CSH6 CH 16 REVIEW QUESTIONS

1. What is malware?
2. Which of the following is the best example of the definition of _worm_?
3. Which of the following is the best example of the definition of _logic bomb_?
4. Which of the following is/are possible outcomes of malware infection?
5. What's a _botnet_?
6. One of the most famous malware outbreaks began on 2 Nov 1988 and took down much of the tiny Internet of that time. What was this malware called?
7. Which of the following is a _vector_ for malware?
8. A malware writer called Ivan Khaturiaski is a Byelorussian national working for the Russian Business Network; in the malicious-code threat model, Ivan is an example of a(n)
9. What's a _bot_?
10. In the malicious-code threat model, the _____ can include any resource of interest.
11. How often should user antimalware software be permitted to update itself?
12. A classic type of virus inserts a JUMP instruction in the infected code so that execution jumps to additional code, then returns to the normal code. This type of virus is a _____.
13. In the malicious-code threat model, the _____ can include an allowed physical or logical path.
14. In the malicious-code threat model, the _____ can include execution of malicious code or logic.
15. Which of the following is the best example of the definition of _virus_?
16. What is one of the elements of the consensus on the idea of using beneficial viruses to patch servers or networks?
17. What do we call viruses that encrypt themselves to generate many different versions in an effort to defeat antivirus scanners?
18. In the 1980s, one of the earliest types of virus was loaded into a computer at bootup from an infected diskette. This type of virus was a _____.
19. Who seem(s) to be writing malware in this decade of the 21st century?
20. In the malicious-code threat model, the _____ can include individuals, organizations, and nation-states.
21. Which of the following describes antimalware functions that rely on strings characteristic of specific known malware?
22. Is writing malware illegal in the US?
23. The MS-Word macro virus of August 1995 raised the threat level for viruses because it _____.
24. What is the oldest method of recognizing malware?
25. Which of the following describes antimalware functions that rely on monitoring systems for unusual activity?
26. In the malicious-code threat model, the _____ can include a variety of results such as surveillance, disruption, destruction, or publicity.
27. What is the consensus on the idea of using beneficial viruses?