CIS4204 Ethnical hacking final exam

Study online at https://quizlet.com/_7oxzdu

1.	**1. Which statement(s) defines malware most accurately?**	B. Trojans are malware. C. Malware covers all malicious software
2.	**2. Which is/are a characteristic of a virus?**	A. A virus is malware C. A virus replicates with user interaction.
3.	**3. A virus does not do which of the following?**	D. Display pop-ups
4.	**4. Which of the following is/are true of a worm?**	A. A worm is malware. B. A worm replicates on its own.
5.	**5. What are worms typically known for?**	A. Rapid replication
6.	**6. What command is used to listen to open ports with netstat?**	A. netstat -an
7.	**7. Which utility will tell you in real time which ports are listening or in another state?**	B. TCPView
8.	**8. Which of the following is not a Trojan**	D. TCPTROJAN
9.	**9. What is not a benefit of hardware keyloggers?**	B. Difficult to install
10.	**10. Which of the following is capable of port redirection?**	C. Netcat
11.	**11. A Trojan relies on to be activated**	C. Social engineering
12.	**12. A Trojan can include which of the following?**	A. RAT

13.	**13. What is a covert channel?**	C. A backdoor
14.	**14. An overt channel is**	A. An obvious method of using a system
15.	**15. A covert channel or backdoor may be detected using all of the following except**	C. An SDK
16.	**16. A remote access Trojan would be used to do all of the following except**	C. Sniff traffic
17.	**17. A logic bomb has how many parts, typically?**	B. Two
18.	**18. A logic bomb is activated by which of the following?**	A. Time and date C. Actions D. Events
19.	**19. A polymorphic virus.**	C. Evades detection through rewriting itself
20.	**20. A sparse infector virus.**	C. Infects files selectively
21.	**21. On a switch, each switchport represents a**	D. Collision domain
22.	**22. Wireless access points function as a.**	B. Bridge
23.	**23. What mode must be configured to allow an NIC to capture all traffic on the wire?**	D. Promiscuous mode
24.	**24. Which of the following prevents ARP poisoning?**	B. IP DHCP Snooping
25.	**25. Jennifer is a system administrator who is researching a technology that will secure network traffic from potential sniffing by unauthorized machines. Jennifer is not concerned with the**	C. SSH

	future impact on legitimate troubleshooting. What technology can Jennifer implement?	
26.	**26. MAC spoofing applies a legitimate MAC address to an unauthenticated host, which allows the attacker to pose as a valid user. Based on your understanding of ARP, what would indicate a bogus client?**	C. A reverse ARP request maps to two hosts.
27.	**27. Bob is attempting to sniff a wired network in his first pen test contract. He sees only traffic from the segment he is connected to. What can Bob do to gather all switch traffic?**	A. MAC flooding
28.	**28. What technique funnels all traffic back to a single client, allowing sniffing from all connected hosts?**	B. ARP poisoning
29.	**29. Which Wireshark filter displays only traffic from 192.168.1.1?**	C. ip.addr == 192.168.1.1
30.	**30. What common tool can be used for launching an ARP poisoning attack?**	A. Cain & Abel
31.	**31. Which command launches a CLI version of Wireshark?**	C. tshark
32.	**32. Jennifer is using tcpdump to capture traffic on her network. She would like to save the capture for later review. What command can Jennifer use?**	D. tcpdump -w capture.log
33.	**33. What is the generic syntax of a Wireshark filter?**	A. protocol.field operator value
34.	**34. Tiffany is analyzing a capture from a client's network. She is particularly interested in NetBIOS traffic. What port does Tiffany filter for?**	B. 139
35.	**Jennifer is using tcpdump to capture traffic on her network. She would like to review a capture log gathered previously. What command can Jennifer use?**	A. tcpdump -r capture.log

36.	**Wireshark requires a network card to be able to enter which mode to sniff all network traffic?**	B. Promiscuous mode
37.	**37. Which network device can block sniffing to a single network collision domain, create VLANs, and make use of SPAN ports and port mirroring?**	B. Switch
38.	**38. What device will neither limit the flow of traffic nor have an impact on the effectiveness of sniffing?**	A. Hub
39.	**39. The command-line equivalent of WinDump is known as what?**	B. Tcpdump
40.	**40. Phishing takes place using.**	B. Email
41.	**41. Training and education of end users can be used to prevent.**	A. Phishing B. Tailgating/piggybacking
42.	**42. Social engineering can be thwarted using what kinds of controls?**	A. Technical B. Administrative C. Physical
43.	**43. Social engineering preys on many weaknesses, including**	B. People C. Human nature D. Physical
44.	**44. Social engineering can use all the following except .**	D. Viruses
45.	**45. Social engineering is designed to**	A. Manipulate human behavior
46.	**46. Phishing can be mitigated through the use of .**	A. Spam filtering B. Education
47.	**47. Which mechanism can be used to influence a targeted individual?**	A. Means of dress or appearance
48.		A. Phishing

	48. 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?	
49.	**49. What is the best option for thwarting social-engineering attacks?**	B. Training
50.	**50. Janet receives an email enticing her to click a link. But when she clicks this link she is taken to a website for her bank, asking her to reset her account info. However, Janet noticed that the bank is not hers and the website is not for her bank. What type of attack is this?**	C. Phishing
51.	**51. Jason receives notices that he has unauthorized charges on his credit card account. What type of attack is Jason a victim of?**	C. Identity theft
52.	**52. 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?**	D. Tailgating
53.	**53. What is a vulnerability scan designed to provide to those executing it?**	D. A way to reveal vulnerabilities
54.	**54. In social engineering a proxy is used to.**	C. Keep an attacker's origin hidden
55.	**55. Social engineering can be used to carry out email campaigns known as.**	B. Phishing
56.	**56. Human beings tend to follow set patterns and behaviors known as.**	B. Habits
57.	**57. When talking to a victim, using can make an attack easier**	B. Keywords

58.	**58. An attacker can use which technique to influence a victim?**	C. Name-dropping
59.	**60. 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?**	C. Identity theft
60.	**61. Which of the following best describes a web application?**	B. Code designed to be run on the server
61.	**62. is a client side scripting language.**	A. JavaScript
62.	**63. Which of the following is an example of a server - side scripting language? A. JavaScript**	B. PHP
63.	**64. Which of the following is used to access content outside the root of a website?**	D. Directory traversal
64.	**65. Which of the following can prevent bad input from being presented to an application through a form?**	B. Input validation
65.	**66. can be used to identify a web server.**	B. Banner grab
66.	**67. In the field of IT security, the concept of defense in depth is layering more than one control on another. Why would this be helpful in the defense of a system of session hijacking?**	A. To provide better protection
67.	**68. Which of the following is used to set permissions on content in a website?**	C. ACL
68.	**69. What could be used to monitor application errors and violations on a web server or application?**	D. Logs
69.	**70. Which of the following is an attribute used to secure a cookie?**	

		B. Secure C. HttpOnly D. Domain
70.	**71. A POODLE attack targets what exactly?**	? A. SSL
71.	**72. What is used to store session information?**	A. Cookie
72.	**73. Which attack can be used to take over a previous session?**	B. Session hijacking
73.	**74. Which command would retrieve banner information from a website at port 80?**	A. nc 192.168.10.27 80
74.	**75. How is a brute force attack performed?**	A. By trying all possible combinations of characters
75.	**76. What is the command to retrieve header information from a web server using Telnet?**	A. telnet 80
76.	**77. Groups and individuals who may hack a web server or web application based on principle or personal beliefs are known as.**	D. Hacktivists
77.	**78. The Wayback Machine would be useful in viewing what type of information relating to a web application?**	C. Archived versions of websites
78.	**79. What may be helpful in protecting the content on a web server from being viewed by unauthorized personnel?**	A. Encryption
79.	**80. A common attack against web servers and web applications is .**	D. Buffer overflow