

Name _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 1) The three common security goals are _____. 1) _____
A) confidentiality, integrity, and availability
B) confidentiality, information, and authorization
C) confidentiality, information, and availability
D) confidentiality, integrity, and authentication
- 2) When a threat succeeds in causing harm to a business, this is a _____. 2) _____
A) breach
B) compromise
C) Both A and B
D) Neither A nor B
- 3) When a threat succeeds in causing harm to a business, this is a(n) _____. 3) _____
A) countermeasure
B) breach
C) Both A and B
D) Neither A nor B
- 4) Another name for safeguard is _____. 4) _____
A) countermeasure
B) compromise
C) Both A and B
D) Neither A nor B
- 5) Which of the following is a type of countermeasure? 5) _____
A) Corrective.
B) Detective.
C) Both A and B
D) Neither A nor B
- 6) The TJX data breach was due to _____. 6) _____
A) a single security weakness.
B) multiple security weaknesses.
C) Neither A nor B. There were no security weaknesses—only very good attackers.
- 7) If TJX had met the PCI-DSS control objectives, it would have _____ avoided the data breach. 7) _____
A) probably
B) definitely
C) definitely not
D) probably not
- 8) If TJX had met the PCI-DSS control objectives, the data breach _____ have occurred 8) _____
A) definitely would
B) probably would
C) definitely would not
D) probably would not
- 9) TJX failed to meet the _____ CIA security goal. 9) _____
A) availability
B) authorization
C) confidentiality
D) integrity
- 10) Employees are dangerous because they _____. 10) _____
A) often have access to sensitive parts of the system
B) are trusted by companies
C) Both A and B
D) Neither A nor B

- 11) What type of employee is the most dangerous when it comes to internal IT attacks? 11) _____
 A) IT professionals. B) Financial professionals.
 C) IT security professionals. D) Data entry clerks.
- 12) _____ is the destruction of hardware, software, or data. 12) _____
 A) Denial of Service B) Hacking
 C) Extortion D) Sabotage

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 13) The definition of hacking is "accessing a computer resource without authorization or in excess of authorization." 13) _____
- 14) The definition of hacking is "intentionally accessing a computer resource without authorization." 14) _____
- 15) The terms "intellectual property" and "trade secret" mean about the same thing. 15) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 16) In _____, the perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest. 16) _____
 A) hacking B) abuse C) extortion D) fraud
- 17) _____ consists of activities that violate a company's IT use policies or ethics policies. 17) _____
 A) Extortion B) Fraud C) Abuse D) Hacking
- 18) _____ is a generic term for "evil software." 18) _____
 A) Threat B) Virus C) Malware D) Worm
- 19) _____ attach themselves to other programs. 19) _____
 A) Viruses B) Worms
 C) Both A and B D) Neither A nor B
- 20) _____ can spread through e-mail attachments. 20) _____
 A) Worms B) Viruses
 C) Both A and B D) Neither A nor B
- 21) Some _____ can jump directly between computers without human intervention. 21) _____
 A) viruses B) worms
 C) Both A and B D) Neither A nor B
- 22) The fastest propagation occurs with some types of _____. 22) _____
 A) viruses B) worms C) bots D) Trojan horses
- 23) In a virus, the code that does damage is called the _____. 23) _____
 A) vector B) payload C) exploit D) compromise

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 24) Nonmobile malware can be on webpages that users download. 24) _____

- 25) A Trojan horse is a program that hides itself by deleting a system file and taking on the system file's name. 25) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 26) A program that gives the attacker remote access control of your computer is specifically called a _____. 26) _____
A) spyware program B) Trojan horse
C) cookie D) RAT
- 27) A _____ is a small program that, after installed, download a larger attack program 27) _____
A) Trojan pony B) Trojan horse C) Downloader D) Stub
- 28) Which of the following can be a type of spyware? 28) _____
A) A cookie. B) A keystroke logger.
C) Both A and B D) Neither A nor B

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 29) Most cookies are dangerous. 29) _____
- 30) In general, Trojan horses are more dangerous than rootkits. 30) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 31) Which type of program can hide itself from normal inspection and detection? 31) _____
A) Rootkit. B) Trojan horse. C) Stealth Trojan. D) Spyware.
- 32) Mobile code usually is delivered through _____. 32) _____
A) e-mail B) webpages
C) directly propagating worms D) All of the above.

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 33) Mobile code usually is contained in webpages. 33) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 34) _____ attacks take advantage of flawed human judgment by convincing the victim to take actions that are counter to security policies. (Choose the best answer) 34) _____
A) E-mail attachment B) Mobile code
C) Spam D) Social engineering

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 35) The definition of spam is "unsolicited commercial e-mail." 35) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 36) You receive an e-mail that seems to come from your bank. Clicking on a link in the message takes you to a website that seems to be your bank's website. However, the website is fake. This is _____. 36) _____
(Pick the most precise answer)
A) a hoax B) phishing
C) spear fishing D) social engineering
- 37) You receive an e-mail that seems to come from a frequent customer. It contains specific information about your relationship with the customer. Clicking on a link in the message takes you to a website that seems to be your customer's website. However, the website is fake. This is _____. 37) _____
(Pick the most precise answer)
A) social engineering B) spear fishing
C) phishing D) a hoax
- 38) Traditional external attackers were *heavily* motivated by _____. 38) _____
A) making money through crime B) the thrill of breaking in
C) Both A and B D) Neither A nor B
- 39) ICMP Echo messages are often used in _____. 39) _____
A) IP address scanning B) port scanning
C) Both A and B D) Neither A nor B
- 40) Sending packets with false IP source addresses is _____. 40) _____
A) a port scanning attack B) IP address spoofing
C) a IP address scanning attack D) None of the above.

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 41) Attackers cannot use IP address spoofing in port scanning attack packets. 41) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 42) To obtain IP addresses through reconnaissance, an attacker can use _____. 42) _____
A) IP address spoofing B) a chain of attack computers
C) Both A and B D) Neither A nor B
- 43) Following someone through a secure door without using your own ID card for access is _____. 43) _____
(Choose the most specific answer)
A) shoulder surfing B) door hacking
C) social engineering D) piggybacking
- 44) Watching someone type their password in order to learn the password is _____. 44) _____
A) piggybacking B) shoulder surfing
C) Both A and B D) Neither A nor B

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 45) In pretexting, an attacker calls claiming to be a certain person in order to ask for private information about that person. 45) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 46) A(n) _____ attack attempts to make a server or network unavailable to serve legitimate users by flooding it with attack packets. 46) _____
A) virus B) bot
C) DoS D) directly-propagating worm
- 47) A(n) _____ attack requires a victim host to prepare for many connections, using up resources until the computer can no longer serve legitimate users. (Choose the most specific choice) 47) _____
A) directly-propagating worm B) DoS
C) SYN Flooding D) distributed malware
- 48) A botmaster can remotely _____. 48) _____
A) fix a bug in the bots B) update bots with new functionality
C) Both A and B D) Neither A nor B

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 49) Botmasters usually have multiple owners over time. 49) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 50) One of the two things that characterize expert hackers is characterized _____. 50) _____
A) automated attack tools B) dogged persistence
C) Both A and B D) Neither A nor B
- 51) Sophisticated attacks often are difficult to identify amid the "noise" of many _____ attacks. 51) _____
A) virus B) script kiddie
C) distributed malware D) DoS attacks
- 52) The dominant type of attacker today is the _____. 52) _____
A) career criminal B) IT or security employer
C) national government D) wizard hacker

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 53) Compared to non-computer crime, computer crime is very small. 53) _____
- 54) Prosecuting attackers in other countries is relatively straightforward under existing computer crime laws. 54) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 55) Many e-commerce companies will not ship to certain countries because of a high rate of consumer fraud. To get around this, attackers use _____. 55) _____
A) transshippers B) IP address spoofing
C) money mules D) host name spoofing

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 56) In fraud, the attacker deceives the victim into doing something against the victim's financial self-interest. 56) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 57) To illegally receive an excess amount of money, a homepage that posts banner ads, it may resort to _____ 57) _____
A) false reporting B) extortion C) e-theft D) click fraud
- 58) _____ threaten to do at least temporary harm to the victim company's IT infrastructure unless the victim pays the attacker. 58) _____
A) Bluffers B) DoSers C) Extortionists D) Fraudsters

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 59) Identity theft is stealing credit card numbers. 59) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 60) Stealing credit card numbers is also known as _____. 60) _____
A) carding B) identity theft
C) Both A and B D) Neither A nor B

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 61) Carding is more serious than identity theft. 61) _____
- 62) Under current U.S. federal laws, if a company allows personal information to be stolen, it may be subject to government fines. 62) _____
- 63) When a company visits a website to collect public information about a competitor, this is a form of trade secret espionage. 63) _____

MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.

- 64) If a company wishes to prosecute people or companies that steal its trade secrets, it must take _____ precautions to protect those trade secrets. 64) _____
A) no (Trade secret protection is automatic under the law.)
B) reasonable
C) at least some
D) extensive
- 65) _____ may engage in commercial espionage against a firm. 65) _____
A) Competitors B) National governments
C) Both A and B D) Neither A nor B
- 66) Cyberwar is conducted by _____. 66) _____
A) terrorists B) national governments
C) Both A and B D) Neither A nor B

- 67) Countries would engage in cyberwar _____. 67) _____
A) before a physical attack B) after a physical attack
C) Both A and B D) Neither A nor B
- 68) Terrorists can use IT to _____. 68) _____
A) destroy utilities B) finance their terrorism
C) Both A and B D) Neither A nor B
- 69) If an attacker breaks into a corporate database and deletes critical files, this is a attack against the _____ security goal. 69) _____
A) integrity B) confidentiality
C) Both A and B D) Neither A nor B

TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.

- 70) You accidentally find someone's password and use it to get into a system. This is hacking. 70) _____
- 71) Someone sends you a "game." When you run it, it logs you into an IRS server. This is hacking. 71) _____
- 72) You have access to your home page on a server. By accident, you discover that if you hit a certain key, you can get into someone else's files. You spend just a few minutes looking around. This is hacking. 72) _____

Answer Key

Testname: UNTITLED1

- 1) A
- 2) C
- 3) B
- 4) A
- 5) C
- 6) B
- 7) A
- 8) D
- 9) C
- 10) C
- 11) C
- 12) D
- 13) FALSE
- 14) FALSE
- 15) FALSE
- 16) C
- 17) C
- 18) C
- 19) A
- 20) C
- 21) B
- 22) B
- 23) B
- 24) TRUE
- 25) TRUE
- 26) D
- 27) C
- 28) C
- 29) FALSE
- 30) FALSE
- 31) A
- 32) B
- 33) TRUE
- 34) D
- 35) TRUE
- 36) B
- 37) B
- 38) B
- 39) A
- 40) B
- 41) TRUE
- 42) B
- 43) D
- 44) B
- 45) TRUE
- 46) C
- 47) C
- 48) C
- 49) TRUE
- 50) B

Answer Key

Testname: UNTITLED1

- 51) B
- 52) A
- 53) FALSE
- 54) FALSE
- 55) A
- 56) TRUE
- 57) D
- 58) C
- 59) FALSE
- 60) A
- 61) FALSE
- 62) TRUE
- 63) FALSE
- 64) B
- 65) C
- 66) B
- 67) C
- 68) C
- 69) A
- 70) TRUE
- 71) FALSE
- 72) TRUE