Question 95. What is the Ping of Death?

Answer 95. Option A.
Explanation: The Ping of Death attack sends packets that, when reassembled, are too large and cause the system to crash or lock up

Question 96. How does a Denial of Service attack work?

Answer 96. Option C.
Explanation: A Denial of Service attack works by preventing legitimate users from accessing the system

Question 97. What is the goal of a Denial of Service attack?

Answer 97. Option B.
Explanation: The goal of a Denial of Service attack is to overload a system and cause it to stop responding

Question 98. Which of the following tools is only for Sun Solaris systems?

- A. Juggernaut
- B. T-Sight
- C. IP Watcher
- D. TTYWatcher

Answer 98. Option D.
Explanation: TTYWatcher is used to perform session hijacking on Sun Solaris systems.

Question 99. What is a sequence number?

- A. A number that indicates where a packet falls in the data stream
- B. A way of sending information from the sending to the receiving station
- C. A number that the hacker randomly chooses in order to hijack a session
- D. A number used in reconstructing UDP session

Answer 99. Option A.
Explanation: A sequence number indicates where the packet is located in the data steam so the receiving station can reassemble the data

Question 100. What type of information can be obtained during a session-hijacking attack? (Choose all that apply.)

- A. Passwords
- B. Credit card numbers
- C. Confidential data
- D. Authentication information

Answer 100. Options A, B, C.
Explanation: Passwords, credit card numbers, and other confidential data can be gathered in a session-hijacking attack. Authentication information isn't accessible because session hijacking occurs after the user has authenticated.

Question 101. Which of the following is essential information to a hacker performing a session-hijacking attack?

- A. Session ID
- B. Session number
- C. Sequence number
- D. Source IP address

Answer 101. Option C.
Explanation: In order to perform a session-hijacking attack, the hacker must know the sequence number to use in the next packet so the server will accept the packet

Question 102. Which of the following is a session-hijacking tool that runs on Linux operating systems?

- A. Juggernaut
- B. Hunt
- C. TTYWatcher
- D. TCP Reset Utility

Answer 102. Option A.
Explanation: Juggernaut runs on Linux operating systems.

Question 103. Which of the following is the best countermeasure to session hijacking?

Answer 103. Option B.
Explanation: Encryption make any information the hacker gathers during a session-hijacking attempt unreadable.

Question 104. Which of the following best describes sniffing?

Answer 104. Option B.
Explanation: Sniffing is usually used to locate the sequence number, which is necessary for a session hijack.

Question 105. What is session hijacking?

- A. Monitoring UDP session
- B. Monitoring TCP sessions
- C. Taking over UDP sessions
- D. Taking over TCP sessions

Answer 105. Option D.
Explanation: The most common form of session hijacking is the process of taking over a TCP session.

Question 106. What types of packets are sent to the victim of a session-hijacking attack to cause them to close their end of the connection?

- A. FIN and ACK
- B. SYN or ACK
- C. SYN and ACK
- D. FIN or RST

Answer 106. Option D.
Explanation: FIN (finish) and RST (reset) packets are sent to the victim to desynchronize their connection and cause them to close the existing connection

Question 107. What is an ISN?

- A. Initiation Session Number
- B. Initial Sequence Number
- C. Initial Session Number
- D. Indication Sequence Number

Answer 107. Option B.
Explanation: ISN is the Initial Sequence Number that is sent by the host and is the starting point for the sequence numbers used in later packets.

Question 108. Which of the following are types of HTTP web authentication? (Choose all that apply.)

- A. Digest
- B. Basic
- C. Windows
- D. Kerberos

Answer 108. Options A, B.
Explanation: Digest and basic are the types of HTTP web authentication.

Question 109. Which of the following is a countermeasure for a buffer overflow attack?

- A. Input field length validation
- B. Encryption
- C. Firewall
- D. Use of web forms

Answer 109. Option A.
Explanation: Validating the field length and performing bounds checking are countermeasures for a buffer overflow attack.

Question 110. A hardware device that displays a login that changes every 60 seconds is known as a/an _____.

- A. Login finder

- B. Authentication server
- C. Biometric authentication
- D. Token

Answer 110. Option D.
Explanation: A token is a hardware device containing a screen that displays a discrete set of numbers used for login and authentication.

Question 111. Which is a common web server vulnerability?

- A. Limited user accounts
- B. Default installation
- C. Open shares
- D. No directory access

Answer 111. Option B.
Explanation: Default installation is a common web server vulnerability.

Question 112. A password of P@SSWORD can be cracked using which type of attack?

- A. Brute force
- B. Hybrid
- C. Dictionary
- D. Zero day exploit

Answer 112. Option B.
Explanation: A hybrid attack substitutes numbers and special characters for letters.

Question 113. Which of the following is a countermeasure for authentication hijacking?

- A. Authentication logging
- B. Kerberos
- C. SSL
- D. Active Directory

Answer 113. Option C.
Explanation: SSL is a countermeasure for authentication hijacking.

Question 114. Why is a web server more commonly attacked than other systems?

- A. Always accessible
- B. Does not require much hacking ability
- C. Difficult to exploit
- D. Simple to exploit

Answer 114. Option A.
Explanation: A web server is always accessible, so a hacker can hack it more easily than less-available systems.

Question 115. A client-server program that resides on a web server is called a/an _____.

- A. Internet program
- B. Web application
- C. Patch
- D. Configuration file

Answer 115. Option B.
Explanation: Web applications are client-server programs that reside on a web server.

Question 116. Which is a countermeasure to a directory-traversal attack?

- A. Enforce permissions to folders.
- B. Allow everyone access to the default page only.
- C. Allow only registered users to access the home page of a website.
- D. Make all users log in to access folders.

Answer 116. Option A.
Explanation: A countermeasure to a directory-traversal attack is to enforce permissions to folders.

Question 117. What is it called when a hacker inserts programming commands into a web form?

- A. Form tampering
- B. Command injection
- C. Buffer overflow
- D. Web form attack

Answer 117. Option B.
Explanation: Command injection involves a hacker entering programming commands into a web form in order to get the web server to execute the commands.

Question 118. Entering Password::blah' or 1=1- into a web form in order to get a password is an example of what type of attack?

- A. Buffer overflow
- B. Heap-based overflow
- C. Stack-based overflow
- D. SQL injection

Answer 118. Option D.
Explanation: Use of a single quote indicates a SQL injection attack.

Question 119. Replacing NOPs with other code in a buffer-overflow mutation serves what purpose?

- A. Bypassing an IDS
- B. Overwriting the return pointer
- C. Advancing the return pointer
- D. Bypassing a firewall

Answer 119. Option A.
Explanation: The purpose of mutating a buffer overflow by replacing NOPs is to bypass an IDS.

Question 120. Which of the following is used to store dynamically allocated variables?

- A. Heap overflow
- B. Stack overflow
- C. Heap
- D. Stack

Answer 120. Option C.
Explanation: A heap is using to store dynamic variables.

Question 121. What is the first step in a SQL injection attack?

- A. Enter arbitrary commands at a user prompt.
- B. Locate a user input field on a web page.
- C. Locate the return pointer.
- D. Enter a series of NOPs.

Answer 121. Option B.
Explanation: The first step in a SQL injection attack is to locate a user input field on a web page using a web browser

Question 122. What command is used to retrieve information from a SQL database?

- A. INSERT
- B. GET
- C. SET
- D. SELECT

Answer 122. Option D.
Explanation: The command to retrieve information from a SQL database is SELECT.

Question 123. Which of the following is a countermeasure for buffer overflows?

- A. Not using single quotes
- B. Securing all login pages with SSL
- C. Bounds checking
- D. User validation

Answer 123. Option C.
Explanation: Performing bounds checking is a countermeasure for buffer overflow attacks.

Question 124. What does NOP stand for?

- A. No Operation
- B. Network Operation Protocol
- C. No Once Prompt
- D. Network Operation

Answer 124. Option A.
Explanation: NOP is an acronym for No Operation.

Question 125. A hacker needs to be familiar with the memory address space and techniques of buffer overflows in order to launch a buffer overflow attack.

- A. True
- B. False

Answer 125. Option B
Explanation: A hacker can run a prewritten exploit to launch a buffer overflow.

Question 126. Why are many programs vulnerable to SQL injection and buffer overflow attacks?

- A. The programs are written quickly and use poor programming techniques.
- B. These are inherent flaws in any program.
- C. The users have not applied the correct service packs.
- D. The programmers are using the wrong programming language.

Answer 126. Option A.
Explanation: Programs can be exploited because they're written quickly and poorly.

Question 127. Which command would a hacker enter in a web form field to obtain a directory listing?

- A. Blah';exec master..xp_cmdshell "dir *.*"–
- B. Blah';exec_cmdshell "dir c:*.* /s >c:\directory.txt"–
- C. Blah';exec master..xp_cmdshell "dir c:*.* /s >c:\directory.txt"–
- D. Blah';exec cmdshell "dir c:*.* "–

Answer 127. Option C.
Explanation: Blah';exec master..xp_cmdshell "dir c:*.* /s >c:\directory.txt"– is the command to obtain a directory listing utilizing SQL injection.

Question 128. What are two types of buffer overflow attacks?

Answer 128. Option A.
Explanation: Heap and stack are the two types of buffer overflows.

Question 129. Which of the following security solutions uses the same key for both encryption and authentication?

Answer 129. Option C.
Explanation: WEP uses the same key for encryption and authentication.

Question 130. WEP stands for what?Answer 130. Option B.
Explanation: WEP is an acronym for Wired Equivalent Privacy.

Question 131. What makes WEP crackable?

Answer 131. Option C.
Explanation: WEP is crackable because of the lack of sophistication in using the IV when deploying RC4.

Question 132. Which form of encryption does WPA use?

- A. AES
- B. TKIP
- C. LEAP
- D. Shared key

Answer 132. Option B.
Explanation: WPA uses TKIP.

Question 133. Which form of authentication does WPA2 use?

- A. Passphrase only
- B. 802.1x/EAP/RADIUS
- C. Passphrase or 802.1x/EAP/RADIUS
- D. AES

Answer 133. Option C.
Explanation: WPA2 uses either a passphrase in personal mode or 802.1x/EAP/RADIUS in enterprise mode

Question 134. 802.11i is most similar to which wireless security standard?

- A. WPA2
- B. WPA
- C. TKIP
- D. AES

Answer 134. A.
Explanation: 802.11i is almost the same as WPA2.

Question 135. Which of the following is a layer 3 security solution for WLANs?

- A. MAC filter
- B. WEP
- C. WPA
- D. VPN

Answer 135. Option D.
Explanation: A VPN is a layer 3 security solution for WLANs.

Question 136. A device that sends deauth frames is performing which type of attack against the WLAN?

- A. Denial of Service
- B. Cracking
- C. Sniffing
- D. MAC spoofing

Answer 136. Option A.
Explanation: A DoS can be performed by a device sending constant deauth frames.

Question 137. The most dangerous type of attack against a WLAN is _____.

- A. WEP cracking
- B. Rogue access point
- C. Eavesdropping
- D. MAC spoofing

Answer 137. Option B.
Explanation: A rogue AP is the most dangerous attack against a WLAN because it gives a hacker an open door into the network.

Question 138. 802.11i is implemented at which layer of the OSI model?

- A. Layer 1

- B. Layer 2
- C. Layer 3
- D. Layer 7

Answer 138. Option B.
Explanation: 802.11i is a layer 2 technology.

Question 139. Who is responsible for implementing physical security? (Choose all that apply.)

- A. The owner of the company
- B. Chief information officer
- C. IT managers
- D. Employees

Answer 139. Options A, B, C, D.
Explanation: The chief information officer, along with all the employees, is responsible for implementing physical security.

Question 140 What factor does impact physical security?

- A. Encryption in use on the network
- B. Flood or fire
- C. IDS implementation
- D. Configuration of firewall

Answer 140. Option B.
Explanation: A fire or flood are factors that can affect physical security while all the others are technical security issues.

Question 48. What is the process of hiding text within an image called?

- A. Steganography
- B. Encryption
- C. Spyware
- D. Keystroke logging

Answer 48. Option A.
Explanation: Steganography is the process of hiding text within an image.

Question 49. What is a rootkit?

- A. A simple tool to gain access to the root of the Windows system
- B. A Trojan that sends information to an SMB relay
- C. An invasive program that affects the system files, including the kernel and libraries
- D. A tool to perform a buffer overflow

Answer 49. Option C.
Explanation: A rootkit is a program that modifies the core of the operating system: the kernel and libraries.

Question 50. Why would hackers want to cover their tracks?

- A. To prevent another person from using the programs they have installed on a target system
- B. To prevent detection or discovery
- C. To prevent hacking attempts
- D. To keep other hackers from using their tools

Answer 50. Option B.
Explanation: Hackers cover their tracks to keep from having their identity or location discovered.

Question 51. What is privilege escalation?

- A. Creating a user account with higher privileges
- B. Creating a user account with Administrator privileges
- C. Creating two user accounts: one with high privileges and one with lower privileges
- D. Increasing privileges on a user account

Answer 51. Option D.
Explanation: Privilege escalation is a hacking method to increase privileges on a user account.

Question 52. What are two methods used to hide files? (Choose all that apply.)

- A. NTFS file streaming
- B. Attrib command
- C. Steganography
- D. Encrypted File System

Answer 52. Options A, B.
Explanation: NTFS file streaming and the attrib command are two hacking techniques to hide files.

Question 53. What is the recommended password-change interval?

- A. 30 days
- B. 20 days
- C. 1 day
- D. 7 days

Answer 53. Option A.
Explanation: Passwords should be changed every 30 days for the best balance of security and usability.

Question 54. What type of password attack would be most successful against the password T63k#s23A?

- A. Dictionary
- B. Hybrid
- C. Password guessing
- D. Brute force

Answer 54. Option D.
Explanation: A brute-force attack tries every combination of letters, numbers, and symbols.

Question 55. Which of the following is a passive online attack?

- A. Password guessing
- B. Network sniffing
- C. Brute-force attack
- D. Dictionary attack

Answer 55. Option B.
Explanation: Network sniffing is a passive online attack because it can't be detected.

Question 56. Why is it necessary to clear the event log after using the auditpol command to turn off logging?

- A. The auditpol command places an entry in the event log.
- B. The auditpol command doesn't stop logging until the event log has been cleared.
- C. auditpol relies on the event log to determine whether logging is taking place.
- D. The event log doesn't need to be cleared after running the auditpol command.

Answer 56. Option A.
Explanation: The event log must be cleared because the auditpol command places an entry in the event log indicating that login has been disabled.

Question 57. What is necessary in order to install a hardware keylogger on a target system?

- A. The IP address of the system
- B. The Administrator username and password
- C. Physical access to the system
- D. Telnet access to the system

Answer 57. Option C.
Explanation: A hardware keylogger is an adapter that connects the keyboard to the PC. A hacker needs physical access to the PC in order to plug in the hardware keylogger.

Question 58. What is a wrapper?

- A. A Trojaned system
- B. A program used to combine a Trojan and legitimate software into a single executable
- C. A program used to combine a Trojan and a backdoor into a single executable
- D. A way of accessing a Trojaned system

Answer 58. Option B.
Explanation: A wrapper is software used to combine a Trojan and legitimate software into a single executable so that the Trojan is installed during the installation of the other software.

Question 59. What is the difference between a backdoor and a Trojan?

- A. A Trojan usually provides a backdoor for a hacker.
- B. A backdoor must be installed first.
- C. A Trojan is not a way to access a system.
- D. A backdoor is provided only through a virus, not through a Trojan.

Answer 59. Option A.
Explanation: A Trojan infects a system first and usually includes a backdoor for later access.

Question 60. What port does Tini use by default?

- A. 12345
- B. 71
- C. 7777
- D. 666

Answer 60. Option C.
Explanation: Tini uses port 7777 by default.

Question 61. Which is the best Trojan and backdoor countermeasure?

- A. Scan the hard drive on network connection, and educate users not to install unknown software.
- B. Implement a network firewall.
- C. Implement personal firewall software.
- D. Educate systems administrators about the risks of using systems without firewalls.
  E. Scan the hard drive on startup.

Answer 61. Option A.
Explanation: The best prevention is to scan the hard drive for known Trojans on network connection and backdoors and to educate users not to install any unknown software.

Question 62. How do you remove a Trojan from a system?

- A. Search the Internet for freeware removal tools.
- B. Purchase commercially available tools to remove the Trojan.
- C. Reboot the system.
- D. Uninstall and reinstall all applications.

Answer 62. Option B.
Explanation: To remove a Trojan, you should use commercial tools. Many freeware tools contain Trojans.

Question 63. What is ICMP tunneling?

- A. Tunneling ICMP messages through HTTP
- B. Tunneling another protocol through ICMP
- C. An overt channel
- D. Sending ICMP commands using a different protocol

Answer 63. Option B.
Explanation: ICMP tunneling involves sending what appear to be ICMP commands but really are Trojan communications.

Question 64. What is reverse WWW shell?

- A. Connecting to a website using a tunnel
- B. A Trojan that connects from the server to the client using HTTP
- C. A Trojan that issues command to the client using HTTP
- D. Connecting through a firewall

Answer 64. Option B.
Explanation: Reverse WWW shell is a connection from a Trojan server component on the compromised system to the Trojan client on the hacker's system.

Question 65. What is a covert channel?

- A. Using a communications channel in a way that was not intended
- B. Tunneling software
- C. A Trojan removal tool
- D. Using a communications channel in the original, intended way

Answer 65. Option A.
Explanation: A covert channel is the use of a protocol or communications channel in a nontraditional way.

Question 66. What is the purpose of system-file verification?

- A. To find system files
- B. To determine whether system files have been changed or modified
- C. To find out if a backdoor has been installed
- D. To remove a Trojan

Answer 66. Option B.
Explanation: System-file verification tracks changes made to system files and ensures that a Trojan has not overwritten a critical system file.

Question 67. Which of the following is an example of a covert channel?

- A. Reverse WWW shell
- B. Firewalking
- C. SNMP enumeration
- D. Steganography

Answer 67. Option A.
Explanation: Reverse WWW shell is an example of a covert channel.

Question 68. What is the difference between a virus and a worm?

- A. A virus can infect the boot sector but a worm cannot.
- B. A worm spreads by itself but a virus must attach to an e-mail.
- C. A worm spreads by itself but a virus must attach to another program.
- D. A virus is written in C++ but a worm is written in shell code.

Answer 68. Option C.
Explanation: A worm can replicate itself automatically but a virus must attach to another program.

Question 69. What type of virus modifies itself to avoid detection?

- A. Stealth virus
- B. Polymorphic virus
- C. Multipartite virus
- D. Armored virus

Answer 69. Option B.
Explanation: A polymorphic virus modifies itself to evade detection.

Question 70. Which virus spreads through Word macros?

- A. Melissa
- B. Slammer
- C. Sobig
- D. Blaster

Answer 70. Option A.
Explanation: Melissa is a virus that spreads via Word Macros.

Question 71. Which worm affects SQL servers?

- A. Sobig
- B. SQL Blaster
- C. SQL Slammer
- D. Melissa

Answer 71. Option C.
Explanation: SQL Slammer is a worm that attacks SQL servers.

Question 72. Armored viruses are _____.

Answer 72. Option C.
Explanation: Armored viruses are encrypted.

Question 73. What are the three methods used to detect a virus?

Answer 73. Options A, B, C.
Explanation: Scanning, integrity checking, and virus signature comparison are three ways to detect a virus infection.

Question 74. What components of a system do viruses infect?

Answer 74. Options A, B, E.
Explanation: A virus can affect files, system sectors, and DLL files.

Question 75. All anomalous behavior can be attributed to a virus.

- A. True
- B. False

Answer 75. Option B.
Explanation: Not all anomalous behavior can be attributed to a virus.

Question 76. A virus that can cause multiple infections is know as what type of virus?

Answer 76. Option A.
Explanation: A multipartite virus can cause multiple infections.

Question 77. A way to evade an antivirus program is to do what?

Answer 77. Option A.
Explanation: A custom virus script can be used to evade detection because the script will not match a virus signature.

Question 78. What is sniffing?

Answer 78. Option B.
Explanation: Sniffing is the process of capturing and analyzing data on a network.

Question 79. What is a countermeasure to passive sniffing?

Answer 79. Option A.
Explanation: By implementing a switched network, passive sniffing attacks are prevented.

Question 80. What type of device connects systems on a shared network?

Answer 80. Option C.
Explanation: A network connected via hubs is called a shared network.

Question 81. Which of the following is a countermeasure to ARP spoofing?

Answer 81. Option A.
Explanation: Port-based security implemented on a switch prevents ARP spoofing.

Question 82. What is dsniff?

Answer 82. Option C.
Explanation: Dsniff is a group of hacking tools.

Question 83. At what layer of the OSI model is data formatted into packets?

Answer 83. Option C.
Explanation: Packets are created and used to carry data at layer 3.

Question 84. What is snort?

Answer 84. Option A.
Explanation: Snort is both an intrusion detection system (IDS) and a sniffer.

Question 85. What mode must a network card operate in to perform sniffing?

Answer 85. Option D.
Explanation: A network card must operate in promiscuous mode in order to capture traffic destined to a different MAC address than its own.

Question 86. The best defense against any type of sniffing is _____

Answer 86. Option A.
Explanation: Encryption renders the information captured in a sniffer useless to a hacker.

Question 87. For what type of traffic can winsniffer capture passwords? (Choose all that apply.)

Answer 87. Options A, B, C.
Explanation: Winsniffer can capture passwords for POP3, SMTP, and HTTP traffi

Question 88. Which is a method to prevent Denial of Service attacks?

Answer 88. Option B.
Explanation: Traffic filtering is a method to prevent DoS attacks.

Question 89. What is a zombie?

Answer 89. Option A.
Explanation: A zombie is a compromised system used to launch a DDoS attack.

Question 90. The Trinoo tool uses what protocol to perform a DoS attack?

Answer 90. Option C.
Explanation: Trinoo uses UDP to flood the target system with data.

Question 91. What is the first phase of a DDoS attack?

- A. Intrusion
- B. Attack
- C. DoS
- D. Finding a target system

Answer 91. Option A.

Question 1. Which of the following statements best describes a white-hat hacker?

- A. Security professional
- B. Former black hat
- C. Former grey hat
- D. Malicious hacker

Answer 1. Option A.
Explanation: A white-hat hacker is a “good” guy who uses his skills for defensive purposes.

Question 2. A security audit performed on the internal network of an organization by the network administration is also known as _____.

- A. Grey-box testing
- B. Black-box testing
- C. White-box testing
- D. Active testing
- E. Passive testing

Answer 2. Option C.
Explanation: White-box testing is a security audit performed with internal knowledge of the systems

Question 3. What is the first phase of hacking?

- A. Attack
- B. Maintaining access
- C. Gaining access
- D. Reconnaissance
- E. Scanning

Answer 3. Option D.
Explanation: Reconnaissance is gathering information necessary to perform the attack

Question 4. What type of ethical hack tests access to the physical infrastructure?

- A. Internal network
- B. Remote network
- C. External network
- D. Physical access

Answer 4. Option D.
Explanation: Physical access tests access to the physical infrastructure.

Question 5. The security, functionality, and ease of use triangle illustrates which concept?

- A. As security increases, functionality and ease of use increase.
- B. As security decreases, functionality and ease of use increase.
- C. As security decreases, functionality and ease of use decrease.

- D. Security does not affect functionality and ease of use.

Answer 5. Option B.
Explanation: As security increases it makes it more difficult to use and less functional

Question 6. Which type of hacker represents the highest risk to your network?

- A. Disgruntled employees
- B. Black-hat hackers
- C. Grey-hat hackers
- D. Script kiddies

Answer 6. Option A.
Explanation: Disgruntled employees have information which can allow them to launch a powerful attack.

Question 7. What are the three phases of a security evaluation plan? (Choose three answers.)

- A. Conduct Security Evaluation
- B. Preparation
- C. Conclusion
- D. Final
- E. Reconnaissance
- F. Design Security
- G. Vulnerability Assessment

Answer 7. Options A, B, C.
Explanation: The three phases of a security evaluation plan are preparation, conduct security evaluation, and conclusion.

Question 8. Hacking for a cause is called _____.

- A. Active hacking
- B. Hacktivism
- C. Activism
- D. Black-hat hacking

Answer 8. Option B.
Explanation: Hacktivism is performed by individual who claim to be hacking for a political or social cause.

Question 9. Which federal law is most commonly used to prosecute hackers?

- A. Title 12
- B. Title 18
- C. Title 20
- D. Title 2

Answer 9. Option B.
Explanation: Title 18 of the U.S. Code of law is most commonly used to prosecute hackers

Question 10. When a hacker attempts to attack a host via the Internet it is known as what type of attack?

- A. Remote attack
- B. Physical access
- C. Local access
- D. Internal attack

Answer 10. Option A.
Explanation: An attack from the Internet is known as a remote attack.

Question 11. Which are the four regional Internet registries?

- A. APNIC, PICNIC, NANIC, RIPE NCC
- B. APNIC, MOSTNIC, ARIN, RIPE NCC
- C. APNIC, PICNIC, NANIC, ARIN

- D. APNIC, LACNIC, ARIN, RIPE NCC

Answer 11. Option D.
Explanation: The four Internet registries are ARIN (American Registry of Internet Numbers), RIPE NCC (Europe, the Middle East, and parts of Central Asia), LACNIC (Latin American and Caribbean Internet Addresses Registry), and APNIC (Asia Pacific Network Information Centre).

Question 12. Which of the following is a tool for performing footprinting undetected?

- A. Whois search
- B. Traceroute
- C. Ping sweep
- D. Host scanning

Answer 12. Option A.
Explanation: Whois is the only tool listed that won't trigger an IDS alert or otherwise be detected by an organization.

Question 13. Which of the following tools are used for footprinting? (Choose 3 answers.)

- A. Whois
- B. Sam Spade
- C. NMAP
- D. SuperScan
- E. Nslookup

Answer 13. Options A, B, E.
Explanation: Whois, Sam Spade, and nslookup are all used to passively gather information about a target. NMAP and SuperScan are host and network scanning tools.

Question 14. What is the next step to be performed after footprinting?

- A. Scanning
- B. Enumeration
- C. System hacking
- D. Active information gathering

Answer 14. Option A.
Explanation: According to CEH methodology, scanning occurs after footprinting.

Question 15. Which are good sources of information about a company or its employees? (Choose all that apply.)

- A. Newsgroups
- B. Job postings
- C. Company website
- D. Press releases

Answer 15. Options A, B, C, D.
Explanation: Newsgroups, job postings, company websites, and press releases are all good sources for information gathering.

Question 16. How does traceroute work?

- A. It uses an ICMP destination-unreachable message to elicit the name of a router.
- B. It sends a specially crafted IP packet to a router to locate the number of hops from the sender to the destination network.
- C. It uses a protocol that will be rejected by the gateway to determine the location.
- D. It uses the TTL value in an ICMP message to determine the number of hops from the sender to the router.

Answer 16. Option D.
Explanation: Traceroute uses the TTL values to determine how many hops the router is from the sender. Each router decrements the TTL by one under normal conditions.

Question 17. What is footprinting?

- A. Measuring the shoe size of an ethical hacker
- B. Accumulation of data by gathering information on a target
- C. Scanning a target network to detect operating system types
- D. Mapping the physical layout of a target's network

Answer 17. Option B.
Explanation: Footprinting is gathering information about a target organization.

Question 18. Nslookup can be used to gather information regarding which of the following?

- A. Host names and IP addresses
- B. Whois information
- C. DNS server locations
- D. Name server types and operating systems

Answer 18. Option A.
Explanation: Nslookup queries a DNS server for DNS records such as host names and IP addresses.

Question 19. Which of the following is a type of social engineering?

- A. Shoulder surfing
- B. User identification
- C. System monitoring
- D. Face-to-face communication

Answer 19. Option A.
Explanation: Of the choices listed here, shoulder surfing is considered a type of social engineering.

Question 20. Which is an example of social engineering?

- A. A user who holds open the front door of an office for a potential hacker
- B. Calling a help desk and convincing them to reset a password for a user account
- C. Installing a hardware keylogger on a victim's system to capture passwords
- D. Accessing a database with a cracked password

Answer 20. Option B.
Explanation: Calling a help desk and convincing them to reset a password for a user account is an example of social engineering.

Question 21. What is the best way to prevent a social-engineering attack?

- A. Installing a firewall to prevent port scans
- B. Configuring an IDS to detect intrusion attempts
- C. Increasing the number of help-desk personnel
- D. Employee training and education

Answer 21. Option D.
Explanation: Employee training and education is the best way to prevent a social-engineering attack.

Question 22. Which of the following is the best example of reverse social engineering?

- A. A hacker pretends to be a person of authority in order to get a user to give them information.
- B. A help-desk employee pretends to be a person of authority.
- C. A hacker tries to get a user to change their password.
- D. A user changes their password.

Answer 22. Option A.
Explanation: When a hacker pretends to be a person of authority in order to get a user to ask them for information, it's an example of reverse social engineering.

Question 23. Using pop-up windows to get a user to give out information is which type of social engineering attack?

- A. Human-based
- B. Computer-based
- C. Nontechnical
- D. Coercive

Answer 23. Option B.
Explanation: Pop-up windows are a method of getting information from a user utilizing a computer.

Question 24. What is it called when a hacker pretends to be a valid user on the system?

- A. Impersonation
- B. Third-person authorization
- C. Help desk
- D. Valid user

Answer 24. Option A.
Explanation: Impersonation involves a hacker pretending to be a valid user on the system.

Question 25. What is the best reason to implement a security policy?

- A. It increases security.
- B. It makes security harder to enforce.
- C. It removes the employee's responsibility to make judgments.
- D. It decreases security.

Answer 25. Option C.
Explanation: Security policies remove the employee's responsibility to make judgments regarding a potential social-engineering attack.

Question 26. Faking a website for the purpose of getting a user's password and username is which type of social engineering attack?

- A. Human-based
- B. Computer-based
- C. Web-based
- D. User-based

Answer 26. Option B.
Explanation: Website faking is a form of computer-based social engineering attack.

Question 27. Dumpster diving can be considered which type of social engineering attack?

- A. Human-based
- B. Computer-based
- C. Physical access
- D. Paper-based

Answer 27. Option A.
Explanation: Dumpster diving is a human-based social engineering attack.

Question 28. What port number does FTP use?

- A. 21
- B. 25
- C. 23
- D. 80

Answer 28. Option A.
Explanation: FTP uses TCP port 21. This is a well-known port number and can be found in the Windows services file.

Question 29. What port number does HTTPS use?

- A. 443
- B. 80
- C. 53
- D. 21

Answer 29. Option A.
Explanation: HTTPS uses TCP port 443. This is a well-known port number and can be found in the Windows services file.

Question 30. What is war dialing used for?

- A. Testing firewall security
- B. Testing remote access system security

- C. Configuring a proxy filtering gateway
- D. Configuring a firewall

Answer 30. Option B.
Explanation: War dialing involves placing calls to a series of numbers in hopes that a modem will **Answer the call. It can be used to test the security of a remote-access system.**

Question 31. Banner grabbing is an example of what?

- A. Passive operating system fingerprinting
- B. Active operating system fingerprinting
- C. Footprinting
- D. Application analysis

Answer 31. Option A.
Explanation: Banner grabbing is not detectible; therefore it is considered passive OS fingerprinting.

Question 32. What are the three types of scanning?

- A. Port, network, and vulnerability
- B. Port, network, and services
- C. Grey, black, and white hat
- D. Server, client, and network

Answer 32. Option A.
Explanation: Port, network, and vulnerability are the three types of scanning.

Question 33. What is the main problem with using only ICMP queries for scanning?

- A. The port is not always available.
- B. The protocol is unreliable.
- C. Systems may not respond because of a firewall.
- D. Systems may not have the service running.

Answer 33. Option C.
Explanation: Systems may not respond to ICMP because they have firewall software installed that blocks the responses.

Question 34. What does the TCP RST command do?

- A. Starts a TCP connection
- B. Restores the connection to a previous state
- C. Finishes a TCP connections
- D. Resets the TCP connection

Answer 34. D.
Explanation: The TCP RST command resets the TCP connection.

Question 35. What is the proper sequence of a TCP connection?

- A. SYN-SYN ACK-ACK
- B. SYN-ACK-FIN
- C. SYN-SYNACK-ACK
- D. SYN-PSH-ACK

Answer 35. Option A.
Explanation: A SYN packet is followed by a SYN-ACK packet. Then, an ACK finishes a successful TCP connection.

Question 36. A packet with all flags set is which type of scan?

- A. Full Open
- B. Syn scan
- C. XMAS
- D. TCP connect

Answer 36. Option C.
Explanation: An XMAS scan has all flags set.

Question 37. What is the proper command to perform and NMAP SYN scan every 5 minutes?

- A. nmap -ss – paranoid
- B. nmap -Ss -paranoid
- C. nmap -Ss -fast
- D. namp -Ss -sneaky

Answer 37. Option B.
Explanation: The command nmap -Ss – paranoid performs a SYN scan every 300 seconds or 5 minutes.

Question 38. In order to prevent a hacker from using SMB session hijacking, which TCP and UDP ports would you block at the firewall?

- A. 167 and 137
- B. 80 and 23
- C. 139 and 445
- D. 1277 and 1270

Answer 38. Option C.
Explanation: Block the ports used by NetBIOS null sessions. These are 139 and 445.

Question 39. Why would an attacker want to perform a scan on port 137?

- A. To locate the FTP service on the target host
- B. To check for file and print sharing on Windows systems
- C. To discover proxy servers on a network
- D. To discover a target system with the NetBIOS null session vulnerability

Answer 39. Option D.
Explanation: Port 137 is used for NetBIOS null sessions.

Question 40. SNMP is a protocol used to manage network infrastructure devices. What is the SNMP read/write community name used for?

- A. Viewing the configuration information
- B. Changing the configuration information
- C. Monitoring the device for errors
- D. Controlling the SNMP management station

Answer 40. Option B.
Explanation: The SNMP read/write community name is the password used to make changes to the device configuration.

Question 41. Why would the network security team be concerned about ports 135–139 being open on a system?

- A. SMB is enabled, and the system is susceptible to null sessions.
- B. SMB is not enabled, and the system is susceptible to null sessions.
- C. Windows RPC is enabled, and the system is susceptible to Windows DCOM remote sessions.
- D. Windows RPC is not enabled, and the system is susceptible to Windows DCOM remote sessions.

Answer 41. Option A.
Explanation: Ports in the 135 to 139 range indicate the system has SMB services running and is susceptible to null sessions.

Question 42. Which step comes after enumerating users in the CEH hacking cycle?

- A. Crack password
- B. Escalate privileges
- C. Scanning
- D. Covering tracks

Answer 42. Option A.
Explanation: Password cracking is the next step in the CEH hacking cycle after enumerating users.

Question 43. What is enumeration?

- A. Identifying active systems on the network
- B. Cracking passwords
- C. Identifying users and machine names
- D. Identifying routers and firewalls

Answer 43. Option C.
Explanation: Enumeration is the process of finding usernames, machine names, network shares, and services on the network.

Question 44. What is a command-line tool used to look up a username from a SID?

- A. UsertoSID
- B. Userenum
- C. SID2User
- D. Getacct

Answer 44. Option C.
Explanation: SID2User is a command-line tool to find a username from a SID.

Question 45. Which tool can be used to perform a DNS zone transfer on Windows?

- A. nslookup
- B. DNSlookup
- C. whois
- D. ipconfig

Answer 45. Option A.
Explanation: nslookup is a Windows tool that can be used to initiate a DNS zone transfer that sends all the DNS records to a hacker's system.

Question 46. What is a null session?

- A. Connecting to a system with the administrator username and password
- B. Connecting to a system with the admin username and password
- C. Connecting to a system with a random username and password
- D. Connecting to a system with no username and password

Answer 46. Option D.
Explanation: A null session involves connecting to a system with no username and password.

Question 47. What is a countermeasure for SNMP enumeration?

- A. Remove the SNMP agent from the device.
- B. Shut down ports 135 and 139 at the firewall.
- C. Shut down ports 80 and 443 at the firewall.
- D. Enable SNMP read-only security on the agent device.

Answer 47. Option A.

Question 142. Which of the following is often one of the most overlooked areas of security?

- A. Operational
- B. Technical
- C. Internet
- D. Physical

Answer 142. Option D.
Explanation: Physical security is one of the most overlooked areas of security.

Question 143. A hacker who plants a rogue wireless access point on a network in order to sniff the traffic on the wired network from outside the building is causing what type of security breach?

- A. Physical
- B. Technical
- C. Operational
- D. Remote access

Answer 143. Option A.
Explanation: In order to place a wireless access point, a hacker needs to have physical access.

Question 144. Which area of security usually receives the least amount of attention during a penetration test?

- A. Technical
- B. Physical
- C. Operational
- D. Wireless

Answer 144. Option B.
Explanation: Physical security usually receives the least amount of testing during a penetration test.

Question 145. Which of the following attacks can be perpetrated by a hacker against an organization with weak physical security controls?

- A. Denial of service
- B. Radio frequency jamming
- C. Hardware keylogger
- D. Banner grabbing

Answer 145. Option C.
Explanation: A hardware keylogger can be installed to capture passwords or other confidential data once a hacker gains physical access to a client system.

Question 146. Which type of access allows passwords stored on a local system to be cracked?

- A. Physical
- B. Technical
- C. Remote
- D. Dial-in

Answer 146. Option A.
Explanation: Physical access allows a hacker to crack passwords on a local system.

Question 147. Which of the following is an example of a physical security breach?

- A. Capturing a credit card number from a web server application
- B. Hacking a SQL server in order to locate a credit card number
- C. Stealing a laptop to acquire credit card numbers
- D. Sniffing a credit card number from packets sent on a wireless hotspot

Answer 147. Option C.
Explanation: Theft of equipment is an example of a physical security breach.

Question 148. What type of attack can be performed once a hacker has physical access?

- A. Finding passwords by dumpster diving
- B. Stealing equipment

- C. Performing a DoS attack
- D. Session hijacking

Answer 148. Option B.
Explanation: Stealing equipment requires physical access.

Question 149. What does LKM stand for?

- A. Linux Kernel Module
- B. Linux Kernel Mode
- C. Linked Kernel Module
- D. Last Kernel Mode

Answer 149. Option A.
Explanation: LKM stands for Linux Kernel Module.

Question 150. What GCC command is used to compile a C++ file called source into an executable file called game ?

- A. g++ source.c –o game
- B. gcc source.c –o game
- C. gcc make source.cpp –o game
- D. g++ source.cpp –o game

Answer 150. Option D.
Explanation: g++ source.cpp –o game is the GCC command to create an executable called game from the source file source.

Question 151. What is the command to deny all users access from the network?

- A. Cat “All:All”>> /etc/hosts.deny
- B. Set “All:All”>> /etc/hosts.deny
- C. IP deny “All:All”
- D. Cat All:All deny

Answer 151. Option A.
Explanation: Cat “All:All” /etc/hosts.deny is the command to deny all users access from the network on a Linux system.

Question 152. Of the following, which are common commercial Linux distributions?

- A. SUSE, Knark, and Red Hat
- B. SUSE, Adore, Debian, and Mandrake
- C. SUSE, Debian, and Red Hat
- D. SUSE, Adore, and Red Hat

Answer 152. Option C.
Explanation: SUSE, Debian, and Red Hat are all commercial versions of Linux.

Question 153. What is a Linux live CD?

- A. A Linux operating system that runs from CD
- B. A Linux operating system installed from a CD onto a hard drive
- C. A Linux tool that runs applications from a CD
- D. A Linux application that makes CDs

Answer 153. Option A.
Explanation: A Linux live CD is a fully functioning operating system that runs from a CD.

Question 154. What type of attack can be disguised as an LKM?

- A. DoS
- B. Trojan
- C. Spam virus
- D. Rootkit

Answer 154. Option D.
Explanation: A rootkit can be disguised as an LKM.

Question 155. Which of the following is a reason to use Linux?

- A. Linux has no security holes.
- B. Linux is always up to date on security patches.
- C. No rootkits can infect a Linux system.
- D. Linux is flexible and can be modified.

Answer 155. Option D.
Explanation: Linux is flexible and can be modified because the source code is openly available.

Question 156. Which of the following is not a way to harden Linux?

- A. Physically secure the system.
- B. Maintain a current patch level.
- C. Change the default passwords.
- D. Install all available services.

Answer 156. Option D.
Explanation: Linux should not have unused services running, because each additional service may have potential vulnerabilities.

Question 157. What type of file is used to create a Linux live CD?

- A. ISO
- B. CD
- C. LIN
- D. CDFS

Answer 157. Option A.
Explanation: An ISO file is used to create a Linux live CD.

Question 158. Why is it important to use a known good distribution of Linux?

- A. Source files can become corrupt if not downloaded properly.
- B. Only certain distributions can be patched.
- C. Source files can be modified, and a Trojan or backdoor may be included in the source binaries of some less-known or free distributions of Linux.
- D. Only some versions of Linux are available to the public.

Answer 158. Option C.
Explanation: Known good distributions have been reviewed by the Linux community to verify that a Trojan or backdoor does not exist in the source code.

Question 159. A system that performs attack recognition and alerting for a network is what?

- A. HIDS
- B. NIDS
- C. Anomaly detection HIDS
- D. Signature-based NIDS

Answer 159. Option B.
Explanation: A NIDS performs attack recognition for an entire network.

Question 160. Which of the following tools bypasses a firewall by sending one byte at a time in the IP header?

Answer 160. Option C.
Explanation: Covert_TCP passes through a firewall by sending one byte at a time of a file in the IP header.

Question 161. Which of the following is a honeypot-detection tool?

Answer 161. Option D.
Explanation: Sobek is a honeypot-detection tool.

Question 162. Which of the following is a system designed to attract and identify hackers?

Answer 162. Option A.
Explanation: A honeypot is a system designed to attract and identify hackers.

Question 163. Which of the following is a tool used to modify an attack script to bypass an IDS's signature detection?

Answer 163. Option A.
Explanation: ADMutate is a tool used to modify an attack script to bypass an IDS's signature detection.

Question 164. What is a reverse WWW shell?

Answer 164. Option B.
Explanation: A reverse WWW shell occurs when a compromised web client makes a connection back to a hacker's computer and is able to pass through a firewall.

Question 165. A reverse WWW shell connects to which port on a hacker's system?

Answer 165. Option A.
Explanation: The hacker's system, which is acting as a web server, uses port 80.

Question 166. What is the command to install and run Snort?

Answer 166. Option A.
Explanation: snort –l c:\snort\log –c C:\snort\etc\snoft.conf –A console is the command to install and run the Snort program.

Question 167. What type of program is Snort?

Answer 167. Option B.
Explanation: Snort is a sniffer, HIDS, and traffic-logging tool

Question 168. What are the ways in which an IDS is able to detect intrusion attempts? (Choose all that apply.)

Answer 168. Options B, C.
Explanation: Signature analysis and anomaly detection are the ways an IDS detects instruction attempts.

Question 169. How many keys exist is in a public/private key pair?

Answer 169. Option B.
Explanation: Two keys, a public key and a private key, exist in a key pair.

Question 170. How many keys are needed for symmetric key encryption?

Answer 170. Option A.
Explanation: The same key is used to encrypt and decrypt the data with symmetric key encryption.

Question 171. Which of the following key lengths would be considered uncrackable? (Choose all that apply.)

Answer 171. Options A, B.
Explanation: A key length of 256 bits or more is considered uncrackable.

Question 172. What algorithm outputs a 128-bit message digest regardless of the length of the input?

Answer 172. Option B.
Explanation: MD5 outputs a 128-bit digest with variable-length input.

Question 173. What algorithm outputs a 160-bit key with variable-length input?

Answer 173. Option A.
Explanation: SHA outputs a 160-bit key with variable-length input.

Question 174. Which algorithm is used in the digital signature process?

Answer 174. Option D.
Explanation: MD5 is used in the digital signature process.

Question 175. What is cryptography?

Answer 175. Option C.
Explanation: Cryptography is the study of encryption.

Question 176. What is the process of replacing some characters with others in an encryption key?

Answer 176. Option C.
Explanation: Substitution is the process of replacing some characters with others.

Question 177. Data encrypted with the server's public key can be decrypted with which key?

Answer 177. Option B.
Explanation: Data can be decrypted with the other key in the pair—in this case, the server's private key.

Question 178. Which type of encryption is the fastest to use for large amounts of data?

Answer 178. Option A.
Explanation: Symmetric key encryption is fast and best to use for large amounts of data.

Question 179. What is the purpose of a pen test?

Answer 179. Option C.
Explanation: A penetration test is designed to test the overall security posture of an organization and to see if it responds according to the security policies.

Question 180. Security assessment categories include which of the following? (Choose all that apply.)

Answer 180. Options B, C, D.
Explanation: Security assessments can be security audits, vulnerability assessments, or penetration testing.

Question 181. What type of testing is the best option for an organization that can benefit from the experience of a security professional?

Answer 181. Option C.
Explanation: Manual testing is best, because knowledgeable security professionals can plan, test designs, and do diligent documentation to capture test results.

Question 182. Which type of audit tests the security implementation and access controls in an organization?

Answer 182. Option B.
Explanation: A penetration test produces a report of findings on the security posture of an organization.

Question 183. What is the objective of ethical hacking from the hacker's prospective?

Answer 183. Option A.
Explanation: An ethical hacker is trying to determine the security posture of the organization.

Question 184. What is the first step of a pen test?

Answer 184. Option C.
Explanation: The first step of a pen test should always be to have the client sign a scope of work, NDA, and liability release document.

Question 185. Which tools are not essential in a pen tester's toolbox?

- A. Password crackers
- B. Port scanning tools
- C. Vulnerability scanning tools
- D. Web testing tools
- E. Database assessment tools
- F. None of the above

Answer 185. Option F.
Explanation: All these tools must be used to discover vulnerabilities in an effective security assessment.

Question 186. What are not the results to be expected from a pre-attack passive reconnaissance phase? (Choose all that apply.)

Answer 186. Options D, F.
Explanation: Acquiring the target and executing, implanting, and retracting are part of the active reconnaissance pre-attack phase.

Question 187. Once the target has been acquired, what is the next step for a company that wants to confirm the vulnerability was exploited? (Choose all that apply.)

Answer 187. Options A, D.
Explanation: The next step after target acquisition is to use tools that will exploit a vulnerability and leave a mark or execute a command on a vulnerable system to communicate to another system on the network and leave a mark.

Question 188. An assessment report for management may include suggested fixes or corrective measures.

Answer 188. Option A.
Explanation: An assessment may include corrective suggestions to fix the vulnerability.