Faculty of Business, IT, and Management

HACK2200 Hacking and Exploits

Lab 6: Malware and Viruses

Answer File

**NOTE: There is a 5 marks penalty per extra screenshot, and a 5 marks penalty per command/text not typed when required.**

**Part1- Viruses**

Insert Screenshot#1 Here (10 Marks):

A screenshot of a computer

Description automatically generated

Insert Screenshot#2 Here (10 Marks):

A screenshot of a computer

Description automatically generated with medium confidence

Insert Screenshot#3 Here (10 Marks):

Graphical user interface

Description automatically generated

**Part 2 – Malware Analysis**

Insert Screenshot#4 Here (10 Marks):

Graphical user interface, text, application

Description automatically generated

**Question 1:** The address of the DllMain is **0x1000D02E** (hint: your answer is an address) (10 Marks):

Insert Screenshot#5 Here (10 Marks):

Graphical user interface, text, application

Description automatically generated

**Questions 2.** Use the Imports window to browse to gethostbyname. Where is the import located?

**0x100163CC** (hint: your answer is an address) (5 Marks):

Insert Screenshot#6 Here (10 Marks):

Graphical user interface, table

Description automatically generated

**Questions 3.** How many separate functions call gethostbyname?

**9** (hint: your answer is a number) (10 Marks):

**Question 4:** The DNS request will be made to the url: **pics.praticalmalwareanalysis.com** (5 Marks):

Insert Screenshot#7 Here (5 Marks):

Graphical user interface, text, application

Description automatically generated

**Questions 5.** Use the Strings window to locate the string \cmd.exe /c in the disassembly. Where is it located?

The string resides in **xdoors\_d:10095B34** (hint: your answer is the section name and the address) (5 Marks):