|  |  |
| --- | --- |
| Student Name | <Enter Name Here> |
| Activity Type | Guided Practice / Computer Lab |

## Instructions

Perform the Guided Practice per the instructions in your course. As you complete each lab, insert a screenshot of your results. Perform all the tasks shown below.

**Note: Some tasks in the labs are not completed in this class, instead they are completed in the associated lab class.**

**Only** provide screenshots for the tasks that specify a screenshot. **There** **should** **be** a total of **6 screenshots** for this lab.

Complete the following lab tasks in the Footprinting and **Malware** ILab Module:

1. **Lab 2** - Infect the target system using a virus
   * **Task 1** - Create a virus using the JPS Virus Maker Tool and infect the target system
     1. Screenshot step 23.
2. **Lab 3** - Perform static malware analysis
   * **Task 1** Perform online malware scanning using Hybrid Analysis
   * **Task 2** Perform a string search using BinText
   * **Task 3** Identify packing and obfuscation methods using PEid
   * **Task 4** Analyze ELF Executable File using Detect It Easy (DIE)
   * **Task 5** Find the portable executable (PE) information of a malware executable file using PE Explorer
   * **Task 6** Identify file dependencies using Dependency Walker
   * **Task 7** Perform malware disassembly using IDA and OllyDbg
   * **Task 8** Perform Malware Disassembly using Ghidra
     1. Screenshot step 21.
3. **Lab 4** - Perform dynamic malware analysis.
   * **Task 1** Perform port monitoring using TCPView and CurrPorts
   * **Task 2** Perform process monitoring using Process Monitor
   * **Task 3 -** Perform Registry Monitoring using Reg Organizer
   * **Task 4** Perform Windows services monitoring using Windows Service Manager (SrvMan)
   * **Task 5** Perform startup program monitoring using Autoruns for Windows and WinPatrol
   * **Task 6** Perform installation monitoring using Mirekusoft Install Monitor
   * **Task 7** Perform files and folder monitoring using PA File Sight
   * **Task 8** Perform device driver monitoring using DriverView and Driver Reviver
   * **Task 9** - Perform DNS Monitoring using DNSQuerySniffer
     1. Screenshot step 18.

Complete the following lab tasks in the **Sniffing** ILab Module:

1. **Lab 1** - Perform active sniffing
   * **Task 4** Perform a Man-in-the-Middle (MITM) attack using Cain & Abel
   * **Task 5** Spoof a MAC address using TMAC and SMAC
   * **Task 6** - Spoof a MAC Address of Linux Machine using macchanger
     1. Screenshot step 15.
2. **Lab 2** - Perform network sniffing using various sniffing tools.
   * **Task 2** Analyze a network using the Omnipeek Network Protocol Analyzer
   * **Task 3** Analyze a network using the SteelCentral Packet Analyzer
     1. Screenshot step 39.
3. **Lab 3** - Detect network sniffing
   * **Task 2 -** Detect ARP Poisoning using the Capsa Network Analyzer
     1. Screenshot step 41.

Summary: As a result of this lab, I have learned:

* Include a few paragraphs summarizing the key skills you have acquired during this guided practice.