**PROG8190**

**Computer and Application Security \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Assignment #1 – Kali and Metasploitable 2 – due at the date/time specified in eConestoga**

**Marks: / 20**

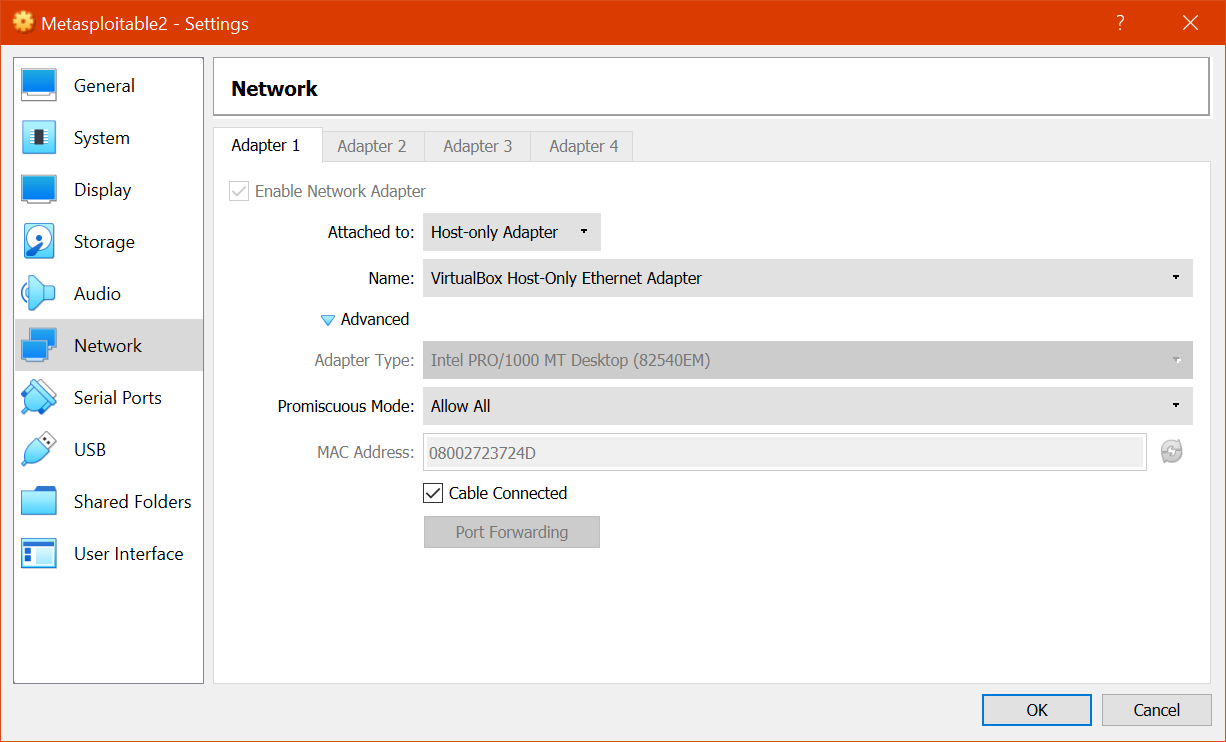
**Weight: 5%**

*This is an individual assignment. Do your own work and do not share your work with others. Sharing work is an Academic Offense and is subject to a penalty. Be aware that all source code and other documentation is automatically checked by eConestoga upon submission.*

The purpose of this assignment is to explore how an exploit from Kali (Metasploit) can be launched onto an unsuspecting and vulnerable version of Ubuntu (Metsplotiable 2)

**This assignment is to be completed individually.**

In this assignment, we will be attempting to exploit the Metasploitable 2 Virutal Machine. Instructions for running this Virtual Machine are available [here](https://youtu.be/fBllzBfFhnw). You may also need to adjust your Network Settings in each Virtual Machine to be using a “Host-only Adapter” connection to have both VMs on the same network:



For tasks 1 through 7 (inclusively), provide a brief sentence about what you are doing.

Task 1

The first step is to find the IP address of each Virtual Machine (Kali and Metasploitable 2). Use the appropriate command on each VM and find out each VM’s IP Address. Remember the values of each IP address. Include these as separate screen shots in a Word document under the heading called “Task 1” **[2 marks]**

Task 2

Verify that the two VMs can communicate with each other by using the **ping** command to ping each other’s IP Address. (You can quit the pings after about 10-15s using CTRL+C in each VM). Include these as separate screen shots in the same Word document as above, but under the heading called “Task 2” **[2 marks]**

Task 3

From your Kali VM, start up Metasploit and issue the command:

search vsftpd 2.3.4

Include the command and its result as a screen shot in the same Word document as above, but under the heading called “Task 3” **[2 marks]**

Task 4

Still within your Kali VM, issue the command:

use exploit/unix/ftp/vsftpd\_234\_backdoor

Include the command and its result as a screen shot in the same Word document as above, but under the heading called “Task 4” **[2 marks]**

Task 5

Still within your Kali VM, issue the command:

show options

Include the command and its result as a screen shot in the same Word document as above, but under the heading called “Task 5” **[2 marks]**

Task 6

Still within your Kali VM, issue the command:

set RHOST {IP Address of Metasploitable 2 VM}

(do not include the braces in the above command)

Include the command and its result as a screen shot in the same Word document as above, but under the heading called “Task 6” **[2 marks]**

Task 7

Still within your Kali VM, issue the command:

exploit

Include the command and its result as a screen shot in the same Word document as above, but under the heading called “Task 7” **[2 marks]**

Under a heading called “Task 8”, provide a Reflection for this Assignment – taking into account the following:

Task 8

* What worked well for you
* What didn’t work well and how you resolved the issue(s)
* What is one thing that you were able to learn or accomplish through this Assignment that you did not know prior to starting.

**[6 marks]**

**Submissions:**

eConestoga submission –

A single MS Word document named:

**FirstName\_LastName\_StudentID\_Assignment1.docx**

Where FirstName, LastName and StudentID (seven-digit student ID) are your particulars.

that contains:

* 1. Assignment Title Page with your name, student ID, “Assignment #1” in the title and date
  2. Answers to the above questions, along with accompanying screen shots
  3. References

Late penalties will apply for any/all submissions submitted past the due date.

A -10% penalty will be applied for any files that are zipped up or not using the correct naming format.

As this is a technical report, proper spelling and grammar will also be required and marks may be lost for reports that have poor spelling and / or grammar. A more detailed marking scheme is shown in the Rubric associated with the Assignment Folder in eConestoga.