CYBR 4840/5840 Final, At-home Section (Maximum point: 30point)

***Late submission is not allowed. This is an exam**

***All commands should be readable in your screenshot**

***All tasks works in our VMware environment**

Please provide screenshot for each task to highlight the commands you used and the results you obtained with red box. **Brief explanations on what you have done and what you have observed for each task are required for the report**.

For the final exam at-home section, you will use Kali Linux (Attacking machine), Windows XP (T1), and Windows 7 (T2) in your **VMware environment**. In case you need to install new Windows XP machines, use **Windows XP… renewed03.7z** from this address (Use your **UCMO** account)

https://drive.google.com/drive/folders/1iJ-773pEs3FRhnjbwDFWyxUmUBvRmPKz?usp=sharing

0. Login Windows 7 using username **georgia**.

1) Open the notepad and enter the following information.
   a. **This is a domain admin password P@$$word123**

   Name the file document.txt and save it under the C:\Users\georgia folder.
2) In Windows Defender setting, turn real-time protection off from "Windows Defender" Tools ⇒ Options ⇒ un-check "Use real-time protection" ⇒ Save

1. **[2pts, IP addresses]** Provide IP addresses of your Kali, Windows XP, and Windows 7 machines.

2. **[4pts, Firewall rules]** On Windows 7, set the firewall to block all inbound TCP traffic from Kali. After that, run Nmap from Kali against Windows 7 to verify that the firewall is working. Logout Windows 7 after you finish this task. Provide screenshots of the commands and scan results.

1. [1pts] First, you need to turn **on** all built-in firewall rule on Windows 7 using the command line, and run Nmap from Kali without any Nmap options (Nmap scan will not work).
2. [1pts] **Allow** all traffic (any protocol) from Kali on firewall rule using the command line and try Nmap from Kali using -Pn option (Nmap scan will work now).
3. [1pts] Then, **Block** TCP traffic from Kali on firewall rule using the command line and try Nmap from Kali using -Pn option (Nmap scan doesn't work finally)
4. [1pts] Finally, **Allow** all traffic (any protocol) from Windows XP on firewall rule using the command line.

3. **[3pts, Attacking Windows XP]** Use Msfvenom from Kali Linux to create a malicious file and save it as file.exe under the /tmp folder. Please use windows/meterpreter/reverse_tcp as the payload. Set up the Metasploit on Kali to listen from the payload. Open a simple http server at /tmp folder. Log in to Windows XP and download and run the file.exe at Windows XP machine. Please do not close the meterpreter session obtained from this task as you will need it for the following tasks.

1. [3pts] Provide screenshots for the msfvenom command, python http server command, and the **sysinfo** command from the meterpreter result.

4. **[6pts, Scanning Windows 7 indirectly]** From Kali, use **two different methods** to do a TCP port scan by pivoting against Windows 7 through Windows XP. To reduce time, scan only 1-500 ports or top 100 popular ports. You need to use the previous meterpreter session obtained in task 3 (You cannot log in Windows XP to do this. And direct scanning from Kali to Windows 7 should not work due to the firewall rules in task 2).

1) [3pts] Provide screenshots when you use MSF module to scan Windows 7's TCP ports.

2) [3pts] Provide screenshots when you use a proxy server to scan Windows 7's TCP ports.

5. **[10pts, Remote Execution]** You want to make Windows 7 to connect to Kali and want to create a service remotely from Windows XP to do this.

- Use the session/shell obtained in task 3 and use the Netcat executable in C:\Tools folder in Windows 7 to create a remote backdoor to connect with Kali.
- Open a Netcat connection using port 3456 with command execution (-e) option to use cmd.exe.
- Use sc to remotely run a command to do this task. You can use the georgia's admin credentials for Windows 7 machine but are not allowed to directly login Windows XP and Windows 7.
- Run **pwd** command at the Netcat connection and provide a screenshot. Be careful with the connecting direction of the Netcat (think of which one should be the client or the server). To get the full point, provide all screenshots of the commands you used.

6. **[5pts, Using Nmap & MSF to get into Windows 7]** Let's try another way to get into the Windows 7 machine. From task 4 scanning result, you can notice that TCP port 445 is open.

1) [2pts] Run the Nmap smb-vuln-ms17-010 NSE script from Kali to confirm Windows 7 is vulnerable. Refer to this page to use the script in the right way (still, you cannot directly use the script against Windows 7) (https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html).

2) [3pts] Then, choose the corresponding exploit module based on the vulnerability name from MSF in Kali to get a meterpreter shell against Windows 7. You can run this exploit using the previous meterpreter session against Windows XP & added route from task 4. Do not close the meterpreter session obtained from this task as you will need it for the next task. You may want to try different stagers if the attack doesn't work well.

7. **[Extra point, 3pts]** Use the session obtained in task 6 or Netcat conection from task 5 to conduct a search on the C drive on Windows 7 to find the password file you created in task 0. All you know is that the administrator may leave a txt file which contains the *password* string under C:\Users directory. You do not know the file name.