INDEX

Sr. No.	Title	Page No.	Sign
Pr 1	a. Files: Lab01-01.exe and Lab01-01.dll. b. Analyze the file Lab01-02.exe. c. . Analyze the file Lab01-03.exe. d. Analyze the file Lab01-04.exe. e. Analyze the malware found in the file Lab03-01.exe using basic dynamic analysis tools. f. Analyze the malware found in the file Lab03-02.dll using basic dynamic analysis tools. g. Execute the malware found in the file Lab03-03.exe while monitoring it using basic dynamic analysis tools in a safe environment. h. Analyze the malware found in the file Lab03-04.exe using basic dynamic analysis tools.		
Pr 2	a. Analyze the malware found in the file Lab05-01.dll using only IDA Pro. The goal of this lab is to give you hands-on experience with IDA Pro. If you've already worked with IDA Pro, you may choose to ignore these questions and focus on reverse-engineering the malware. b. analyze the malware found in the file Lab06-01.exe. c. Analyze the malware found in the file Lab06-02.exe. d. analyze the malware found in the file Lab06-03.exe. e. analyze the malware found in the file Lab06-04.exe.		
Pr 3	a. Analyze the malware found in the file Lab07-01.exe. b. Analyze the malware found in the file Lab07-02.exe. c. For this lab, we obtained the malicious executable, Lab07-03.exe, and DLL, Lab07 03.dll, prior to executing. This is important to note because the mal- ware might change once it runs. Both files were found in the same directory on the victim machine. If you run the program, you should ensure that both files are in the same directory on the		

	analysis machine. A visible IP string beginning with 127 (a loopback address) connects to the local machine. (In the real version of this malware, this address connects to a remote machine, but we've set it to connect to localhost to protect you.) d. Analyze the malware found in the file Lab09-01.exe using OllyDbg and IDA Pro to answer the following questions. This malware was initially analyzed in the Chapter 3 labs using basic static and dynamic analysis techniques. e. Analyze the malware found in the file Lab09-02.exe using OllyDbg to answer the following questions. f. Analyze the malware found in the file Lab09-03.exe using OllyDbg and IDA Pro. This malware loads three included DLLs (DLL1.dll, DLL2.dll, and DLL3.dll) that are all built to request the same memory load location. Therefore, when viewing 44 these DLLs in OllyDbg versus IDA Pro, code may appear at different memory locations. The purpose of this lab is to make you comfortable with finding the correct location of code within IDA Pro when you are looking at code in OllyDbg.		
Pr 4	a. This lab includes both a driver and an executable. You can run the executable from anywhere, but in order for the program to work properly, the driver must be placed in the C:\Windows\ System32 directory where it was origi- nally found on the victim computer. The executable is Lab10-01.exe, and the driver is Lab10-01.sys. b. The file for this lab is Lab10-02.exe. c. This lab includes a driver and an executable. You can run the executable from anywhere, but in order for the program to work properly, the driver must be placed in the C:\Windows\System32 directory where it was originally found on the victim computer. The executable is Lab10-03.exe, and the driver is Lab10-03.sys.		
Pr 5	a. Analyze the malware found in Lab11-01.exe. b. Analyze the malware found in Lab11-02.dll. Assume that a suspicious file named Lab11-02.ini was also found with this malware. c. Analyze the malware found in Lab11-03.exe and		

	Lab11-03.dll. Make sure that both files are in the same directory during analysis		
Pr 6	a.Analyze the malware found in the file Lab12-01.exe and Lab12-01.dll. Make sure that these files are in the same directory when performing the analysis. b.Analyze the malware found in the file Lab12-02.exe. c. Analyze the malware extracted during the analysis of Lab 12-2, or use the file Lab12-03.exe. d. Analyze the malware found in the file Lab12-04.exe.		
Pr 7	a. Analyze the malware found in the file Lab13-01.exe. b. Analyze the malware found in the file Lab13-02.exe. c. Analyze the malware found in the file Lab13-03.exe.		
Pr 8	a. Analyze the malware found in file Lab14-01.exe. This program is not harmful to your system. b. Analyze the malware found in file Lab14-02.exe. This malware has been configured to beacon to a hard-coded loopback address in order to prevent it from harming your system, but imagine that it is a hard-coded external address. c. This lab builds on Practical 8 a. Imagine that this malware is an attempt by the attacker to improve his techniques. Analyze the malware found in file Lab14 03.exe. d. Analyze the sample found in the file Lab15-01.exe. This is a command-line program that takes an argument and prints “Good Job!” if the argument matches a secret code. e. Analyze the malware found in the file Lab15-02.exe. Correct all anti-disassembly countermeasures before analyzing the binary in order to answer the questions. f. Analyze the malware found in the file Lab15-03.exe. At first glance, this binary appears to be a legitimate tool, but it actually contains more functionality than advertised.		

Pr 9	a. Analyze the malware found in Lab16-01.exe using a debugger. This is the same malware as Lab09-01.exe, with added anti-debugging techniques. b. Analyze the malware found in Lab16-02.exe using a debugger. The goal of this lab is to figure out the correct password. The malware does not drop a mali- cious payload. c. Analyze the malware in Lab16-03.exe using a debugger. This malware is similar to Lab09-02.exe, with certain modifications, including the introduction of anti debugging techniques. d. Analyze the malware found in Lab17-01.exe inside VMware. This is the same malware as Lab07-01.exe, with added anti-VMware techniques. e. Analyze the malware found in the file Lab17-02.dll inside VMware. After answering the first question in this lab, try to run the installation exports using rundll32.exe and monitor them with a tool like procmon. f. Analyze the malware Lab17-03.exe inside VMware.		
Pr 10	a. Analyze the file Lab19-01.bin using shellcode_launcher.exe. b. The file Lab19-02.exe contains a piece of shellcode that will be injected into another process and run. Analyze this file. c. Analyze the file Lab19-03.pdf. If you get stuck and can't find the shellcode, just skip that part of the lab and analyze file Lab19-03_sc.bin using shellcode_launcher.exe. d. The purpose of this first lab is to demonstrate the usage of the this pointer. Analyze the malware in Lab20-01.exe. e. Analyze the malware In Lab20-02.exe. f. Analyze the malware in Lab20-03.exe. g. Analyze the code in Lab21-01.exe. h. Analyze the malware found in Lab21-02.exe on both x86 and x64 virtual machines.		