS Control 18: Application Software Security**

| Sub-Control | Asset Type | Security Function | Control Title  | Control Descriptions   | Implementation Groups |   |   |
|-------------|------------|-------------------|--|--|-----------------------|---|---|
|             |            |                   |  |  | 1                     | 2 | 3 |
| 18.1        | N/A        | N/A               | Establish Secure Coding Practices  | Establish secure coding practices appropriate to the programming language and development environment being used.  |                       | ● | ● |
| 18.2        | N/A        | N/A               | Ensure That Explicit Error Checking Is Performed for All In-House Developed Software | For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.           |                       | ● | ● |
| 18.3        | N/A        | N/A               | Verify That Acquired Software Is Still Supported                                     | Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations. |                       | ● | ● |

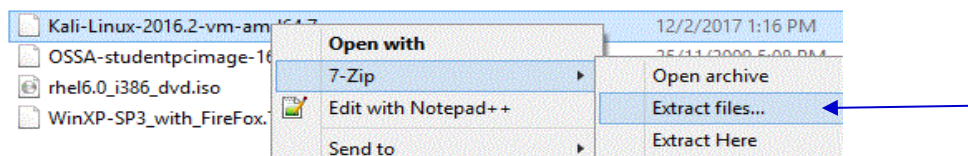
**Exercise 3. Career Opportunities**

1. Search for job postings of penetration testers. What are the skills needed? Are professional certifications required?

**Exercise 4. Setting up your Kali Linux**

In this exercise, you will set up a Kali Linux virtual machine.

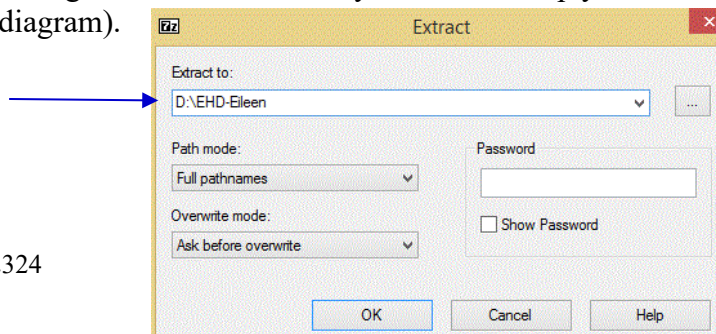
1. Login to the lab desktops.
2. Create a folder D:\EHD-yourname (eg D:\EHD-johntan). You can keep your EHD files in this folder.
3. Go to C:\BaseImages. Right-click on the `kali-linux-2022.1-vmware-amd64.7z` file and choose 7-Zip, Extract files.



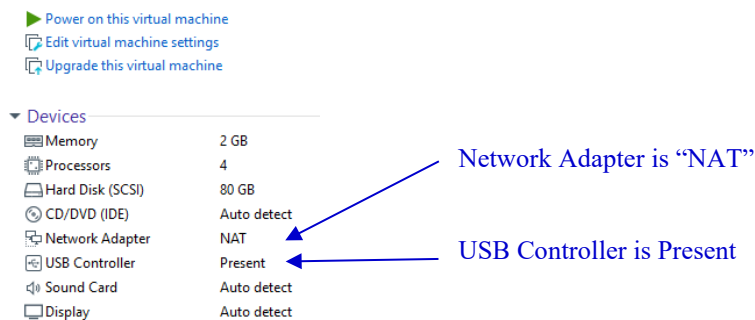
You can also download the 2.5GB Kali Linux VMware machine from the following URL. Or download the latest version from [www.kali.org](http://www.kali.org) using BitTorrent which would be faster.

[https://ichatspedu-my.sharepoint.com/:f/g/personal/eileen\\_yeo\\_ichat\\_sp\\_edu\\_sg1/EjbFVL-5qklEg7ztMeQYLwIBesbKhHZH-U9YikfgfmhRTQ](https://ichatspedu-my.sharepoint.com/:f/g/personal/eileen_yeo_ichat_sp_edu_sg1/EjbFVL-5qklEg7ztMeQYLwIBesbKhHZH-U9YikfgfmhRTQ)

4. Change the folder to where you want to keep your EHD virtual machines (see following diagram).



5. Click OK. The Kali virtual machine will be extracted.
6. When the extract is complete, go to your EHD folder. Open the Kali Linux VM using VMware Workstation.



7. Check that you have a USB Controller listed under Devices for your Win10 virtual machine (see image above).
8. If you do not have a USB Controller, do the following steps to add it :
  - a. Under Commands, click on Edit virtual machine settings.
  - b. Under Hardware, click the Add button at the bottom.
  - c. Select USB Controller and click Next. Click Finish. Click OK.

Adding a USB controller means you can access USB devices in your image.

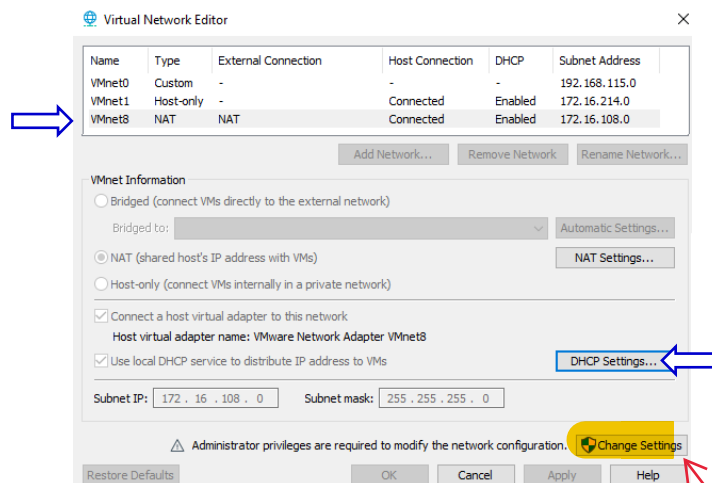
9. Check that the Network Adapter is set to “NAT” or Network Address Translation (see image above).
10. If the Network Adapter is not set to “NAT”, do the following steps to add it :
  - a. Under Commands, click on Edit virtual machine settings.
  - b. Under Hardware, select Network Adapter.
  - c. In the right-hand pane, select the radio button NAT. Click OK.

NAT networking means the virtual machine is in a private network on the Host PC. It will not be visible to other machines outside of the private network.

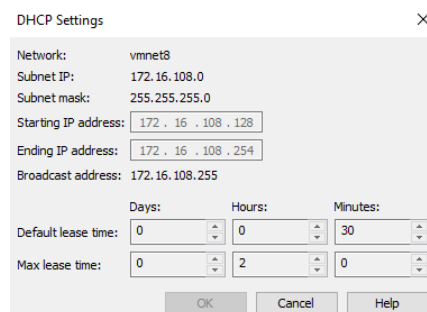
Currently the virtual machines are configured to use DHCP to obtain their IP addresses. As NAT networking is used, the virtual machines will request for IP addresses from the VMware DHCP service. By default, the VMware DHCP services gives out IP addresses with a max lease time of 2 hours, so there is a possibility that your virtual machines may be given a different IP address the next day.

If you prefer your virtual machines to be given the same IP address as much as possible, you can increase the lease time.

11. In the VMware, click on Edit menu, and choose Virtual Network Editor.
12. In the Virtual Network Editor, select the row for NAT. Click DHCP Settings. (see following diagram)



13. In DHCP Settings, you can change the Default and Max lease time to as long as possible.



Note! You may not be able to edit this. Click on Change Settings.

14. Power on the Kali virtual machine. Select "I copied it" when asked,
15. When the boot menu appears, choose the default first item "Kali GNU Linux" and press Enter.
16. Login with username "kali" and password "kali".
17. Right-click anywhere on the Kali desktop and choose Open Terminal.

You are now logged in as a normal user "kali", who has limited access. In order to do admin tasks like installing new software, you need to use the sudo command.

18. As user kali, try to run "fdisk -l" to list out partition tables. You will not be successful as this command requires root permission.
19. Use the sudo command to run the "fdisk -l" command. Enter kali's password when asked.  

```
sudo fdisk -l
```
20. This time, the partitions will be listed.

## Exercise 5. Using Kali Linux

### Description :

We will now explore more commands and settings on Kali.

#### In Kali

1. To change the size of the VM screen, click on the Kali icon in the top left corner and choose Settings -> Display.
2. Choose your desired Screen Resolution. Click Apply.
3. To find out the Kali Linux version or the Kali Linux kernel version, run the following commands :

```
cat /etc/os-release
uname -a
```

4. In a terminal, type “ip addr” to view your IP address.
5. Type “ip route” to see the IP address of the gateway.

In this example, the gateway IP is 172.16.108.2

```
kali@kali:~$ ip route
default via 172.16.108.2 dev eth0 proto dhcp metric 100
172.16.108.0/24 dev eth0 proto kernel scope link src 172.16.108.174 metric 100
```

6. To see the DNS Server :

```
cat /etc/resolv.conf
```

7. To see a list of all the packages installed on your Kali Linux :

```
dpkg --get-selections
```

You can use PageUp and PageDown keys to scroll through the list of installed packages. Press q to quit.

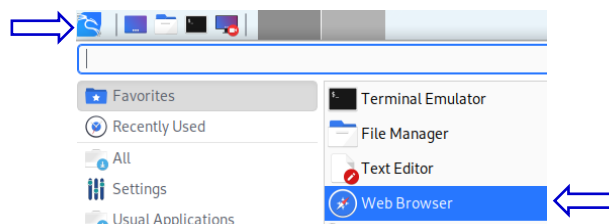
8. You can also use the apt command to view the list of all the packages installed on your Kali Linux :

```
apt list --installed
```

9. You can add the grep command for a quicker way to check if a certain package is already installed. For example, to see if the wireshark package is installed :

```
dpkg --get-selections | grep wireshark
```

10. The web browser in Kali is Firefox and you can start it by clicking the Kali icon in the top left corner and selecting Favorites, Web Browser.



## Exercise 6. Configuring network settings in Kali Linux

In Kali Linux, Network Manager can be used to manage the network connections. The network interface device eth0, is connected to the Connection “Wired Connection 1”. By default it is using DHCP.

### Configuring IP settings through the Network Manager GUI:

1. Click on the Kali icon in the top left corner and choose Settings -> Advanced Network Configuration. (or you can run the command nm-connection-editor)
2. Under Ethernet, double-click on Wired connection 1.
3. Click on the IPv4 settings tab.
4. You can select Automatic (DHCP) or Manual. If you pick Manual, you are setting a static IP address, and need to specify the Address, Netmask and Gateway.
5. If you are setting a static IP, under DNS, you can specify the DNS Server.

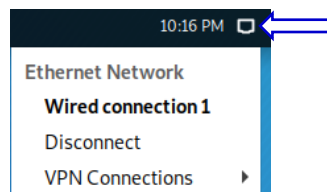
Method: Manual

| Address      | Netmask | Gateway     |
|--------------|---------|-------------|
| 192.168.6.11 | 24      | 192.168.6.1 |

DNS servers: 192.168.6.2

An example of setting a static IP address

6. To make any changes take effect, click on the Network icon in the top right corner and choose Disconnect.



7. Click on the Network icon and choose Wired connection 1 to activate it again.
8. You can also use the nmcli command (Network Manager Command Line Interface) to deactivate and activate the “Wired connection 1” for the changes to take effect.

```
nmcli connection down "Wired connection 1"
nmcli connection up "Wired connection 1"
```

### Configuring IP Settings through the Network Manager configuration file

9. You can also make changes to the IP settings by modifying the config files. To configure “Wired connection 1”, edit the file “/etc/NetworkManager/system-connections/Wired connection 1” (remember sudo may be required) and change the section for ipv4 to the following static IP address

```
[ipv4]
method=manual
address1=172.16.108.191/24,172.16.108.2
```

Change this to the IP address and subnet mask you want to set.

Correct Command!!!

sudo nano /etc/NetworkManager/system-connections/"<connection name>"

← Change this to the gateway.

Note: Wired connection might be named different, cd to system-connections, and then ls

```
(kali@kali)~[/etc/NetworkManager/system-connections]
$ ls
'Wired connection 1.nmconnection'
```

10. Run the following command to get Network Manager to reload the changes you made to the config file.

```
sudo nmcli connection reload "Wired connection 1"
```

11. Down and up the “Wired connection 1”.

```
sudo nmcli connection down "Wired connection 1"
sudo nmcli connection up "Wired connection 1"
```

12. Use “ip addr” to view the new IP address.

13. To reset back “Wired connection 1” to use DHCP, edit the file “/etc/NetworkManager/system-connections/Wired connection 1” and change the section for ipv4 back to “auto” and remove the address and dns lines.

```
[ipv4]
method=auto
```

14. Reload, down and up “Wired connection 1”.

### Configuring IP Settings through command line “ip addr”

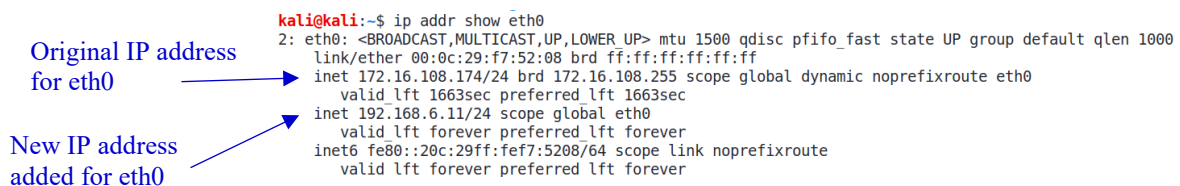
15. You can also make changes to the IP settings at the command line. Changes made using “ip addr” at the command line will be lost upon the next restart.

To add a new IP address for eth0 at the command line:

```
sudo ip addr add 192.168.6.11/24 dev eth0
```

↑  
Change this to the IP address and subnet mask you want to set.

16. Run “ip addr show eth0” to view the newly added IP address to the network interface eth0.



```
kali@kali:~$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:f7:52:08 brd ff:ff:ff:ff:ff:ff
    inet 172.16.108.174/24 brd 172.16.108.255 scope global dynamic noprefixroute eth0
        valid lft 1663sec preferred lft 1663sec
    inet 192.168.6.11/24 scope global eth0
        valid lft forever preferred lft forever
    inet6 fe80::20c:29ff:fef7:5208/64 scope link noprefixroute
        valid lft forever preferred lft forever
```

17. To delete the newly added IP address (change to the IP address and subnet mask that you added earlier):

```
sudo ip addr del 192.168.6.11/24 dev eth0
```

18. To reset back any changes, you can use the nmcli command to deactivate and activate the “Wired connection 1”.

```
nmcli connection down "Wired connection 1"
nmcli connection up "Wired connection 1"
```



## Exercise 7. Setting up a Windows virtual machine

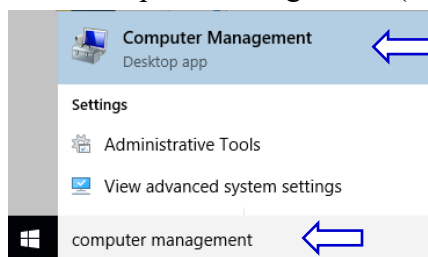
Set up a Windows virtual machine that can be used as a target client in future exercises.

1. Go to C:\BaseImages and copy the Win10 folder to your D:\EHD folder.  
You can also download the Win10 virtual machine `Win10.7z` from the same download links.
2. Use VMware Workstation to open the Win10 virtual machine.
3. Check that the Network Adapter is set to “NAT”. Power on the Win10 virtual machine.
4. Login as user “admin” and password `1qwer$#@!`
5. When the image has started up, you may want to install/update VMware Tools if it is not installed yet. Go to VM menu and choose Install VMware Tools or Update VMware Tools.

## Exercise 8. Configure your Windows operating system

### Screen Resolution and User Accounts

1. To change the size of the VM screen, right-click on the background and choose “Display settings”. Click “Advanced display settings”.
2. Choose your desired Screen Resolution. Click Apply.
3. In the Cortana search textbox, search for “computer management”.
4. Click on Computer Management. (see following diagram)



5. In Computer Management, expand Local Users and Groups.
6. Right-click on Users and choose New User.
7. Create a new user with username “student” and password “1qwer\$#@!” (or you can set another password value).
8. Uncheck “User must change password at next logon”.
9. Check “Password never expires”. (Because this is for testing, we set the password to never expire. )

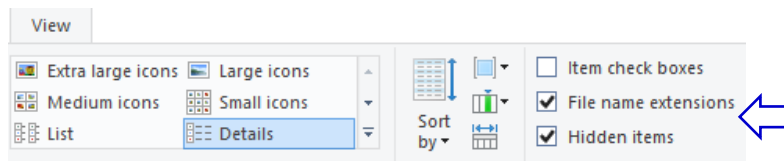
10. Click Create. Click Close.
11. Close the Computer Management window.



Do not hide extensions for known file types

12. In Windows Explorer, click on View menu.

13. Check the boxes for “File name extensions” and “Hidden items”.

IP address and Computer Name

14. In the Cortana search textbox, type “cmd” and select the cmd command (Command Prompt).



15. In the Command Prompt, type “ipconfig”. Take note of your IP address (under Local Area Connection).

(Optional) If you wish to, you can set a static IP for your Win10 VM.

16. If you want to change your computer name, do the following steps:

- d. In Windows Explorer, right-click on “This PC” and choose Properties.
- e. Under Computer name, domain and workgroup settings, click “Change Settings”.
- f. Click on the Change button.
- g. Enter the new computer name. Click OK.
- h. You will be asked to restart your computer. Restart your VM for the new computer name to take effect.

**Exercise 9. Install Wireshark for Windows**In Win10 VM

1. Browse to [www.wireshark.org](http://www.wireshark.org) or Brightspace or the Dropbox link (under Topic 1) and download and install Wireshark (64-bit version) with default options.

**Exercise 10. Test your Understanding**

1. Do the Ethical Hacker Quiz on Brightspace for General Performance marks.

*End of Practical*