**ITP 325 – Lab 02 – Kali Setup**

**Due:**

1 minute before the next class lecture

**Submission:**

1. Answer the questions at the end of this file, and name the document lab02.docx
2. Download the instructor’s GPG key from the following location:

<https://sites.google.com/a/usc.edu/chiso/files>

GPG encrypt the \*.docx with the instructor’s and your own GPG key.

1. Place the encrypted document into the repo and push to changes GitHub

**Procedure:**

1. Go to Code Academy and do the following lesson:

<https://www.codecademy.com/en/courses/learn-the-command-line>

**Note:** If you want you can create a fake account to just finish the lesson. Before you start this, make sure to go over this lab first.

1. Go download Kali Linux at the following location:

<http://www.kali.org/>

1. Read over the different ways you can install Kali Linux at the following location:

<http://docs.kali.org/category/installation>

1. Choose to install Kali Linux in one of the ways listed below on your laptop, USB, or workstation.

* Bootable USB
* Virtual machine with either VirtualBox or VMware
* Dual Booting

**Questions:**

1. Compare and contrast of the different ways to get Kali Linux running on your own machine. Which one did you choose and why?

Dual booting is similar to the Virtual machine kali setup in that almost all of the installation instructions are the same until it gets to the point of partitioning the disk. With dual booting, you would need to select guided- use the largest continuous free space due to the resizing of the windows partitioning steps followed previously. The bootable USB method runs kali live from a USB and is the fastest and easiest method to install kali. It is similar to the other methods in its setup instructions but it is portable and can be booted from any machine anywhere the user chooses. I chose the virtual machine setup because it was the simplest method for me to install on my computer and it was less likely for me to make any kind of mistakes due to the simple instructions.

1. When you setup any type of virtual machine there are different network settings that you can apply to the VM. The general types of networking are bridge, NAT, and Host-Only. When thinking about pentesting, compare and contrast the 3 ways of settings up networking for a VM. Which do you think is best for pentesting?

NAT settings allow the virtual machine to access the network through the host and in the network, the traffic will appear to come from the host. In other words, the VM is hiding behind the host in the network and disguising itself as the host in order to interact with the network. The bridge network settings, on the other hand, allows the VM to access the network through the host but its identity is not hidden behind the host on the network. Instead, the VM has a separate machine on the network (but it still shares the same DHCP server and DNS server with the host) and it shares the resources to the network with the host system, unlike NAT.

The Host-Only network setting is the most restrictive of all the network settings as it does not allow the VM to have access to the internet. The VM’s IP address is assigned through the DHCP server. I think the host only network setting is the safest and best network setting for pentesting because its best to use if you are testing out any worm or viral code. However, the NAT network settings are also a safe route as well for beginners because the identity of the VM is hidden behind the host.

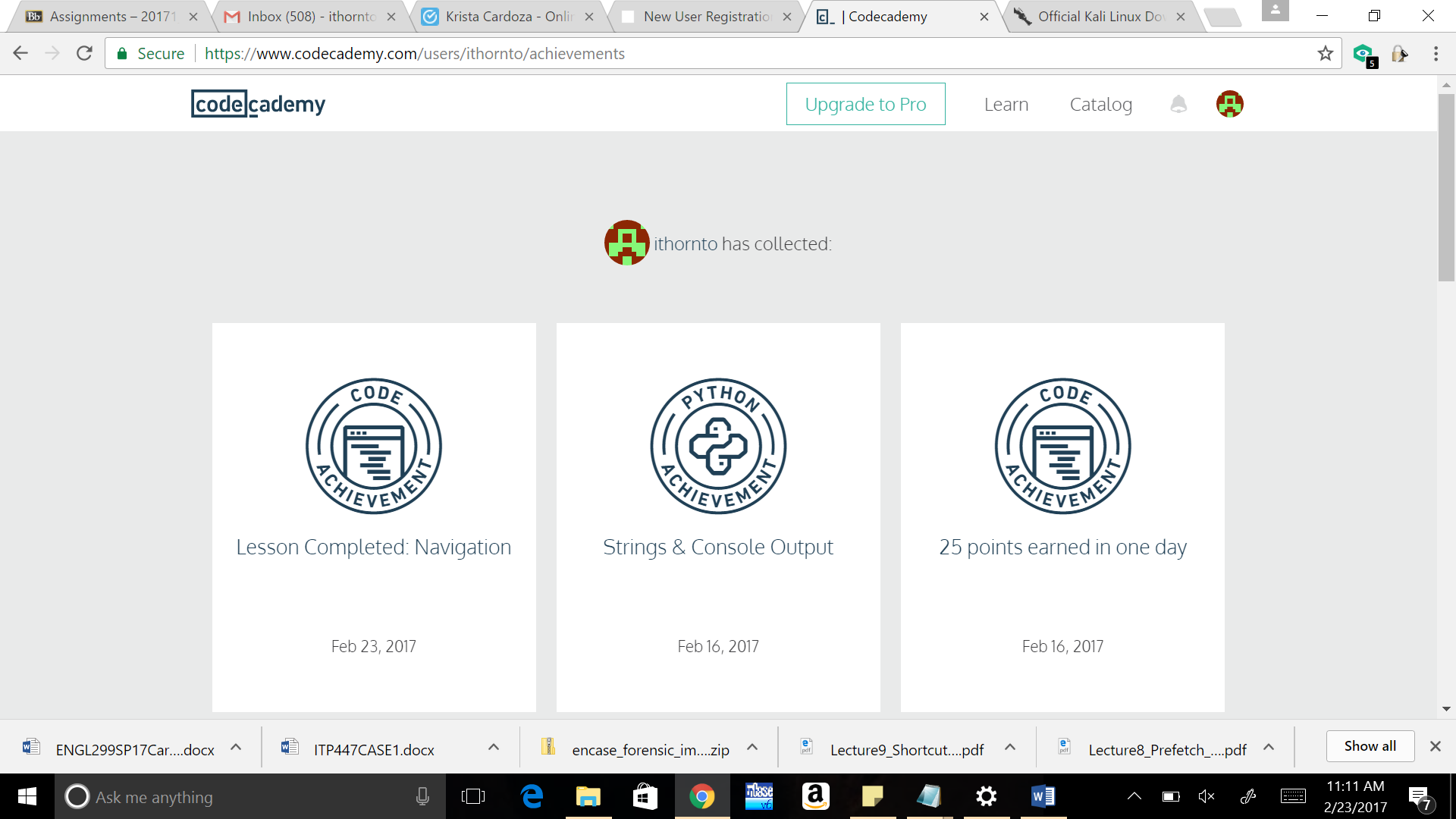
1. In VirtualBox, there are two flavors of NAT. There is just “NAT” and “NAT nework”. What is the difference between the two? Which one is the most similar to NAT within VMware?

NAT or Network Address Translation is for the VM user that wishes to access the internet for simple reasons such as email, simple browsing, and downloading files. The NAT network however, allows the guest machine to access the internet, but does not allow outside machines to access it (the guest machine). Instead the systems using the NAT network are grouped together and prevent systems from outside of this network from directly accessing systems inside of it. The systems inside of this network can communicate with each other and with outside machines using TCP/UDP. The NAT within VMware is most similar to the NAT network because like the NAT network, the addresses of the virtual machines are hidden in a private network that only the host can access. When the virtual machines send a request in the network, the traffic appears to come from the host machine.

<https://www.virtualbox.org/manual/ch06.html#networkingmodes>

<https://www.vmware.com/support/ws3/doc/ws32_network21.html>

1. Prove to the instructor that you completed the Code Academy course. This is an open-ended question, and here is no single right answer. Whatever your proof maybe, make sure to add it into the \*.docx.



**Video:**

**VirtualBox Kali 2.0 Guest Setup**

Read the description of the video to get an idea on the virtual machine setup.

<http://youtu.be/dDPYrePiG9g>

**Installation of Kali 2.0 on VirtualBox**

Read the description of the video to get an idea on the virtual machine setup.

<https://youtu.be/t2A7w_zAPqY>