ITBU 443: Threats and Counter Measures, Homework 06

Chapter 06, *Computer Security, Principles and Practices*

Readings

Read chapter 06 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. Define *malware* as that term refers to malicious computer code.
2. Define *computer virus* as that term refers to malicious computer code. What does a computer virus have in common with a disease-causing virus?
3. Describe the three parts of a computer virus.
4. What is the difference between a polymorphic virus and a metamorphic virus?
5. Define *computer worm* as that term refers to malicious computer code. What does a computer worm have in common with an infectious worm?
6. If you were given an assignment to implement a *user interface redress attack*, how would you implement it? Note that this is a client side attack, so you are llimited to client-side technologies, such as HTML, CSS, JavaScript, etc.
7. What is a *Trojan Horse* as that term is used to rever to malware? Give a brief summary of how a Trojan Horse would work.
8. What is a *logic bomb*? Write some pseudo-code to implement a logic bomb You can assume that calling the function `totallyDestroyComputer()` will activate the payload.
9. How would an attacker implement a program to steal a user's identity?
10. Make the case that implementing a *backdoor* is a good idea. When I developed applications, I commonly included a backdoor as a good practice, but I was never caught. How would you defend this practice?
11. Important question: What is the difference between kernel mode and user mode?
12. What is the difference between *phishing* and *spear-phishing*? What is *whaling*?