# Week – Security

1. Which of the following is a software program that displays advertising on your computer?

A. Adware

B. Spyware

C. Grayware

D. Virus

2. Which of the following uses the network to duplicate its code to the hosts on a network,

often without any user intervention?

A. Adware

B. Spyware

C. Virus

D. Worm

3. Which of the following is technically a worm and is a threat that is hidden in software

that appears to do one thing, but does another?

A. Virus

B. Spyware

C. Adware

D. Trojan

4. Which of the following is a form of attack that prevents users from accessing normal

services, such as e-mail or web server?

A. Ping of death

B. Denial of service

C. E-mail bomb

D. Distributed denial of service

5. Which of the following is an encryption system that protects data as if it is on a private

network, even though the data is actually traveling over the Internet or other unsecured

public networks?

A. Data encryption

B. Port protection

C. Virtual private network

D. File system security

6. What characterizes a DDoS attack?

A. Many hosts participate in a coordinated attack.

B. It takes only a short time to set up.

C. Home computers with Internet connections are not susceptible.

D. It is easy to determine a packet’s intent.

7. Which two of the following threats are physical threats?

A. Laptops are stored in an unlocked cabinet.

B. Antivirus software has outdated virus definitions.

C. All users use the same generic username and password to connect to the network.

D. The network server and network equipment are kept in the corner of the office for

easy access.

E. The computers are secured to the desks of each user.

8. Which type of security threat installs to a computer without the user’s knowledge and

then monitors all computer activity?

A. Adware

B. Grayware

C. Malware

D. Spyware

9. Which type of security threat uses e-mail that appears to be from a legitimate sender

and asks the e-mail recipient to visit a website to enter confidential information?

A. Badware

B. Phishing

C. Stealth virus

D. Worm

10. A technician is attempting to secure a wireless network. Which two options should be

performed to secure access to the network?

A. Change the default administrator password for all access points.

B. Install a security appliance to stop all wireless traffic.

C. Enable the broadcasting of the SSID for only one access point.

D. Use MAC filtering.

. Use the default SSID values for the access points.

11. A technician has configured a wireless network with WEP encryption. Several users

who were able to use the wireless network are now unable to connect to the access

point. What is the probable cause of the connection problem?

A. WEP is a strong encryption technique that requires a successful handshake to establish

connectivity.

B. The access point cannot broadcast SSIDs when WEP is enabled.

C. The users have not configured their computers for WEP encryption.

D. The access point uses 64-bit encryption, which is obsolete with newer wireless

NICs.

12. Which step should a technician perform first when troubleshooting security issues?

A. Gather data from the computer.

B. Gather data from the customer.

C. Evaluate the problem.

D. Verify the obvious issues.

13.What type of security is biometric and door locks?

A. data security

B. login security

C. Wireless Security

D. Physical Security

14. A software or hardware that monitors and checks the information of internet and either blocks it or allows it is called:

A. Firewall

B. Antivirus

C. AntiSpyware

D. Adware

15. Which is weak wireless security?

A. EAP

B. PSK

C. WEP

D. WPA

# Answers

1. A

2. D

3. D

4. B

5. C

6. A

7. A, D

8. D

9. B

10. A, D

11. C

12. B

13.D

14.A

15.C