CS 370 Introduction to Security **Week 9: Problem Set 9**
Instructor Name: Rakesh Bobba

Introduction/Purpose

The purpose of this assignment is to help you work on the concepts of Malware covered in Week 9

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

- Malware: Viruses
- Malware: Worms
- Malware: Other

Chapter 6 from the reference book Stallings and Brown

Instructions/Questions

Please answer the questions below.

Malware

Q1 [5 pts] What is the difference between a metamorphic virus and a stealth virus? How are they similar?

- Whereas Metamorphic viruses rewrite themselves on each infection, stealth viruses attempt to stay hidden by having signatures that are constant (i.e. they do not rewrite themselves), but are designed to be harder to find to avoid virus protection software. These viruses are similar, though, because they are both trying to avoid getting caught by the malware scanners on a machine – one by having a low profile signature / one that is hard to detect or identify, and one that constantly changes its signature across infections.

Q2 [5 pts] Traditionally, what is the difference between a Virus and a Worm? Can a malware exhibit the traits of both a Virus and a Worm?

- Traditionally, worms differ from viruses as they are self sufficient, requiring no host program to ‘latch on to’, or a human to distribute them. Worms are designed to replicate and spread all on their own, as a standalone piece of malware that replicates. This is contrasted with Viruses which typically need to planted on a computer and then spreads to the executables or data on that system.
- Yes, there exists malware that can be classified as - or exhibit traits of – both. For example malware that were to replicate itself and include a component that replicates to other servers (worm) but then also infects the executables of the local system while its there (virus) would check both boxes.

Q3 [5 pts] What is a rootkit? Name two ways a kernel mode rootkit can change the

underlying system programs?

- A Rootkit is a piece of malware that tries to remain hidden and slightly modify the functioning of the system. It can do this in many way, a couple of which are listed below:
- A Rootkit can change the pointers of a syscall table to redirect calls of those syscalls through the kit functions.
- A Windows Rootkit could also modify the pointers of the Windows API, such that programs from the rootkit are used instead of the expected API call.

Q4 [5 pts] What is difference between a polymorphic virus and an encrypted virus?

- A Polymorphic virus is one that can take many forms (mutate) while retaining the original function. This is contrasted with an encrypted virus which is mostly encrypted except for the key and decryption algorithm.

Submission Details

Submit a PDF file with the questions and your corresponding answers
The assignment is worth 20 points. It is due Saturday of Week 9 at Midnight.