CEH (v8) Practice Exam (With Key)

1. A person who uses hacking skills for defensive purposes is called a:
A. Hacktivist
B. Grey hat hacker
C. Black hat hacker
D. White hat hacker

Answer: D

2. What is the preparatory phase of hacking called?
A. Scanning
B. Reconnaissance
C. Enumeration
D. Footprinting

Answer: B

3. Which of the following is a weakness in a system, application, network or process?
A. Threat
B. Exploit
C. Vulnerability
D. Attack

Answer: C

4. Which of the following refers to an attacker exploiting vulnerabilities before the vendor has a patch or mitigation for them?
A. Day 1 attack
B. Zero-day attack
C. Exploit
D. Category I attack

Answer: B

5. Which of the following refers to an unskilled hacker that uses pre-made scripts and tools to hack into systems?
A. Ethical Hacker
B. Grey Hat
C. Cyber Terrorist
D. Script Kiddie

Answer: D

6. Gathering information about a target without direct contact is called:
A. Social engineering
B. Passive footprinting
C. Active footprinting
D. Enumeration

Answer: B

7. All of the following information is typically gathered during the footprinting stage of an attack EXCEPT:
A. Log files
B. IP address range
C. Domain names
D. Website names

Answer: A

8. Determining which hosts on a network are running SMTP services is an example of:
A. DNS footprinting
B. Email footprinting
C. WHOIS footprinting
D. Google hacking

Answer: B

9. Which of the following Google hacking operators will return search query results that contain ALL of the query terms in the web site title?
A. `intitle`
B. `site`
C. `allinurl`
D. `allintitle`

Answer: D

10. All of the following information can be gathered from WHOIS footprinting EXCEPT:
A. Web server vulnerabilities
B. Domain name
C. Registered IP addresses
D. DNS server information

Answer: A

11. A full TCP scan on a host or network involves:
A. Setting all TCP flags to “on”
B. A complete TCP 3-way handshake
C. Setting all TCP flags to “off”
D. Scanning all TCP ports

Answer: B

12. During a “ping sweep”, an active host returns what type of response?
A. ARP REPLY
B. ICMP ECHO REQUEST
C. ICMP ECHO REPLY
D. Nothing

Answer: C

13. What type of scan is accomplished by running the command: `nmap -sS 192.168.10.13`?
A. An ACK scan
B. A SYN scan
C. A ping sweep
D. An XMAS scan

Answer: B

14. Which TCP flag signifies a complete transmission?
A. FIN
B. SYN
C. ACK
D. RST

Answer: A

15. An XMAS scan consists of which TCP flags set as “on”?
A. FIN, URG, PSH
B. RST, URG, PSH
C. SYN, SYN/ACK, FIN
D. SYN, ACK, RST

Answer: A

16. Which of the following ports is used by the Domain Name Service?
A. 135
B. 53
C. 67
D. 25

Answer: B

17. Enumerating TCP port 25 can give you information on which of the following services?
A. SNMP
B. SMTP
C. LDAP
D. NTP

Answer: B

18. Which of the following built-in commands can enumerate NetBIOS services on a Windows machine?
A. `nmap.exe`
B. `nc.exe`
C. `netstat.exe`
D. `nbtstat.exe`

Answer: D

19. What is the default read/write community string for SNMP?
A. `secret`
B. `public`
C. `private`
D. `password`

Answer: C

20. Which SMTP enumeration command is used to identify the recipients of a message?
A. `EXPN`
B. `VRFY`
C. `RCPT TO`
D. `HELO`

Answer: C

21. Which type of password attack makes use of extensive wordlists to hash and run against a captured password hash?
A. Character
B. Brute Force
C. Rainbow tables
D. Dictionary

Answer: D

22. Where are password hashes stored on a Windows system?
A. /etc/shadow
B. SAM file
C. PASSWORDS file
D. C:\Windows\system32\shadow

Answer: B

23. Which of the following is a popular password cracking tool for Linux-based systems?
A. John the Ripper
B. Cain and Abel
C. KeyPass
D. Passcrack

Answer: A

24. Which of the following types of rootkits work at the core of the operating system?
A. Library rootkits
B. Application-level rootkit
C. Kernel-level rootkit
D. Firmware rootkit

Answer: C

25. Which file system supports alternate data streams (ADS)?
A. EXT3
B. NTFS
C. FAT
D. HPFS

Answer: B

26. What kind of communications channel does a Trojan facilitate?
A. Open
B. Encrypted
C. Overt
D. Covert

Answer: D

27. All of the following are symptoms of a Trojan attack EXCEPT:
A. Abnormal increase of hard disk activity
B. Abnormal increase in network traffic from host
C. Unexplained pop-up messages
D. Computer shutdown due to overheating

Answer: D

28. A Trojan is installed on a system by means of a _____:
A. Dropper
B. Wrapper
C. Macro
D. Batch file

Answer: A

29. Which switch causes the netcat Trojan to listen on a specific inbound port?
A. `e`
B. `l`
C. `p`
D. `d`

Answer: B

30. A _____Trojan uses a victim's host machine to act as an attacker
A. Proxy
B. Botnet
C. Zombie
D. Remote access

Answer: A

31. A virus composed of a series of otherwise legitimate actions in an application such as Microsoft Word is called a _____:
A. Boot sector virus
B. Multipartite virus
C. Macro virus
D. File virus

Answer: C

32. Viruses that change their characteristics and signatures on infection to avoid antivirus detection are called:
A. Encryption viruses
B. Polymorphic viruses
C. Companion viruses
D. Boot sector viruses

Answer: B

33. Which of the following files could be considered as a “safe” file, rather than a potential file extension virus?
A. work.doc.cmd
B. work.exe
C. work.txt.vbs
D. work.txt

Answer: D

34. A piece of malware that is able to spread to a variety of hosts across a network, without human intervention, is called a _____.
A. Trojan
B. Spreader virus
C. Worm
D. Bot

Answer: C

35. All of the following are characteristics of worms, EXCEPT:
A. Corrupts executable programs
B. Self-replicating
C. Does not modify programs
D. Easily removed

Answer: A

36. Which of the following protocols is most vulnerable to sniffing attacks?
A. FTP
B. SSH
C. SSL
D. IPSec

Answer: A

37. Which network device mitigates sniffing attacks?
A. Repeaters
B. Bridges
C. Hubs
D. Switches

Answer: D

38. All of the following are susceptible to sniffing EXCEPT:
A. Plaintext passwords
B. FTP file transfers
C. Encrypted communications sessions
D. Telnet sessions

Answer: C

39. What mode must a network adapter be placed in to facilitate sniffing attacks?
A. Listening mode
B. Promiscuous mode
C. Non-switched mode
D. Active mode

Answer: B

40. Which of the following is the most effective way to defend against sniffing attacks?
A. Two-factor authentication
B. Data compression
C. Complex passwords
D. Encryption

Answer: D

41. All of the following human traits contribute to the success of social engineering attacks EXCEPT:
A. Suspicion
B. Trust
C. Social obligation
D. Ignorance

Answer: A

42. Which of the following social engineering techniques is used to get an individual's password as it is entered on the keyboard?
A. Eavesdropping
B. Dumpster diving
C. Shoulder surfing
D. Tailgating

Answer: C

43. Which type of computer-based social- engineering attack attempts to persuade users to click on links in an email?
A. Spam
B. Phishing
C. Pop-ups
D. Fake antivirus

Answer: B

44. An attack that targets specific individuals in an organization is known as a(n) _____ attack.
A. whaling
B. spear phishing
C. impersonation
D. authority

Answer: B

45. Which is the best type of defense for social engineering attacks?
A. Strong passwords
B. Permissions
C. Encryption
D. Education

Answer: D

46. What type of DoS attack starts the first part of a TCP three-way handshake using a spoofed source IP address, but does not complete the process?
A. ICMP flood
B. XMAS attack
C. SYN attack
D. UDP flood

Answer: C

47. Which protocol is used to perpetrate a “Ping of Death” attack?
A.UDP
B. ICMP
C. TCP
D. FTP

Answer: B

48. A large network of compromised hosts, all remotely controlled to attack a victim host or network, is called a:
A. Botnet
B. Honeynet
C. Malnet
D. Trojan Army

Answer: A

49. Which of the following tools can be used to conduct a Denial of Service attack on a host?
A. HPing3
B. netcat
C. Nmap
D. Nessus

Answer: A

50. All of the following are defenses against DoS attacks EXCEPT:
A. Packet filtering
B. Dropping HTTP packets at the firewall
C. TCP/IP stack hardening
D. In-line IDS

Answer: B

51. All of the following items make session hijacking successful EXCEPT:
A. Plaintext passwords
B. HTTP referrer
C. Session ID
D. Public keys

Answer: D

52. Which of the following are needed to successfully break into a TCP communications session?
A. Port number
B. Serial number
C. Sequence number
D. Protocol number

Answer: C

53. What must be done after finding a connection of interest to begin the session hijacking attempt?
A. Desynchronizing the connection
B. Decrypting the session
C. Sniffing the connection
D. Flooding the connection

Answer: A

54. Which of the following attempts to take over the session a client establishes with a web server?
A. TCP hijacking
B. Cross-site scripting
C. Spoofing
D. Flooding

Answer: B

55. Which type of session hijacking attack requires that the attacker's transmission follow a specific network or Internet path?
A. Source routing
B. Reverse routing
C. IP spoofing
D. Sequence prediction

Answer: A

56. All of the following are web server attack vectors EXCEPT:
A. Faulty directory permissions
B. Plaintext passwords
C. Encrypted password hashes
D. Unpatched server software

Answer: C

57. Which of the following is an example of a web server configuration issue that an attacker may exploit?
A. Default user passwords
B. Expired SSL certificates
C. Use of older, less secure browsers
D. Use of non-standard ports

Answer: A

58. Which attack allows the attacker to view files outside the web server root directory?
A. Session hijacking attack
B. Privilege escalation attack
C. Default shares attack
D. Directory traversal attack

Answer: D

59. Which attack allows an attacker to intercept communications between a client and web server?
A. TCP/IP hijacking attack
B. Man-in-the-middle attack
C. Birthday paradox attack
D. Sniffing attack

Answer: B

60. An attack where malicious HTML tags or scripts are injected into a victim website is called a_____.
A. session hijacking attack
B. cross-site request forgery attack
C. cross-site scripting attack
D. SQL injection attack

Answer: C

61. An attacker can alter a cookie to thwart:
A. Integrity
B. Non-repudiation

C. Encryption
D. Authentication

Answer: D

62. Entering data into a web form that the form was not designed to handle is an example of:
A. Parameter manipulation
B. Unvalidated input
C. XML injection
D. SQL injection

Answer: B

63. An attack that allows database commands to be appended to invalid form input is known as:
A. Cross-site request forgery
B. Parameter tampering
C. SQL injection
D. XML injection

Answer: C

64. Which type of attack takes advantage of a web application not properly programmed to manage memory or data storage?
A. XML injection attack
B. Buffer overflow attack
C. Cross-site scripting attack
D. Command injection attack

Answer: B

65. All of the following could result from improper error handling in a web application EXCEPT:
A. Denial of service
B. Command shell
C. Memory errors
D. Weak passwords

Answer: D

66. Which SQL command is used to determine which records to retrieve from a database table?
A. Update
B. Select
C. Insert
D. Delete

Answer: B

67. In which type of SQL injection attack are the results of the command string entered not visible to the attacker?
A. Blind SQL injection
B. Hidden SQL injection
C. False SQL injection
D. Simple SQL injection

Answer: A

68. Which text can be appended to an SQL command to generate an error or get access to an entire database table?
A. #=1
B. ‘ OR 1=1
C. $SHELL
D. ==

Answer: B

69. Which of the following RDBMS applications are vulnerable to SQL injection?
A. Oracle
B. Microsoft SQL Server
C. Postgres
D. All of the above

Answer: D

70. Which of the following is the best mitigation for SQL injection attacks?
A. Input validation
B. Encryption
C. Complex passwords
D. File permissions

Answer: A

71. WEP is a vulnerable wireless protocol due to all of the following EXCEPT:
A. Small IV size
B. Use of AES
C. Use of RC4
D. Repeating keys

Answer: B

72. Which of the following wireless security protocols use AES?
A. Open WEP
B. WPA
C. WPA2
D. Shared WEP

Answer: C

73. Which of the following commands will place a wireless network card into monitor mode?
A. `airodump-ng mon0`
B. `airmon-ng start wlan0`
C. `aireplay mon0`
D. `airmon-ng start mon0`

Answer: B

74. What must be captured during a wireless attack on WPA/WPA2?
A. 4-way handshake
B. 3-way handshake
C. 802.1X key
D. WEP key

Answer: A

75. Which command or program is used to perform a dictionary attack on a WPA/WPA2 capture file to obtain the key?
A. aircrack-ng
B. aireplay-ng
C. Netcat
D. Jack the Ripper

Answer: A

76. Which of the following terms applies to a mobile device that has been rendered inoperable due to attempts to hack it?
A. rooting
B. bricking
C. jailbreaking
D. Sandboxing

Answer: B

77. A secure environment in which mobile applications run is called a _____.
A. Chrooted jail
B. Sandbox
C. Firewall
D. Cleanroom

Answer: B

78. The Android mobile operating system is based upon _____.
A. BSD
B. Mac OS
C. Windows
D. Linux

Answer: D

79. Which of the following are programs designed to root an Android device?
A. Cydia
B. ZitMo
C. SuperOneclick
D. Redsn0w

Answer: C

80. A(n) _____ can be used by security professionals and hackers to test exploits against mobile devices.
A. simulator
B. sandbox
C. emulator
D. virtual device

Answer: C

81. Which of the following is the most effective scanning technique used to detect firewalls on a network?
A. Full TCP connect scan
B. SYN scan
C. ICMP scan
D. ACK scan

Answer: D

82. What scanning technique is useful for avoiding IDS detection?
A. TCP scan
B. Stealth scan
C. Ping sweep
D. XMAS scan

Answer: B

83. Which of the following can make it difficult for an IDS to read the traffic from an attacker?
A. Encryption
B. Spoofing
C. Tunneling
D. Flooding

Answer: A

84. What type of device emulates other operating systems on a network?
A. Scanner
B. Sniffer
C. Honeypot
D. Spammer

Answer: C

85. Which common protocol is often used to tunnel malicious traffic through, as it is frequently not blocked through firewalls?
A. TELNET
B. HTTP
C. FTP
D. ICMP

Answer: B

86. Which attack takes advantage of small allocation areas for memory space and strings in a program?
A. XML injection
B. Command injection
C. SQL injection
D. Buffer overflow attack

Answer: D

87. Which of the following programming languages is popular in developing buffer overflow programs?
A. SQL
B. Shell scripts
C. PERL
D. C++

Answer: D

88. A popular compiler on the Linux platform, used to help create buffer overflow programs, is:
A. gcc
B. gdd
C. netcat
D. vim

Answer: A

89. A buffer set to hold 25 characters will overflow when the number of characters entered into it is:
A. Validated
B. Exceeded
C. Reduced
D. Converted

Answer: B

90. Which of the following will reduce the number of buffer overflow conditions?
A. Bounds checking
B. Input validation
C. Expanding buffer sizes
D. Reducing buffer sizes

Answer: A

91. Which of the following is generally considered to be public knowledge, instead of confidential?
A. Private key
B. Password
C. Algorithm
D. Symmetric key

Answer: C

92. Which of the following are hashing algorithms?
A. AES
B. SHA-256
C. 3DES
D. RC4

Answer: B

93. Which of the following algorithms is used to generate a private/public key pair?
A. TWOFISH
B. AES
C. RC4
D. RSA

Answer: D

94. If Bobby sends Tim a message encrypted with Tim's public key, which key is required to decrypt it?
A. Bobby's public key
B. Bobby's private key
C. Tim's private key
D. Tim's public key

Answer: C

95. Which cryptography attack requires the attacker to have a confirmed piece of plaintext, and its corresponding ciphertext, in order to derive the key?
A. Known plaintext attack
B. Chosen plaintext attack
C. Known ciphertext attack
D. Chosen ciphertext attack

Answer: A

96. Which type of penetration test is completely blind in terms of organizational and infrastructure knowledge possessed by the tester?
A. Black box test
B. Grey box test
C. External test
D. White box test

Answer: A

97. Which type of test actually exploits weaknesses found in a system?
A. White box test
B. Black box test
C. Vulnerability assessment
D. Penetration test

Answer: D

98. What is the most critical element in the planning phase of a penetration test?
A. Scope and schedule
B. Permission to test from the system owner
C. Personnel assignments
D. Equipment list

Answer: C

99. A penetration test specifically targeted at one part of the infrastructure is considered a:
A. White box assessment
B. Limited scope assessment
C. Vulnerability assessment
D. Security audit

Answer: B

100. Which of the following should be included in the final penetration testing report?
A. Blame
B. Offers of additional services
C. Criticisms of personnel
D. Mitigations

Answer: D

101. Which of the following ports are used by FTP?
A. 21
B. 23
C. 22
D. 53

Answer: A

102. All of the following are considered cleartext protocols EXCEPT:
A. Telnet
B. FTP
C. SSH
D. HTTP

Answer: C

103. Which port is used when a hacker uses the Telnet protocol to communicate with a mail server to enumerate it?
A. 23
B. 25
C. 129
D. 22

Answer: B

104. During a port scan, nmap discovers that port 1433 is open on a host. Which service listens on port 1433?
A. SSL
B. MS SQL Server
C. NTP
D. POP3

Answer: B

105. If port 111 is identified on a host during a port scan, which operating system is likely to be running on the host?
A. Mac OS
B. Windows 7
C. Windows XP
D. Unix

Answer: D

106. Which of the following is a popular web application vulnerability scanner?
A. Metasploit
B. Nmap
C. Acunetix
D. NetToolsPro

Answer: C

107. Which command can be used to compile a buffer overflow program?
A. `gcc buffer_overflow.c:buff_ovflw`
B. `gcc buffer_overflow.c -o buff_ovflw`
C. `gcc buffer_overflow.txt -o buff_ovflw.c`
D. `gcc buffer_overflow > buff_ovflw`

Answer: B

108. Which command in Windows can be used to insert a file into another via NTFS streams?
A. `type`
B. `cat`
C. `gcc`
D. `start`

Answer: A

109. Which of the following commands starts a netcat listener?
A. `nc -lvp 3333`
B. `nc 192.168.163.129 3333`
C. `nc -lvp 192.168.163.129`
D. `nc -e cmd.exe 3333`

Answer: A

110. Which of the following programs is used to detect NTFS Alternate Data Streams (ADS)?
A. Netcat
B. LADS
C. StegDetect
D. type

Answer: B

111. Which of the following is a popular password cracking tool for Windows?
A. Netcat
B. Jack the Ripper
C. Cain and Abel
D. Nessus

Answer: C

112. All of the following are considered to be popular Trojan horse programs EXCEPT:
A. Kriptomatic
B. Back Oriffice
C. Metasploit
D. NetBus

Answer: C

113. Using which of the following password cracking techniques risks locking an account?
A. Online attack
B. Offline attack
C. Brute force attack
D. Rainbow tables attack

Answer: A

114. Which switch enables Nmap to perform OS fingerprinting?
A. `-sP`
B. `-A`
C. `-sT`
D. `-U`

Answer: B

115. Which tool enables a hacker to actually exploit vulnerabilities found on a host?
A. Metasploit
B. Nmap
C. Nessus
D. Netcat

Answer: A

116. Where are user accounts stored on a Linux host?
A. /etc/SAM
B. /etc/shadow
C. /etc/passwd
D. /etc/password

Answer: C

117. Which secure protocol uses TCP port 443?
A. SSL
B. SSH
C. IPSec
D. SFTP

Answer: A

118. Which of the following is true regarding physical system access?
A. Most operational procedures prevent physical system access
B. Physical access can be used to break encryption keys
C. Session encryption may prevent physical access
D. Firewalls and other security devices may be bypassed

Answer: D

119. Hackers may try to cover tracks by deleting _____.
A. user accounts
B. audit logs
C. encryption keys
D. shared data

Answer: B

120. How many characters are in a MD5 hash?
A. 160
B. 128
C. 32
D. 16

Answer: C

121. Which type of device plugs into a port on a host to capture information?
A. IDS
B. Keystroke logger
C. Sniffer
D. Proxy

Answer: B

122. Which of the following can be used to steal password hashes from a Windows machine?
A. Pwdump
B. Nmap
C. Nessus
D. Acunetix

Answer: A

123. Which Security Identifier (SID) suffix identifies the true administrator account on a Windows host, even if it has been renamed?
A. 1000
B. 500
C. 501
D. 0

Answer: B

124. After obtaining user-level access to a host, what is the next most likely step for a hacker?
A. Scanning
B. Footprinting
C. Covering tracks
D. Escalation of privileges

Answer: D

125. Which type of configuration issue is most easily exploitable by a hacker?
A. Restrictive directory permissions
B. Use of AES encryption
C. Default passwords
D. Disabling file and print sharing

Answer: C