Lab 1: Network Devices and Technologies - Capturing Network Traffic

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

By performing this lab, students will learn the process of capturing network traffic using three different methods, tcpdump command, Wireshark, and Network Minor.

**Materials**

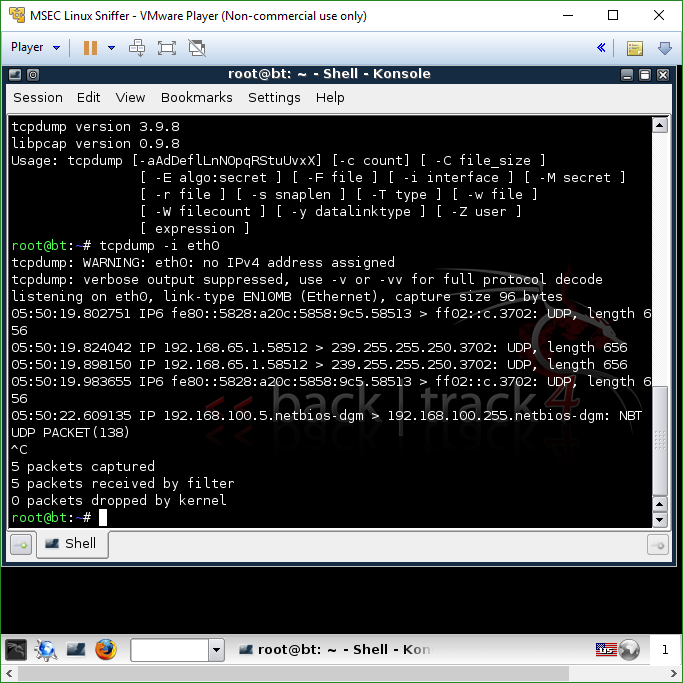
1. Windows 7 Attack Machine
2. Windows 2003 Server
3. Linux Sniffer
4. Backtrack 4

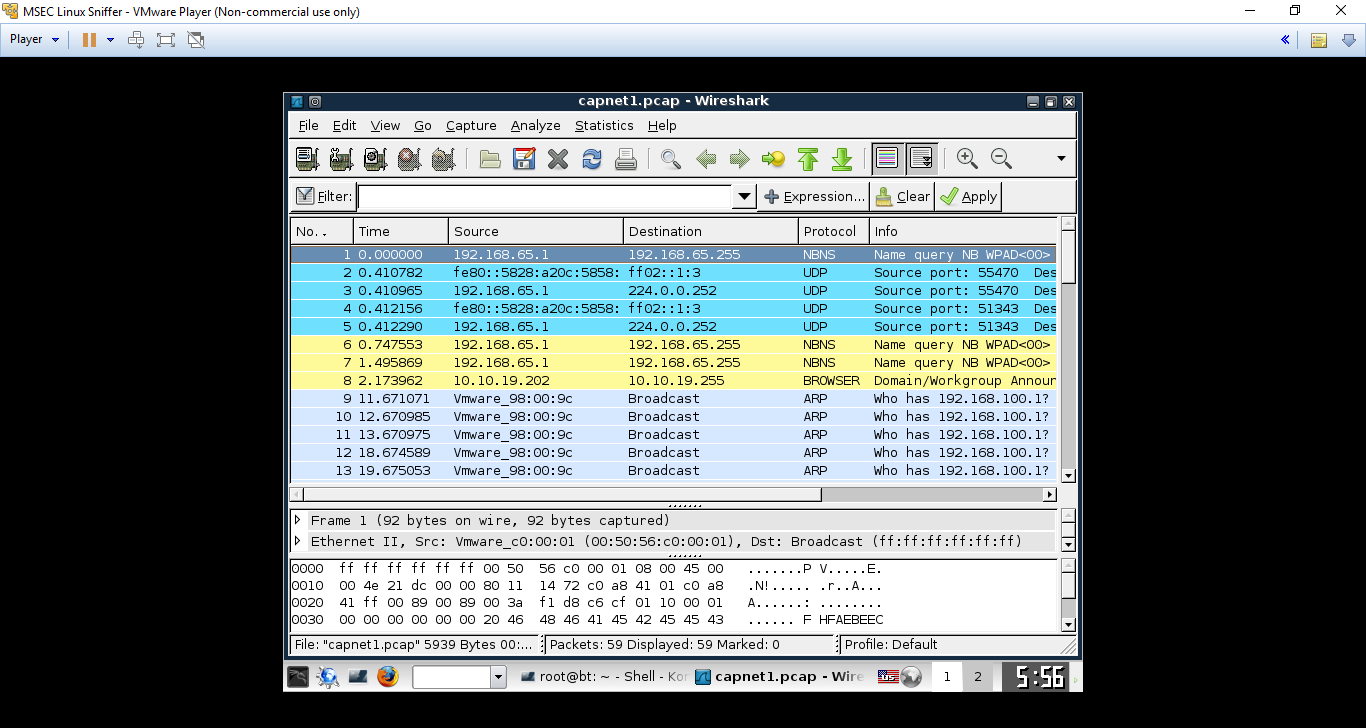
**Methodology**

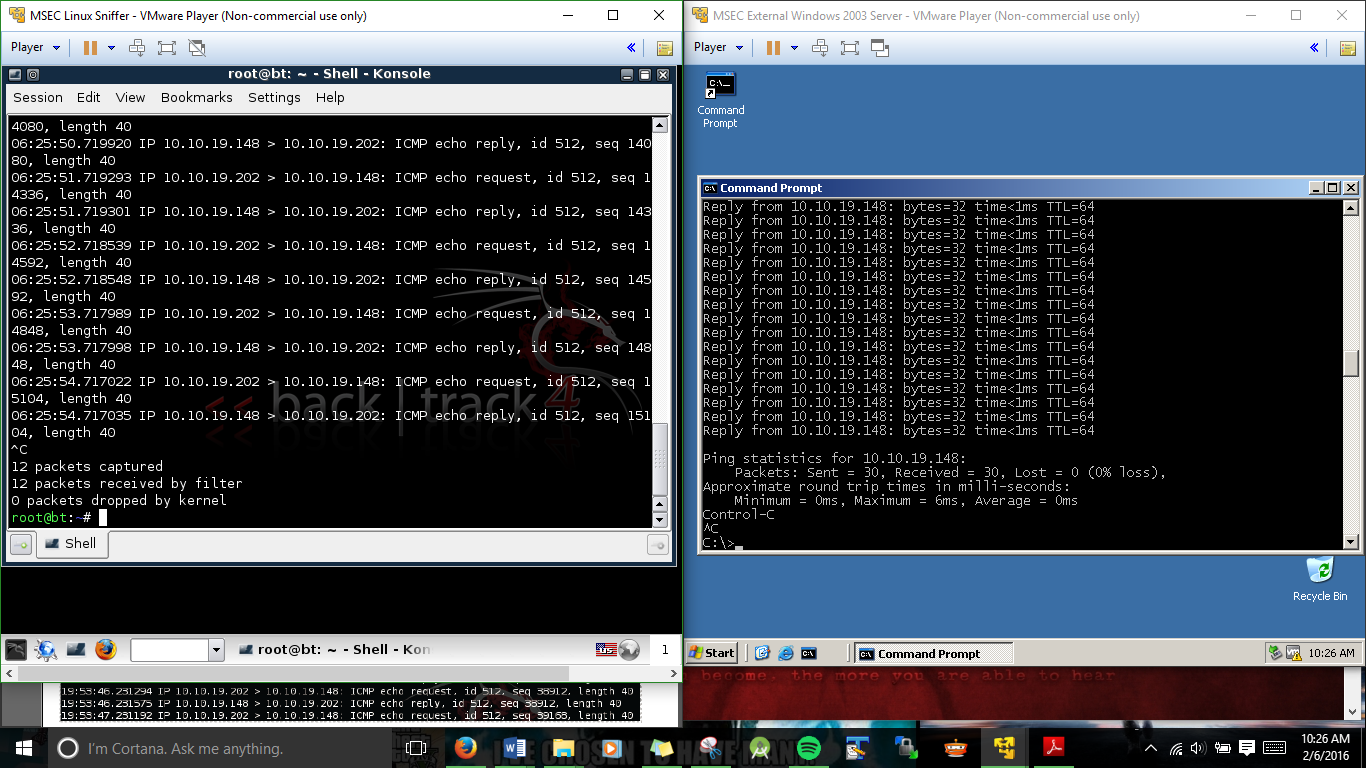
Several tasks using the terminal to ping, scan, and mine information from each VM

**Lab**

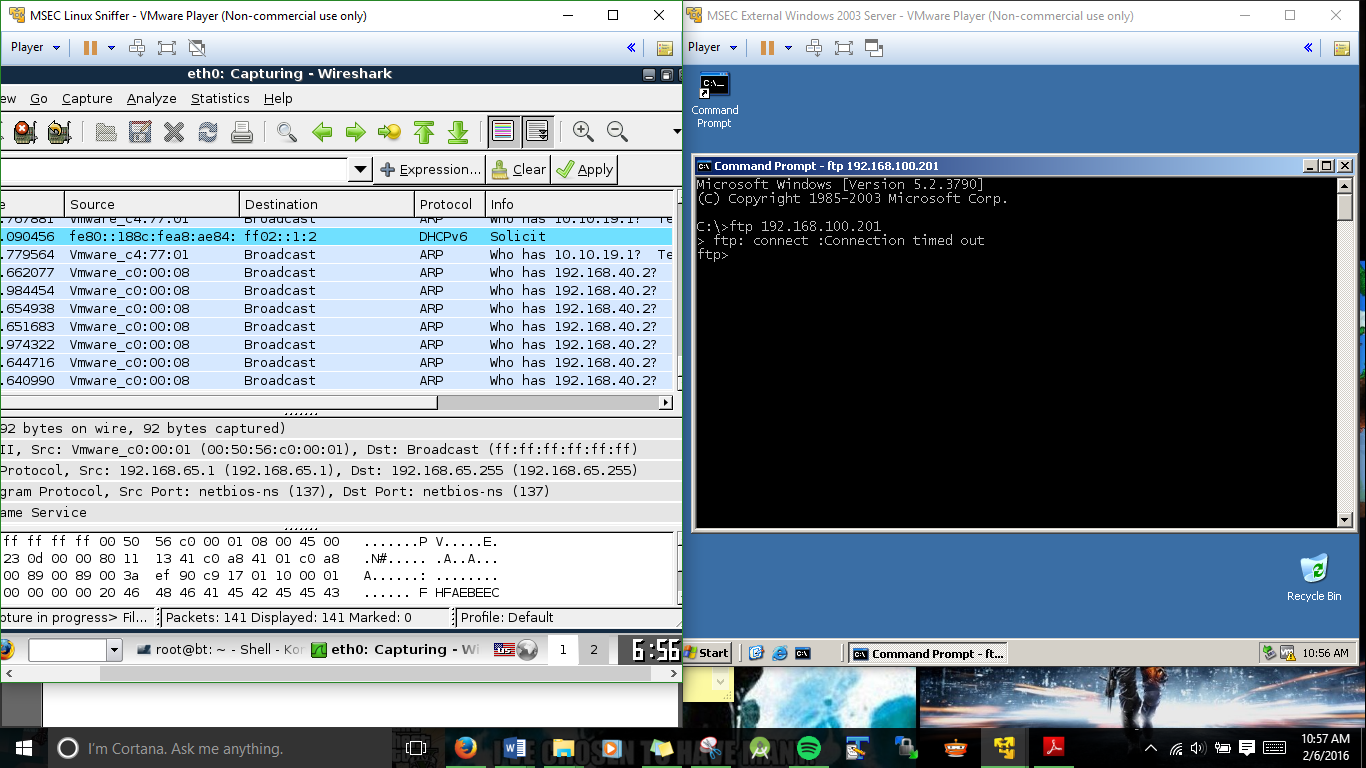
Task 1:

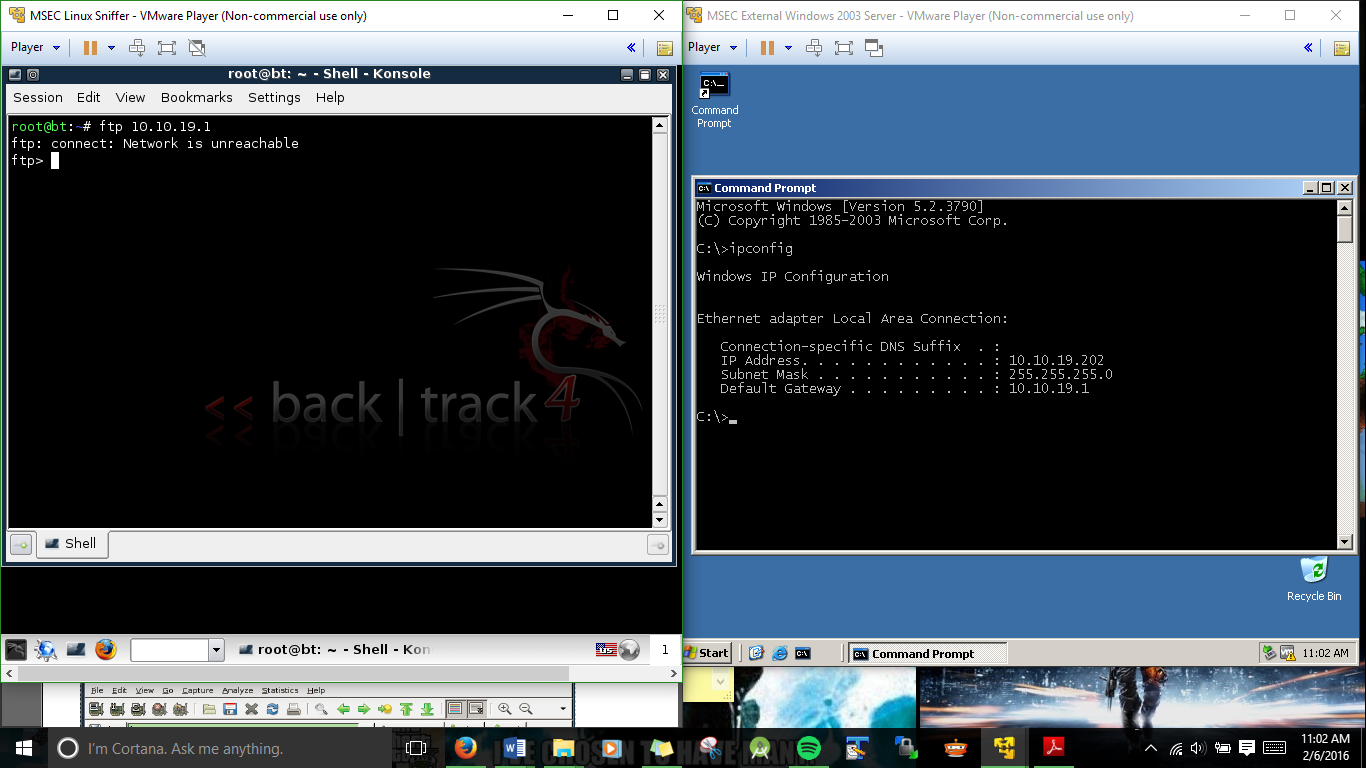
1. 

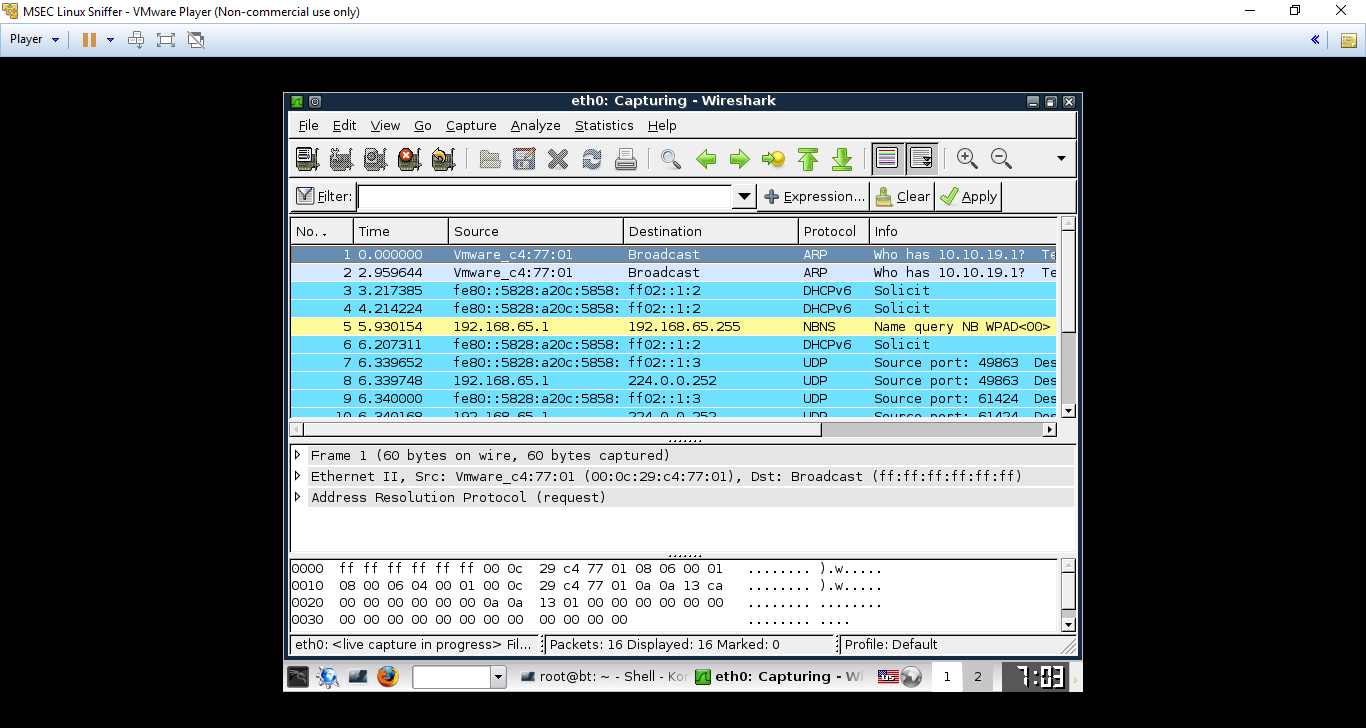
2, 

3. 

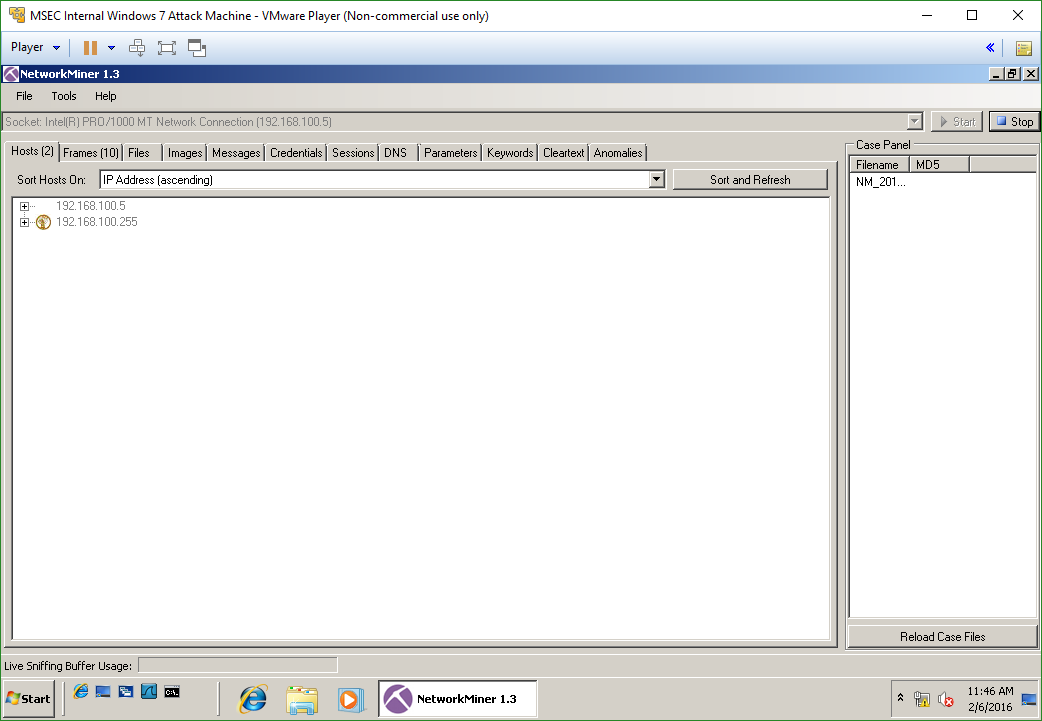
Task 2:

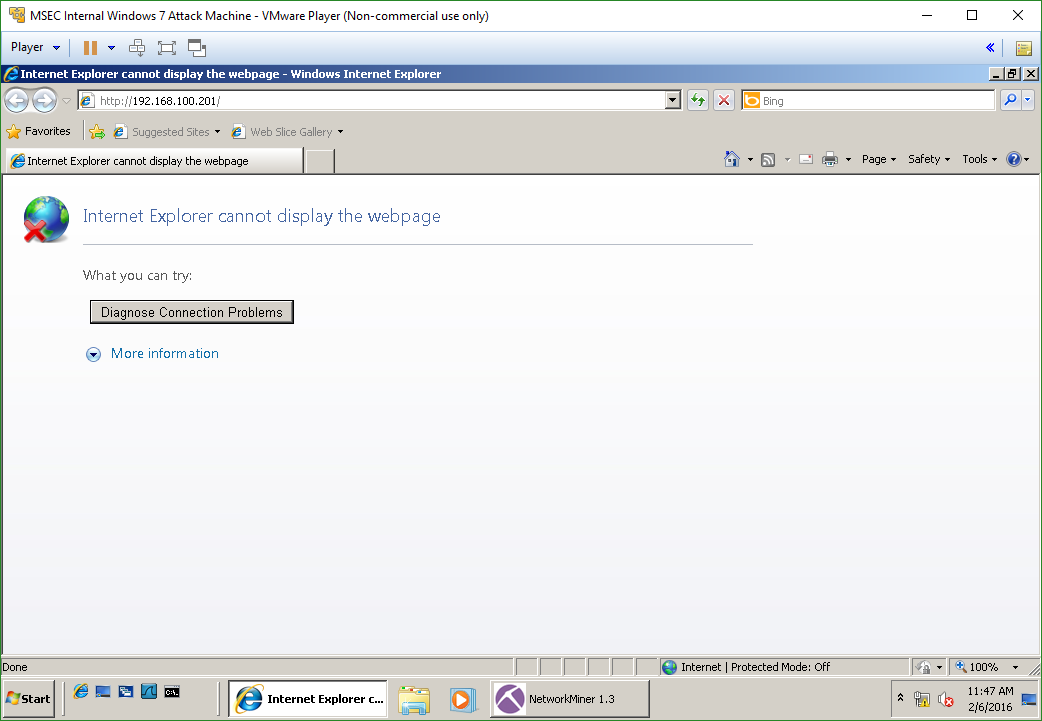
1. 

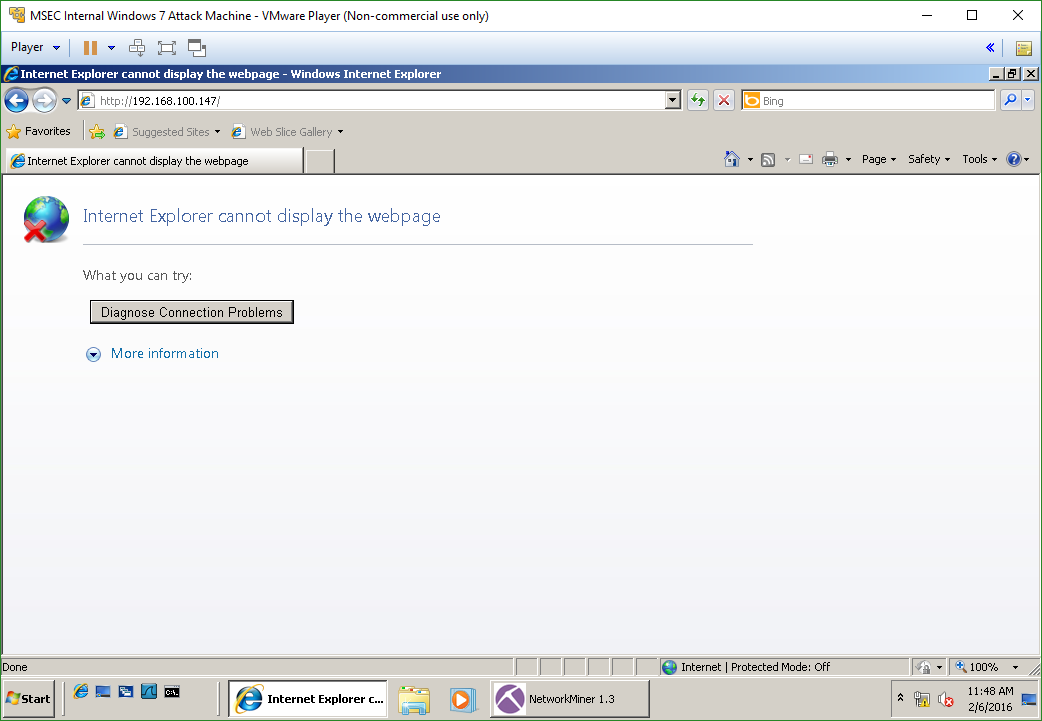
2.

3.

Task 3

1. 

2.

3.

**Questions:**

Task 1

1. Does a network interface on a sniffer machine require an IP Address? **No**
2. In what mode does a sniffer’s network interface operate? **With an up and down position**
3. How do you determine available switches for tcpdump? **By checking the ifconfig command for both the eth0 and eth1 networks and see the positions of the switches**
4. How can you display all the network interfaces in Linux? **Ifconfig will display the network interface’s current status**

Task 2

1. Do FTP usernames and passwords appear in clear text? **As it showed in the pdf, yes they do, which leads me to believe that ftp is unencrypted**
2. How do you choose the interface to capture on within Wireshark? **By clicking the capture tab and choosing the network to capture**
3. How do you filter for a certain protocol within the Wireshark program? **By typing in the search bar with the protocol you desire**
4. How do you open the Wireshark program from the terminal in Linux? **Simply by typing ‘wireshark’**

Task 3

1. What kind of tool is Network Miner? **It appears to be a type of software that will download a website to your machine in order to make a backup of it or for your own personal use**
2. On what operating systems will the network miner program run? **From the lab using it on a Windows 7 VM, I assume it only works on windows based operating systems**
3. How do you parse out web pages of visited sites in Network Miner? **By selecting the site in the file tab**

**Conclusion**

I was having some trouble with the networking configuration, so my pictures for task 2 and 3 aren’t exactly correct to the lab. However, I still think I understood how Wireshark and Network Miner were used in the lab. From my understanding Wireshark was being used to track the user id and password since they were in plaintext on the ftp server, and the Network Miner was used to download or parse the web pages you accessed in the lab. Hopefully this is correct, and maybe later down the line I can get my network configuration up to par on my VM’s but until then this lab has taught me more about the VM’s interface at least.

**Grading Rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | **Points Allowed** | **Points Actual** | **Comments** |
|  |  |  |  |
| **Title page** | **5** |  |  |
| **Screen shots** | **5** |  |  |
| **Questions** | **10** |  |  |
| **Conclusion** | **5** |  |  |
|  |  |  |  |
| **Extra Credit** |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Total Points** | **25** |  |  |