1. Which statement defines session hijacking most accurately? Session hijacking is an attack that aims at stealing a legitimate session and posing as that user while communicating with the web resource or host machine.
2. Jennifer has been working with sniffing and session hijacking toolson her company network. Since she wants to stay white hat - that is ethical - she has gotten permission to undertake these activities. What would Jennifer's activites be categorized as? Passive
3. Based on the diagram, what attack is occurring? MITM
4. Jennifer is a junior system administrator for a small firm of 50 employees. For the lst week a few users have been complaining of losing connectivity intermittently with no suspect behavior on their part such as large downloads or intensive processes. Jennifer runs wireshark on Monday morning to investigate. She sees a large amout of ARP broadcasts being sent at a fairly constant rate. What is Jennifer most likely seeing? ARP Poisoning
5. Which of the following is not a source of session IDs? Anonymous Login
6. Which kind of values is injected into a connection to the host machine in an effort to increment the sequence number in a predictable fashion? Null
7. An ethical hacker sends a packet with a deliberate and specific path to its destination. What technique is the hacker using? Source routing
8. Network level hijacking focuses on the mechanics of a connection such as the manipulation of packet sequencing. What is the main focus of web app session hijacking? Stealing session IDs
9. A public use workstation contains the browsing history of multiple users who logged in during the lsat seven days. While digging through the history, a user runs across the following web address: www.snaz22enu.com/&w25/session=22525. What kind of embedding are you seeing? URL embedding
10. Julie has sniffed an ample amount of traffic between the targeted victim and an authenticated resource. She has been able to correctly guess the packet sequence numbers and inject packets, but she is unable to receive any of the responses. What does this scenario define? Blind hijacking
11. Session hijacking can be performed on all of the following protocols except which one? IPsec
12. Which technology can provide protection against session hijacking? IPsec
13. Session fixation is a vulnerability in which of the following? Web Applications
14. Session hijacking can be thwarted with which of the following? Authentication
15. XSS is typically targeted toward which of the following? Web Browsers
16. A man-in-the-browser attack is typically enabled by using which mechanism? Trojans
17. A man-in-the-middle attack is an attack where the attacking party does which of the following? Insert themselves into an active session
18. A session hijack can happen with which of the following? Network and Applications
19. A session hijack can be initiated from all of the following except which one? Cookies and devices
20. Session hijacking can do all of the following except which one? Place a cookie on a server
21. In order to perform network sniffing, the network card needs to be put in which mode? Promiscuous mode
22. In order to perform network sniffing across "all" virtual networks on a switch, what type of port needs to be created on the switch? SPAN/mirror port
23. Which protocols below can be sniffed and "read" without additional processing/analyzing? IP POP SMTP
24. When Computer A asks the network, "Who has this IP address?" is an example of what? ARP Request
25. When Computer B tells Computer A, "I have that MAC. My IP address is [what it is]" is an example of what? ARP Reply
26. When an attacker computer tells a network the IP address of bigbank.com is an illigitimate address, that is a form of what attack? DNS poisoning
27. A MITM attack depends on which of the following successful attacks to be completed first? ARP/DNS poisoning
28. A sender starts with an innocuous image but adjusts ever 100th pixel to correspond to a letter in the alphabet is an example of what? Steganography
29. Which statement(s) defines malware most accurately?
30. Which is/are a characteristic of a virus?
31. A virus does NOT do which of the following? Display Pop ups
32. Which of the following is/are true of a worm? Replicates on its own
33. What are worms typically known for? Rapid replication
34. What command is used to listen to open ports with netstat? Netstat -an
35. Which utility will tell you in real time which ports are listening or in another state? TCPview
36. Which of the following is NOT a trojan? TCPTROJAN
37. What is NOT a benefit of hardware keyloggers? Difficult to install.
38. Which of the following is capable of port redirection? netcat
39. A Trojan relies on \_\_\_\_\_\_ to be activated. Social engineering
40. A Trojan can include which of the following? RAT
41. What is a covert channel? backdoor
42. An overt channel is \_\_\_\_\_\_\_ Obvious method of using a system
43. A covert channel or backdoor may be detected using all of the following except \_\_\_\_\_\_\_\_\_ An SDK
44. A remote access Trojan would be used to do all of the following except \_\_\_\_\_ Sniff traffic
45. A logic bomb has how many parts, typically? Two
46. A logic bomb is activated by which of the following? Time and Date, actions and events
47. A polymorphic virus \_\_\_\_\_\_\_ Evades detection by rewriting itself
48. A sparse infector virus \_\_\_\_\_\_\_ Infects files selectively
49. Malware is code that has an adverse impact on which of the following? CIA
50. Malicious code triggered by user action is an example of what? Virus
51. What phase of a virus is when it is replicating itself? Propagation phase
52. What phase of a virus is when it performs its malicious action or payload? Action phase
53. When a logical condition causes a virus to move from a dormant or propagation phase is which phase? Trigerring phase
54. A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself is a? worm
55. Conficker is an example of which malware? worm
56. Which malware is named after ancient Greek history? trojan
57. What malware modified an operating system to hide the existence of itself or other malware? Root kit
58. What form of malware can track browsing or buying habits? adware
59. What form of malware can track user data such as keystrokes or screen capture? spyware
60. A bot, which is part of a botnet is also known as what? zombie
61. Antivirus uses which of the following methods for detection? Signature scanning
62. Signature based antivirus has which advantage over Heuristics based antivirus?
63. Heuristics based antivirus has which advantage over signature based antivirus?
64. After each infection, a virus modifies a portion of its code before propagating is an example of what? Polymorphism
65. The three basic event categories in the Windows XP Event Viewer are? Application, system, security
66. In linux, which file contains authentication logs? /var/log/auth.log
67. In linux, which file contains general information and system related stuff? /var/log/message
68. What "Log Collection System" also analyzes log files in real time? SIEM
69. Which tool within Burp would you use to decode or encode web request data? Burp decoder
70. Which tool within Burp would you use to rewrite HTML? Burp proxy
71. Which of the following is an example of an URI? Htm.html#one
72. What tool would you use to "hook" a victim who happens to browse to your malicious website? BEEF
73. What is the current standard for web security and has replaced SSL, but is often used interchangably? TLS
74. Burp has which of the following components as part of its suite?
75. An HTTP Response contains which of the following?
76. An HTTP response code of 500 means? Internal server error
77. An HTTP response code of 200 means? OK
78. An HTTP Request contains which of the following?
79. After confirming certificate validity and that it has not expired, what is the next step in setting up an SSL Web session? Generate symmetric key
80. A pure web server has which characteristics?
81. A hybrid web server has which characteristics?
82. What is SQL Injection?
83. A website forum that has user posted comments might be vulnerable to which type of Cross Site Scripting attack? Persistent XSS
84. Which of the following is an example of a rogue access point? Any acc pnt within org
85. Which of the following best describes a web application?
86. \_\_\_\_\_\_ is a client-side scripting language. Javascript
87. Which of the following is an example of a server-side scripting language? PHP
88. Which of the following is used to access content outside the root of a website? Directory traversals
89. Which of the following can prevent bad input from being presented to an application through a form? Input validation
90. \_\_\_\_\_\_ can be used to identify a web server. Banner grab
91. In the field of IT security, the concept of defense in depth is layering more than one control on another. Why would this be helful in the defense of a system of session-hijacking? To provide better protection
92. Which of the following is used to set permissions on content in a website? ACL
93. What could be used to monitor application errors and violations on a web server or application? Logs
94. Which of the following is an attribute used to secure a cookie?
95. A POODLE attack targets what exactly? ssl
96. What is used to store session information? A cookie
97. Which attack can be used to take over a previous session? Session hijacking
98. Which command would retrieve banner information from a website at port 80? Nc 192.168.10.27 80
99. How is a brute-force attack performed?
100. What is the command to retrieve header information from a web server using telnet? telnet <website name> 80
101. Groups and individuals who may hack a web server or web applications based on principle or personal beliefs are known as \_\_\_\_\_\_? Hacktivists
102. The Wayback Machine would be useful in viewing what type of information relating to a web application? Archived versions of websites
103. What may be helpful in protecting the content on a web server from being viewed by unauthorized personnel? Encryption
104. A common attack against web servers and web applications is \_\_\_\_\_? Buffer overflow
105. Input validation is used to prevent which of the following? Sql injection
106. Web application are used to \_\_\_\_\_?
107. Which of the following challenges can be solved by firewalls? Protection against scanning
108. Databases can be a victim of code exploits depending on which of the following? configuration
109. In addition to relational databased, there is also what kind of database? hierarchical
110. Which of the following is a scripting language? cgi
111. \_\_\_\_ is used to audit databased? SQLping
112. Browsers do not display \_\_\_\_\_\_? Hidden fields
113. Proper input validation can prevent what from occuring? Sql injection attacks
114. \_\_\_\_\_\_ can be used to attack databased? Sql injection
115. Which command can be used to access the command prompt in SQL Server? Xp\_cmdshell
116. Which command is used to query data in SQL Server? select
117. Which statement is used to limit data in SQL Server? where
118. Which command is used to remove a table from a database? Drop tables
119. SQL injection attacks are aimed at which of the following? databases
120. Which of the following is another name for a record in a database? Row
121. What type of database has its information pread across many disparate systems? distributed
122. What type of database used multiple tables linked together in complex relationships? relational
123. What can an error message tell an attacker? All
124. A blind SQL injection attack is used when which of the following is true? Error messages are not available
125. WEP is designed to offer security comparable to which of the following? Wired networks
126. Which of the following operates at 5GHz? 802.11a
127. Which of the following specifies security standards for wireless? 802.11i
128. Which of the following options shows the protocols in order from strongest to weakest? WPA2, WPA, WEP, open
129. Which of the following is designed to locate wireless access points? Site survey
130. What is a client-to-client connection called? Ad hoc
131. When a wireless client is attached to an access point, it is known as which of the following? infrastructure
132. Bluesnarfing is used to perform what type of attack? Read information from a device
133. Monitor mode is used by wireless cards to do what? Capture info about wireless networks
134. A honeyspot is designed to do what? Attract victims to connect to it
135. An SSID is used to do which of the following? Identify a network
136. AirPcap is used to do which of the following? Assist in sniffing of wireless traffic
137. What is a rogue access point? Access point not managed by a company
138. Bluejacking is a means of which of the following? Sending unsolicited messages
139. The wardriving process involves which of the following? Locating wireless networks
140. Warchalking is used to do which of the following? Make others aware of a wireless network
141. A closed network is typically which of the following? Private networks
142. Which feature makes WPA easy to defeat? WPS support
143. What is a PSK? A key entered into each client
144. Which of the following is a device used to perform a DoS on a wireless network? Wifi jammer
145. 802.11 was developed by IEEE in? 1997
146. 802.11b was released second and operates in the 2.4GHz range 1999
147. Which of the following tools could you use to crack a wireless network's pre-shared key? Aircrack-ng
148. What can be used along with WPA to improve security? VPN
149. Phishing takes place using \_\_\_\_\_\_\_email
150. Training and educations of end users can be used to prevent \_\_\_\_\_\_\_\_\_phishing
151. Social engineering can be thwarted using what kinds of controls? Technical, admin, physical
152. Social engineering preys on many weaknesses, including \_\_\_\_\_\_\_
153. Social engineering can use all of the following except \_\_\_\_\_\_\_\_viruses
154. Social engineering is designed to \_\_\_\_\_\_\_\_manipulate
155. Phishing can be mitigated through the use of \_\_\_\_\_\_spam filtering
156. Which mechanism can be used to influence a targeted individual? Means of dress or appearance
157. Jennifer receives an email claiming that her bank account information has been lost and that she needs to click a link to update the bank's database. However, she doesn't recognize the bank, because it is not one she does business with. What type of attack is she being presented with? phishing
158. What is the best option for thwarting social-engineering attacks? training
159. Janet receives an email enticing her to click a link. But when she click this link she is taken to a website for her bank, asking her to reset her acconut info. However, Janet noticed that the bank is not hers and the website is not for her bank. What type of attack is this? Phishing
160. Jason receives notices that he has unauthorized charges on his credit card account. What type of attack is Jason a victim of? Identity theft
161. A security camera picks up someone who doesn't work at the company following closely behind an employee while they enter the building. What type of attack is taking place? tailgating
162. What is a vulnerability scan designed to provide to those executing it? Way to reveal vulns
163. In social engineering a proxy is used to\_\_\_\_\_\_keep attacker’s origin hidden
164. Social engineering can be used to carry out email campaigns known as \_\_\_\_\_\_Phishing
165. Human beings tend to follow set patterns and behaviors known as \_\_\_\_\_\_habits
166. When talking to a victim, using \_\_\_\_\_\_ can make an attack easier. keywords
167. An attacker can use which technique to influence a victim? Name dropping
168. Jason notices that he is receiving mail, phone calls, and other requests for information. He has also noticed some problems with his credit checks such as bad debts and loans he did not participate in. What type of attack did Jason become a victim of? Identity theft
169. Physical security can prevent which of the following? tailgating
170. Which of the following is a detective control when not used in real time? alarm
171. For a fence to deter a determined intruder, it should be at least how many feet tall? 8 feet
172. A \_\_\_\_\_\_\_ is used to prevent cars from ramming a building. bollards
173. While gueards and dogs are both good for physical security, which of the following is a concen with dogs? liability
174. Which of the following is a good defense against tailgating and piggybacking? mantraps
175. Which of the following is a wall that is less than full height? False wall
176. In the field of IT security, the concept of defense in depth is the layering of more than one control on another. Why is this? To provide better protection
177. Which intrusion prevention system can be used in conjunction with fences? bollards
178. Frequency of type 2 errors is also known as what? False rejection rates
179. Which type of biometric system is frequently found on laptops buy can be used on entry ways as well? fingerprint
180. Which of the following could be considered required components of an alarm systems? A visual and audio alerting systems
181. Lock-pick sets typically contain which of the following at a minimum? A pick and a tension wrench
182. During an assessment you discovered that the target company was using a fax machine. Which of the following is the least important? The phone is publicly avbailable
183. What is a drop ceiling? A false ceiling
184. What is another word for portals? Mantraps
185. What is a type of combination lock? Cipher lock
186. What is the first defense that a physical intruder typically encounters? Fences
187. What mechanism is intended to deter theft of hard drives? Encryption
188. Which of the following is a characteristic of USB flash drives that makes security a problem? Easily hidden
189. An anomaly detection IDS relies on a database of known attacks? Pattern matching systems
190. Which of the following is not a common Snort keyword? -ack, -flags, -id, -ttl, -msg
191. Which of the following is not a method of identifiying a firewall? Port scanning, banner grabbing
192. A symmetric encryption algorithm uses different keys for encryption and decryption? False
193. Which of the following uses a symmetric algorithm? HMAC, AES, DES, Blowfish
194. Which of the following uses an asymmetric algorithm? RSA, Diffie helman, elliptical curve
195. A hashing algorithm producing the same hash value for two or more files is called? collision
196. Which of the following is not a component of public key infrastructure?
197. Which fire suppression system class is required for protecting server rooms full of computing equipment? Class C fire extinguisher