CYBR545- Kali Linux Exercise #2

(Team-based, 100 points)

### Due on Monday 2/20/2023 @11:49PM Group No.:

### Group members names:

# Introduction and submission:

Read each of the following questions and provide your answers after each question, or as instructed in the questions. Keep the format of this file as is and provide group information above. This is a team-based assessment, each group is required to male one submission on eCampus, and each member is expected to submit one peer evaluation for this assessment.

# Grading Rubric:

Questions 1,3,4: 20 points each  
Question 2: 50 points  
Question 5: 10 points

1. First, we need to have Kali Linux and Windows XP added to your virtual box.
   1. In the virtual box, go to tools.
   2. Under NAT Networks, click on create and give a name to your NAT network and an IP address of your choice. You may refer to Figure 1 to see the configuration used and the IP address I used.

****

Figure : Screenshot of NAT Networks settings

* 1. From the settings of each Kali and Windows virtual box settings, add the NAT network created in the previous step as the network adapter as shown in Figure 2.

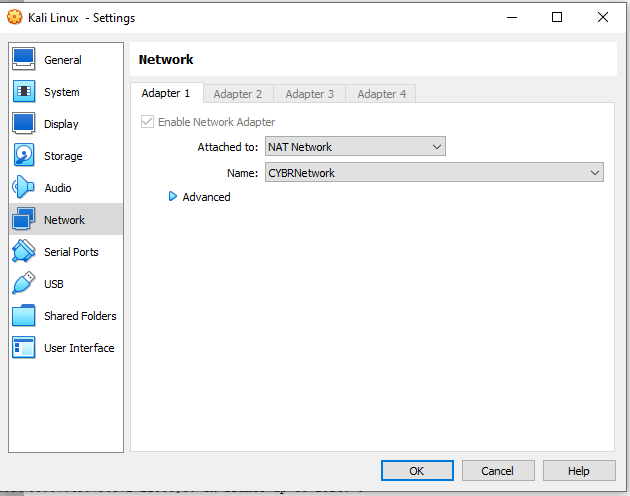


Figure : Screenshot of Network Settings for Kali Linux Network Adapter

* 1. Disable to Firewall of Windows XP
  2. Identify the IP address given to each Kali and Windows.
  3. Start both Kali and Windows
  4. From Kali terminal, ping the windows machine.
  5. From Windows command prompt, ping the kali Linux.
  6. Take s screenshot of the ping results of the kali terminal and windows cmd. You should get a positive response on each, indicating that both systems are on the same network.

**Note**: You will lose access to the internet on both Kali and windows if you keep them using the NAT network. You may change the network adapter for each after Question #5.

1. On your Kali Linux, use Nessus to create a new policy:
   1. Configure your policy to scan your localhost IP address and the Windows virtual machine.
   2. What is the purpose of the policy?
   3. In your own words, what does policy exactly do? How can we benefit from it?
   4. Describe the information that the policy will gather about the target systems and explain why this information is important.
   5. Conduct a scan using your new policy, exports the output as pdf, and submit it with this homework. Name your file [Your\_Group\_Number]\_Nessus\_Policy.
   6. In your own words, summarize the results of the scan.
   7. What actions would you recommend doing based on the results of your scan?
2. Provide a command to view all Nmap Scripting Engine scripts available on your kali Linux.

1. Using Nmap, provide a Kali Linux command to run the default script of the Nmap Scripting Engine def, and implement a porta scan on the windows virtual machine.
   1. Which ports are available?
   2. Provide a screenshot of the results of executing the command in Step 4.
2. On your Kali Linux, start wire shark and start capturing packets.
   1. Are there any packets captured? Why, why not?
   2. On your kali terminal, ping the Windows virtual machine.
   3. Provide a screenshot of your Wireshark captured packets.
   4. Explain what you see. What exactly is happening and what exactly are you monitoring.
   5. Stop pinging the windows machine.