CIS4204 Final

Study online at https://quizlet.com/_7mf53w

1.	**Which of these is not a fundamental security property:** **a) Privacy** **b) Confidentiality** **c) Availability**	A
2.	**Which of these is a significant concern when discussing the scope of a penetration test:** **a) Scope creep** **b) Contact info for all individuals carrying out the engagement** **c) Social engineering pretexts**	A
3.	**In what situation might you need to consult cloud service provide amazon.com about accessing their computers:** **a) On any pen test I perform** **b) When you are performing a pen test for a company that uses their cloud services** **c) Never, unless Amazon is a customer hiring me for my services**	B
4.	**Which of these terms is not defined in the Florida Computer Crimes Act:** **a) Computer** **b) Authorization** **c) Access**	B
5.	**Which of these provides individuals in the European Union with control over their data:** **a) The General Data Protection Regulation** **b) The Council of Europe Convention 185 on Cybercrime** **c) The Luhn Algorithm**	A

6. **Which of these is a linux shell built-in command:** B

a) ls
b) cd
c) grep

7. **What work is likely based, in part, on Johny Long's "Google Hacking for Penetration Testers":** B

a) The Pen Test Execution Standard
b) Untangling the Web: A Guide to Internet Research
c) The Recon-ng web reconnaissance framework

8. **What is the Microsoft DREAD model used to quantify:** A

a) Information Security Risk
b) Incident response time
c) Cost of recovering from a vulnerability

9. **What key element of James Comey's comments about his instagram account at the National Security Alliance Dinner led to Ashley Feinberg identifying his twitter account:** C

a) He said he followed his son, Brien Comey.
b) He mentioned that his advisor from William and Mary, Reinhold Niebuhr, followed him.
c) He said he had about nine followers, all relatives or close friends.

10. **Which of these could be the netmask for the network with IP address 255.255.64.0:** A

a) 255.255.192.0
b) 255.255.0.0
c) 255.255.128.0

11. **What does a dig request for record type AXFR achieve:** A

a) Zone transfer.
b) Transfer of an Address record.
c) Nothing, you totally made that up.

12. **What kind of dns lookup does fierce use in order to get a name server that won't provide zone transfer to reveal a host name that's not in the fierce wordlist:** A

a) Reverse lookup.
b) Zone transfer.
c) None. There's no way to do this.

13. **Which of these is not a layer in the OSI networking model?** C

a) Physical
b) Presentation
c) Protocol

14. **If, in starting a TCP connection, host X sends a SYN packet to host Y with sequence number A, what will be true of a correct response by host Y?** B

a) It will have ACK (but not SYN) set and the sequence number will be A+1.
b) It will have SYN and ACK set and the sequence number will be chosen randomly.
c) It will have SYN and ACK set and the acknowledgment number will be randomly chosen.

15. **What is the number of bits in TCP port?** B

a) 8
b) 16
c) 32

16. **What is done to the TTL field of each successive group of 3 IP packets sent by traceroute to identify those hosts routing packets between two machines** C

on the internet?

a) It is decremented by 1.
b) Nothing. It remains the same.
c) It is incremented by 1.

17. **What is contained in the data of an ICMP type 11 packet?** B

a) there is no data associated with this control message.
b) The original packet that caused this response to be generated.
c) An application-specific data payload.

18. **What do the last 3 octets of a MAC address identify?** B

a) The vendor who manufactured this device.
b) The specific device ID.
c) The network address.

19. **How does nmap determine that a port is closed?** C

a) It gets no response to a SYN packet.
b) It gets a FIN response to a SYN packet.
c) It gets a RST response to a SYN packet.

20. **If you don't specify what ports nmap is to scan, how does it decide?** B

a) No defaults are provided. This question is moot.
b) It uses the ports that are most often interrogated.
c) It randomly selects ports.

21. **How does Masscan achieve better performance than nmap?** A

a) It uses a custom TCP stack.
b) It uses GPUs.
c) It uses cyclic multiplicative groups.

22. **Which of these is not a service that is used to support OpenVas?** B

a) openvas manager service
b) openvas reporting service
c) openvas scanning service

23. **Which of these must you use rather than set in order to get remote code execution on a target host with Metasploit?** B

a) An option
b) An exploit
c) A payload

24. **What would you not do with OpenVas if you have an exhaustive list of all machines to be tested?** A

a) Perform discovery.
b) Use the ultimate scanning feature.
c) Limit the number of ports scanned.

25. **Which of these malware artifacts did not use the vulnerability identified in MS08-067?** C

a) Conficker
b) Stuxnet
c) Eternal Blue

26. **If I see a file with permissions rwsr-xr-x, which of these statements is true?** C

a) It has the sticky bit set.
b) It is not executable by the owner.
c) It is a set-user executable file.

27. **Which of these statements is true?** B

a) If we use symmetric encryption, then sharing the

password file is completely secure.
b) Salting password hashes helps obscure the use of identical passwords.
c) Using a salt but not recording it would make unix password hashes more secure and usable.

28. **Which of these is true about the RockYou password breach?** B

a) This breach occurred in 2016.
b) The passwords were stored in plain text.
c) 64 Million passwords were exfiltrated.

29. **Which of these is most likely to keep a penetration tester from being able to guess passwords through SMB on a particular machine?** C

a) Make sure the host uses hashed passwords.
b) Closing ports 135, 139, 445, and 3389 with a fire-wall that limits traffic entering the network for that machine.
c) Closing ports 139 and 445 with the machine's local firewall.

30. **What did I report as the most common length for a password in the H ave I Been Pwned password list?** B

a) 5
b) 9
c) 12

31. **The Zack Attack can also be described as an** C

a) attack on Kerberos.
b) NTLM reflective attack.
c) NTLM relay attack.

32. **If you want to generate a stealthy attack which of these would you prefer to use?** A

a) ncat connector from victim host to attack host on port 80
b) ncat listener on victim host port 80
c) ncat listener on victim host port 4444

33. **What is special about the hex string 0xAAD3B435B51404EE?** C

a) It is the hash assigned to the local administrator on every Windows system.
b) It is the hash assigned to the default Windows administrator account password.
c) It is the hash assigned to an empty last 7 bytes of an LM hash.

34. **What can you do to insure that your hashed password will not be stored in the Security Accounts Manager (SAM) file?** C

a) Use Windows 8.1 or Windows Server 2012 or newer.
b) Set the "Short Passwords Allowed" GPO to false.
c) Choose a password longer than 14 characters.

35. **Which type of encryption must be enforced in order to get a server long term key?** C

a) MD4
b) kerberos
c) RC4

36. **Which of these was not a vulnerability of LDAP(S) session signing?** B

a) The "MIC is Set" bit was checked but not the MIC itself.
b) The relayer could use its NetBIOS computer name in relayed messages.
c) A blank NetBIOS computer name could be passed in requests.

37. **Where was the AES-encrypted Microsoft Local Administrator password stored for distribution (until some time after 2014)?**

    a) In the SYSVOL directory on the domain controller.
    b) In the Security Accounts Manager (SAM) local file.
    c) Nowhere. RC4 encryption was used for this password.

    A

38. **What account executes sethc.exe when 5 successive shit key press event occur before login?**

    a) The current user.
    b) NT AUTHORITY/System.
    c) The local Administrator account (UID 500).

    B

39. **What method of Local Administrator credentials does Microsoft now suggest one use?**

    a) Creation of Individual Local Administrator Accounts
    b) Local Administrator Password Solution (LAPS)
    c) Global Group Policy Preference Assignment

    B

40. **Which of these detection methods requires a malware artifact to have been previously encountered in order for anti-virus to function properly?**

    a) Signature
    b) Behavioral
    c) Heuristic

    A

41. **Which of these is the worst potential reasonable outcome of sharing part of your filesystem in an rdesktop connection.**

    a) You cannot get local access to your own filesystem when it is remotely mounted.
    b) You may experience network delay when referencing back to your own filesystem.

    C

c) A process on the remote machine can modify your filesystem in unexpected ways.

42. **Why might it be preferable to use a powershell payload rather than a native .exe file payload?** A

a) The powershell payload need never be stored in the filesystem.
b) A machine might execute powershell, but not native code.
c) Powershell runs much faster than native code.

43. **How are reflected XSS attacks typically delivered to a victim:** A

a) Through a URL provided in a phishing attack
b) In a metasploit payload
c) Using RFC 1145-compliant carriers

44. **What javascript file is typically used to hook a browser using BeEF:** C

a) beef.js
b) beefhook.js
c) hook.js

45. **What kind of cookies should be used in order to protect their contents from being used in a cross-site request forgery attack:** B

a) HSTS supercookies
b) HttpOnly cookies
c) Base-64 encoded cookies

46. **Which hacker zine published "Smashing the Stack for Fun and Profit":** B

a) 2600
b) Phrack
c) 4chan

47. **What register normally stores the frame pointer on an Intel X64 machine:** A

a) %rbp
b) %rsp
c) %eip

48. **What does CFI stand for:** B

a) Common File Interface
b) Control Flow Integrity
c) Causal Function Invocation

49. **How can an attacker exploit the following unquoted service path: C:\Program Files\Printer Software\EpsonDriver.exe** A

a) By doing what either of the other two answers says
b) By storing Printer.exe in "C:\Program Files"
c) By storing Program.exe in C:

50. **Which of these will not help you dump logon passwords in mimikatz:** C

a) Enabling debug privilege
b) Using the sekurlsa::logonPasswords function
c) Using a non-networked console connection

51. **Where does the sekurlsa::logonpasswords function get it's information:** C

a) From the SAM password database
b) From the Windows registry
c) From the LSASS memory

52. **According the ECPA, is a base-64 encoded message readily accessible:** C

a) No

B) Yes
c) It's not completely clear because some terms are not defined in the Act

53. **What is the mandatory civil fine for a second violation of the ECPA:** C

a) $1,000
b) $250
c) $500

54. **According to the Electronic Communications Privacy Act (ECPA), is a VoIP transmission (from one person to another over the internet) an oral communication:** A

a) No
b) Yes

55. **Who created SSLStrip:** C

a) Dug Song
b) John McAfee
c) Moxie Marlinspike

56. **Where does the SSLStrip iptables rule send packets destined for port 80:** C

a) To port 443 on the destination host
b) To port 80 on the destination host
c) To the sslstrip.py executable.

57. **Which of these is not true about carrying a successful stealthy arpspoof campaign?** A

a) We must be running a web server on port 80.
b) We must be able to perform IP forwarding.
c) We must have access to the affected hosts on a single layer 2 network.

58. B

Which of the following is true of HSTS super-cookies?

a) Once stored by a compliant browser, they never expire.
b) They cannot be removed from a compliant browser by using any browser function available to the user.
c) They are a server technology that requires no special browser support.

59. **What is the most interesting difference between Socks4a and Socks5 proxies?** C

a) Socks4a proxies require user authentication, a requirement removed by Socks5.
b) Socks4a is available as a metasploit module but Socks5 is not.
c) Socks4a provides TCP but not UDP while Socks5 provides both.

60. **What does the command "net LocalGroup Administrators hax0r /add" do?** A

a) Adds user hax0r to the Administrators group.
b) Adds user Administrators to the LocalGroup group with password hax0r.
c) Adds user LocalGroup to the group Administrators with password hax0r.

61. **What service is consulted by many Windows machines when DNS fails to yield a response for a host lookup?** B

a) WPAD
b) LLMNR
c) PAC

62. **What is the underlying vulnerability exploited by Eternal Blue?** C

a) Type confusion.
b) An integer overflow.
c) A buffer overflow.

63. **Why did Linus Torvalds' remove the patch that addressed the problem underlying Dirty Cow in around 2007?** C

a) Russian hacker group Fancy Bear paid him to leave it vulnerable.
b) It didn't actually resolve the problem.
c) It caused problems for IBM S390 machines.

64. **Which of these encodings is used for HTTP Basic Authentication?** A

a) Base-64
b) AES
c) Blowfish

65. **Which of these files is used by IIS to provide information to web applications?** B

a) boot.ini
b) global.asa
c) htaccess

66. **Which web server uses the htaccess file to control authentication** B

a) IIS
b) apache
c) Demonoid

67. **Which of these is an accurate statement?** B

a) Javascript can effectively block inputs to a web form that contain blacklisted elements.
b) Javascript can effectively verify that inputs to a web form satisfy blacklisting rules.

c) Javascript can effectively filter out malicious inputs to a web form.

68. **Which of these approaches can effectively reduce opportunities for SQL injection?** C

a) Use session tokens with low entropy so they are hard to guess or generate.
b) Make sure to patch web server software to the most recent version so that injection is less likely to be exploitable.
c) Use prepared statements that pass parameters of a query separately from the query string.

69. **Which of these statements is true of digest authentication?** C

a) This technique uses Windows user credentials to authenticate a user using AD or NTLM.
b) This is a method that requires the user to implement custom code in a web form.
c) An MITM attack can downgrade Digest Auth to Basic Auth to capture hashed password information.

70. **Which of these things is robots.txt designed to do?** A

a) Tell web spiders what parts of a web site to ignore.
b) Tell web spiders what parts of a web site to search.
c) Provide configuration information for specified web spiders.

71. **Which of these is true of sqlmap?** C

a) It supports a very limited set of back-end databases.
b) It cannot do blind sql injections without a script file.
c) It does not inject POST parameters without a template.

72. **What can CRLF injection be used to achieve?** C

a) Covertly passing unicode characters using ascii strings.
b) Covertly passing extra get parameters to a web server.
c) Covertly passing headers to a web server through parameters.

73. **Which wifi channels are not designated for civilian use in the U.S.?** A

a) 12 through 14.
b) All channels can be legally used by civilians in the U.S.
c) 13 and 14.

74. **Which of these is not a reason that ARP packets are replayed in the FMS attack?** C

a) ARP packets are easy to identify because of their packet length.
b) Every reply to a replayed ARP request will likely have the same plain text.
c) The ARP destination address is the access point's MAC.

75. **Which of these is true of a WPA2 password cracking attack?** C

a) The attack requires multiple deauthentications of a station, to replay the handshake numerous times.
b) The attack ties to decrypt the Pairwise Transient Key.
c) The attack involves using a dictionary to verify the Pairwise Master Key.

76. **Which of these is true of EAP wireless connections?** C

a) Use of EAP eliminates the possibility of password

guessing.
b) Client devices will always validate a RADUIS server's CA authenticity.
c) The four-way handshake is carried out with unencrypted communications.

77. **Which of these methods is not true of an attack on WPA2/EAP with RADIUS-WPE?** C

a) Deauth floods may be used to capture handshakes.
b) One can capture encrypted credentials when a station connects for the first time.
c) Only a single EAP type will be used by any client when connecting.

78. **Which of these is true of KRACK Attack?** A

a) The MITM must not use the Access Point's channel.
b) The method has been available with a proof of concept since 2014.
c) Unpatched Linux versions are harder to attack than BSD.

79. **Which of these is the key vulnerability exploited in the Reaver attack?** C

a) The use of a known hash for the PMK makes it possible to employ a dictionary attack.
b) Successive deauth packets can be sent during WPS setup causing replay of the handshake.
c) The algorithm for verifying the PIN makes brute forcing efficient.

80. **Which of these is true of a Kismet wardriving expedition?** C

a) There is little benefit to using a tool like Kismet in a wireless penetration test.
b) Kismet makes it easy to mount an evil-twin attack.

c) One benefit of using Kismet is that is completely undetectable.

81. **How did your instructor use Scapy to get wireless devices to attempt connections to an access point?** A

a) Sent fake beacons corresponding to the 10,000 most common SSIDs.
b) Sent fake probes corresponding to the 10,000 most common SSIDs.
c) Sent multiple deauth packets to get devices to replay their handshakes.

82. **Which of these wireless standards is most likely to be used both now and in the future?** A

a) LTE
b) CDMA
c) GSM

83. **Which of these is not true of SS7?** C

a) German hackers abused it to rob bank accounts.
b) Using just a phone number, one can reroute U.S. calls for a given number.
c) It was developed in the late 1990s to route international cell phone calls.

84. **Which of these is true of the Stingray IMSI catcher device that law enforcement agencies through the U.S. employ.** B

a) The device can be configured so it can only detect IMSIs associated with specific people.
b) The FBI claims its use of the device is supported by the Electronic Communications Privacy Act.
c) Courts nationwide have determined that law enforcement agencies must provide detailed information about any IMSI-catcher devices they use.

85. **Which of these is not an effective approach to protect a machine against malicious file system modification after boot from a removable device?**

a) Always log out and turn off your machine.
b) Encrypt your file system.
c) Make sure there is a BIOS password and the boot order does not include removable devices.

A

86. **Which of these devices was demonstrated in class by your instructor as a way to deliver an exploit to an unsuspecting user with a USB HID device?**

a) The Packet Squirrel.
b) The Bash Bunny.
c) The USB Rubber Ducky.

C

87. **Which of these devices was demonstrated in class by your instructor as a way to mount a responder attack via USB on a (possibly screen-locked) machine.**

a) The Bash Bunny.
b) The USB Rubber Ducky.
c) The Packet Squirrel.

A

88. **What virtual machine is used to evaluate Android .apk files?**

a) Dalvik.
b) Android.
c) Valdik.

A

89. **What is the Android vulnerability in which a disagreement in the order of checking vs. loading PK file elements can lead to execution of malicious elements.**

a) Stagefright.
b) Master Key Vulnerability.
c) Dirty Cow.

B

90. **What does the Drammer Android exploit attack?** B

a) Wifi chips.
b) Memory cells.
c) A double-free in the heap.

91. **What operating system was the original iOS operating system based on?** B

a) Linux.
b) NeXTSTEP.
c) OS 360.

92. **What software-independent jailbreak (based on axi0mX's exploit) was just released by Pangu?** B

a) Qwertyurioup.
b) Checkra1n.
c) Electra.

93. **Why are there no third party vulnerability scanners that will dynamically test the security of iOS apps?** C

a) There's no need to do this because the Apple app verification process guarantees security.
b) The app store has a policy forbidding such apps.
c) One app cannot access another on iOS.

94. **Which of these is not an action one can take on an S3 bucket?** C

a) LIST
b) DELETE
c) MODIFY

95. **Which of these AWS web services controls access to resources?** A

a) IAM

b) ACL
c) WD30

96. **Which of these is a non-relational database service?** A

a) DynamoDB
b) MySQL
c) Aurora

97. **Which kind of testing requires expert knowledge of the language and frameworks?** A

a) Manual code review.
b) Automated static analysis.
c) Use of a dynamic analysis sandbox.

98. **Which level of the Mobile Application Security Verification Standard is appropriate for apps that employ sensitive data?** A

a) MASVS-L2.
b) MASVS-R.
c) MASVS-L1.

99. **Which of these is not a resilience requirement,** C

a) Executable files and libraries of the app are encrypted or packed.
b) The app either terminates or warns the user when run in a jailbroken/rooted device.
c) Debugging code has been removed from the app.

100. **What UDP port does the TPLink LB-120 light bulb use for communication?** A

a) 9999
b) 99
c) 8080

101. A

What method did Thomas Wilson use to capture non-broadcast packets traveling between the controlling app and the light bulb.

a) Tcpdump from a rooted phone.
b) Tcpdump from wifi on a laptop.
c) Tcpdump from a proxy device.

102. **How many bytes (at most) will a person have to brute force in order to decode an autocipher encoded text?** C

a) You can't brute force and autocipher encoded text.
b) 65,535.
c) 1.