**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 Explore Security Certifications**

1. Go to www.eccouncil.org. Look for information on the Certified Ethical Hacker training.
2. Still in 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.

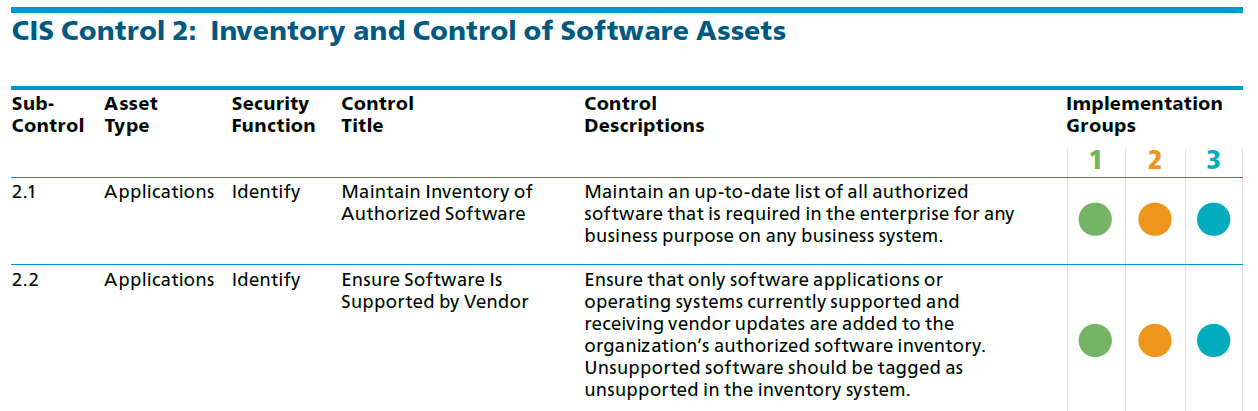
**Exercise Explore SANS website**

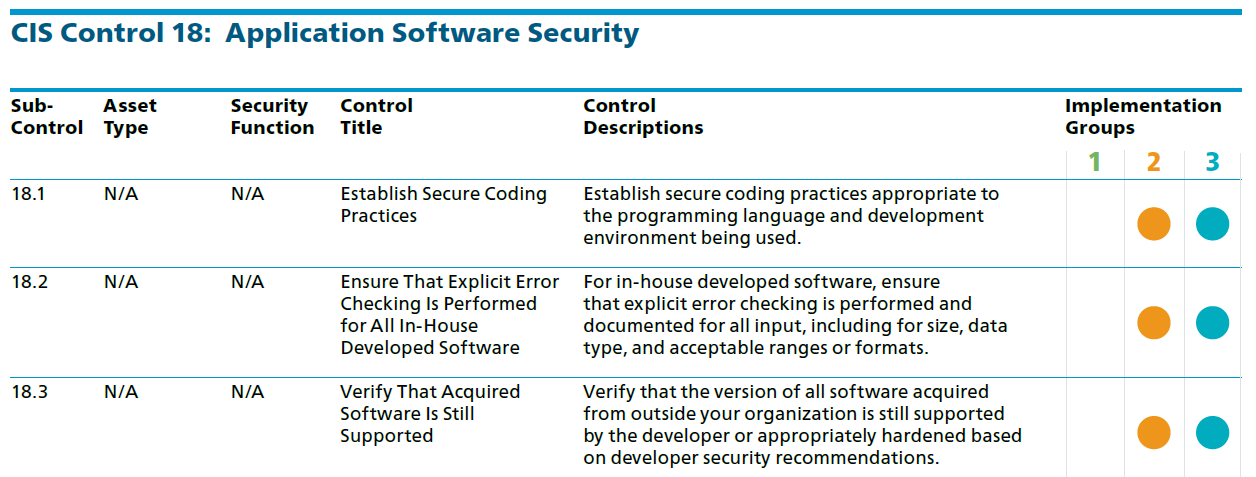
1. Go to www.sans.org. Under Resources, click on The Critical Security Controls. Click on the CIS Critical Security Controls (<http://www.cisecurity.org/critical-controls>).

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

1. Browse through the CIS Controls.

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





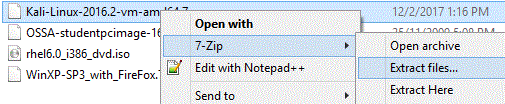
**Exercise Career Opportunities**

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

**Exercise Setting up your Kali Linux**

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

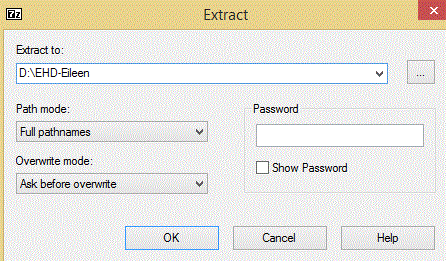
1. Login to the lab desktops.
2. Create a folder D:\EHD-yourname (eg D:\EHD-johntan). You can keep your EHD files in this folder.
3. Go to C:\BaseImages. Right-click on the kali-linux-2022.1-vmware-amd64.7z file and choose 7-Zip, Extract files.



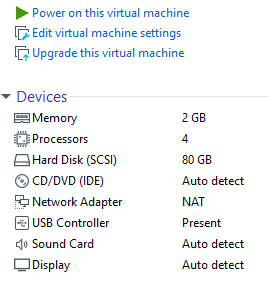
You can also download the 2.5GB Kali Linux VMware machine from the following URL. Or download the latest version from [www.kali.org](http://www.kali.org) using BitTorrent which would be faster.

<https://ichatspedu-my.sharepoint.com/:f:/g/personal/eileen_yeo_ichat_sp_edu_sg1/EjbFVL-5qklEg7ztMeQYLwIBesbKhHZH-U9YikfgfmhRTQ>

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



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



Network Adapter is “NAT”

USB Controller is Present

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

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

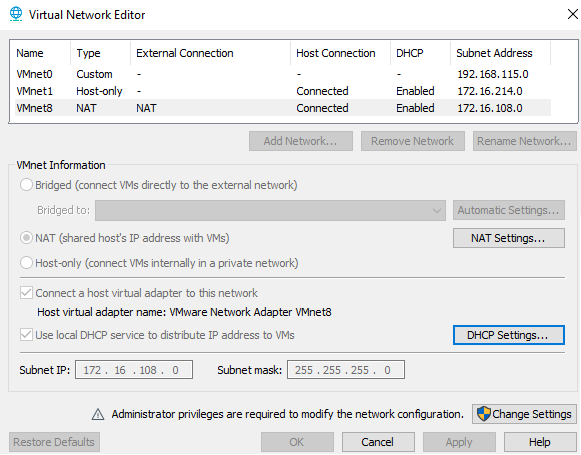
1. Check that the Network Adapter is set to “NAT” or Network Address Translation (see image above).
2. If the Network Adapter is not set to “NAT”, do the following steps to add it :
   1. Under Commands, click on Edit virtual machine settings.
   2. Under Hardware, select Network Adapter.
   3. In the 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.

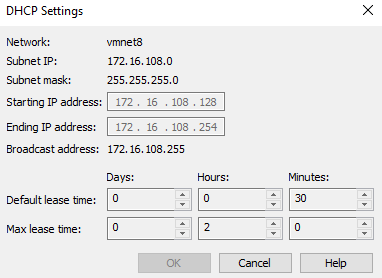
Currently the virtual machines are configured to use DHCP to obtain their IP addresses. As NAT networking is used, the virtual machines will request for IP addresses from the VMware DHCP service. By default, the VMware DHCP services gives out IP addresses with a max lease time of 2 hours, so there is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

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



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



You can increase the Default and Max lease time to as long as possible

1. Power on the Kali virtual machine. Select “I copied it” when asked,
2. When the boot menu appears, choose the default first item "Kali GNU Linux" and press Enter.
3. Login with username “kali” and password “kali”.
4. 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.

1. As user kali, try to run “fdisk -l” to list out partition tables. You will not be successful as this command requires root permission.
2. Use the sudo command to run the “fdisk -l” command. Enter kali’s password when asked.

sudo fdisk -l

1. This time, the partitions will be listed.

**Exercise Using Kali Linux**

**Description :**

We will now explore more commands and settings on Kali.

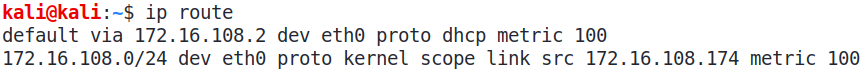
In Kali

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

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



In this example, the gateway IP is 172.16.108.2

1. To see the DNS Server :

cat /etc/resolv.conf

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

dpkg --list

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

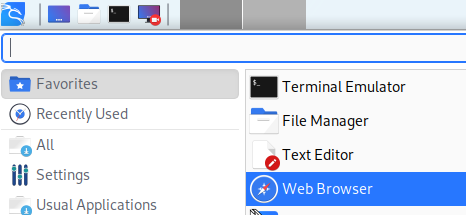
1. You can also use the apt command to view the list of all the packages installed on your Kali Linux :

apt list --installed

1. 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 --list | grep wireshark

1. 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.

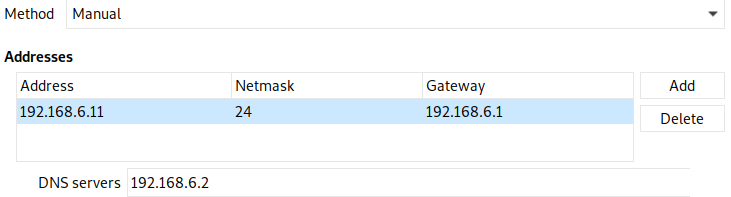


**Exercise Configuring network settings in Kali Linux**

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.

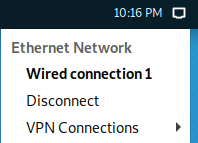
Configuring IP settings through the Network Manager GUI:

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.



An example of setting a static IP address

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



1. Click on the Network icon and choose Wired connection 1 to activate it again.
2. 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

1. 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

Change this to the gateway.

address1=172.16.108.191/24,172.16.108.2

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

1. 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"

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

sudo nmcli connection down "Wired connection 1"

sudo nmcli connection up "Wired connection 1"

1. Use “ip addr” to view the new IP address.
2. 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

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

Configuring IP Settings through command line “ip addr”

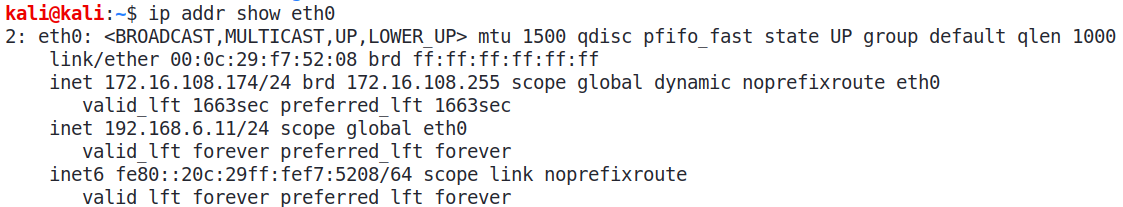
1. You can also make changes to the IP settings at the command line. Changes made using “ip addr” at the command line will be lost upon the next restart.

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.

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



Original IP address for eth0

New IP address added for eth0

1. 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

1. 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 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.

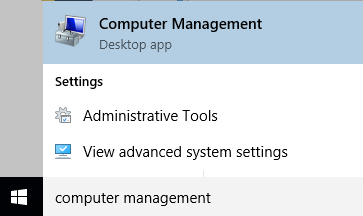
You can also download the Win10 virtual machine Win10.7z from the same download links.

1. Use VMware Workstation to open the Win10 virtual machine.
2. Check that the Network Adapter is set to “NAT”. Power on the Win10 virtual machine.
3. Login as user “admin” and password 1qwer$#@!
4. 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.

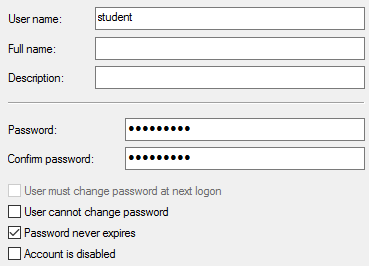
**Exercise Configure your Windows operating system**

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)



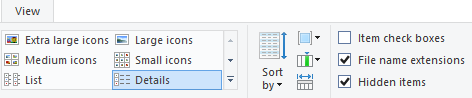
1. In Computer Management, expand Local Users and Groups.
2. Right-click on Users and choose New User.
3. Create a new user with username “student” and password “1qwer$#@!” (or you can set another password value).
4. Uncheck “User must change password at next logon”.
5. Check “Password never expires”.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



1. Click Create. Click Close.
2. Close the Computer Management window.

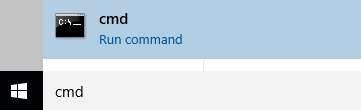
Do not hide extensions for known file types

1. In Windows Explorer, click on View menu.
2. Check the boxes for “File name extensions” and “Hidden items”.



IP address and Computer Name

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



1. 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.

1. If you want to change your computer name, do the following steps:
   1. In Windows Explorer, right-click on“This PC” and chooseProperties.
   2. Under Computer name, domain and workgroup settings, click “Change Settings”.
   3. Click on the Change button.
   4. Enter the new computer name. Click OK.
   5. You will be asked to restart your computer. Restart your VM for the new computer name to take effect.

**Exercise Install Wireshark for Windows**

In Win10 VM

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

**Exercise Test your Understanding**

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

*End of Practical*