**Chapter 6 – Malicious Software**

**TRUE/FALSE QUESTIONS:**

T F 1. Malicious software aims to trick users into revealing sensitive personal data.

T F 2. Keyware captures keystrokes on a compromised system.

T F 3. Metamorphic code is software that can be shipped unchanged to a

heterogeneous collection of platforms and execute with identical semantics.

T F 4. A virus that attaches to an executable program can do anything that the

program is permitted to do.

T F. 5. It is not possible to spread a virus via a USB stick.

T F 6. A logic bomb is the event or condition that determines when the payload is

activated or delivered.

T F 7. Many forms of infection can be blocked by denying normal users the right to

modify programs on the system.

T F 8. A macro virus infects executable portions of code.

T F 9. E-mail is a common method for spreading macro viruses.

T F 10. In addition to propagating, a worm usually carries some form of payload.

T F 11. A Trojan horse is an apparently useful program containing hidden code that,

when invoked, performs some harmful function.

T F 12. Packet sniffers are mostly used to retrieve sensitive information like

usernames and passwords.

T F 13. A bot propagates itself and activates itself, whereas a worm is initially

controlled from some central facility.

T F 14. Every bot has a distinct IP address.

T F 15. Programmers use backdoors to debug and test programs.

**MULTIPLE CHOICE QUESTIONS:**

1. A program that is covertly inserted into a system with the intent of compromising the integrity or confidentiality of the victim’s data is \_\_\_\_\_\_\_\_\_\_.

A. Adobe B. Animoto

C. malware D. Prezi

1. \_\_\_\_\_\_\_\_\_\_ are used to send large volumes of unwanted e-mail.

A. Rootkits B. Spammer programs

C. Downloaders D. Auto-rooters

1. A \_\_\_\_\_\_\_\_\_\_ is code inserted into malware that lies dormant until a predefined condition, which triggers an unauthorized act, is met.

A. logic bomb B. trapdoor

C. worm D. Trojan horse

1. The term “computer virus” is attributed to \_\_\_\_\_\_\_\_\_\_.

A. Herman Hollerith B. Fred Cohen

C. Charles Babbage D. Albert Einstein

1. Computer viruses first appeared in the early \_\_\_\_\_\_\_\_\_\_.

A. 1960s B. 1970s

C. 1980s D. 1990s

6. The \_\_\_\_\_\_\_\_\_\_ is what the virus “does”.

A. infection mechanism B. trigger

C. logic bomb D. payload

7. The \_\_\_\_\_\_\_\_\_\_ is when the virus function is performed.

A. dormant phase B. propagation phase

C. triggering phase D. execution phase

8. During the \_\_\_\_\_\_\_\_\_\_ the virus is idle.

A. dormant phase B. propagation phase

C. triggering phase D. execution phase

9. A \_\_\_\_\_\_\_\_\_\_ uses macro or scripting code, typically embedded in a document and triggered when the document is viewed or edited, to run and replicate itself into other such documents.

A. boot sector infector B. file infector

C. macro virus D. multipartite virus

10. \_\_\_\_\_\_\_\_\_\_ is the first function in the propagation phase for a network worm.

A. Propagating B. Fingerprinting

B. Keylogging D. Spear phishing

11. Unsolicited bulk e-mail is referred to as \_\_\_\_\_\_\_\_\_\_.

A. spam B. propagating

C. phishing D. crimeware

12. \_\_\_\_\_\_\_\_\_\_ is malware that encrypts the user’s data and demands payment in order to access the key needed to recover the information.

A. Trojan horse B. Ransomware

C. Crimeware D. Polymorphic

13. A \_\_\_\_\_\_\_\_\_\_ attack is a bot attack on a computer system or network that causes a loss of service to users.

A. spam B. phishing

C. DDoS D. sniff

14. The ideal solution to the threat of malware is \_\_\_\_\_\_\_\_\_\_.

A. identification B. removal

C. detection D. prevention

15. \_\_\_\_\_\_\_\_\_\_ will integrate with the operating system of a host computer and monitor program behavior in real time for malicious actions.

A. Fingerprint-based scanners B. Behavior-blocking software

C. Generic decryption technology D. Heuristic scanners

**SHORT ANSWER QUESTIONS:**

1. A \_\_\_\_\_\_\_\_\_ is a set of programs installed on a system to maintain covert access to that system with administrator (root) privileges while hiding evidence of its presence.
2. A \_\_\_\_\_\_\_\_\_\_ uses multiple methods of infection or propagation to maximize the speed of contagion and the severity of the attack.
3. A computer \_\_\_\_\_\_\_\_\_\_ is a piece of software that can “infect” other programs or any type of executable content and tries to replicate itself.
4. Sometimes referred to as the “infection vector”, the \_\_\_\_\_\_\_\_\_\_ is the means by which a virus spreads or propagates.
5. Sometimes known as a “logic bomb”, the \_\_\_\_\_\_\_\_\_\_ is the event or condition that determines when the payload is activated or delivered.
6. The four phases of a typical virus are: dormant phase, triggering phase, execution phase and \_\_\_\_\_\_\_\_\_\_ phase.
7. During the \_\_\_\_\_\_\_\_\_\_ phase the virus is activated to perform the function for which it was intended.
8. A \_\_\_\_\_\_\_\_\_\_ virus is explicitly designed to hide itself from detection by anti-virus software.
9. \_\_\_\_\_\_\_\_\_\_ code refers to programs that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
10. A \_\_\_\_\_\_\_\_\_\_ is when a user views a Web page controlled by the attacker that contains a code that exploits the browser bug and downloads and installs malware on the system without the user’s knowledge or consent.
11. A \_\_\_\_\_\_\_\_\_\_ is a collection of bots capable of acting in a coordinated manner.
12. A bot can use a \_\_\_\_\_\_\_\_\_\_ to capture keystrokes on the infected machine to retrieve sensitive information.
13. Countermeasures for malware are generally known as \_\_\_\_\_\_\_\_\_ mechanisms because they were first developed to specifically target virus infections.
14. Because \_\_\_\_\_\_\_\_\_\_ software can block suspicious software in real time, it has an advantage over such established anti-virus detection techniques as fingerprinting or heuristics.
15. Two types of perimeter monitoring software are \_\_\_\_\_\_\_\_\_ monitoring and egress monitoring.