

The configuration allows a wired or wireless network C. Promiscuous interface

controller to pass all traffic it receives to the central processing

unit (CPU), rather than passing only the frames that the controller is intended

to receive.

Which of the following is being described?

- A. WEM
- B. Multi-cast mode
- C. Promiscuous mode
- D. Port forwarding
- 2. In Risk Management, how is the term "likelihood" related to the concept of "threat?"
  - A. Likelihood is the probability that a vulnerability is exploit a vulnerability.

    a threat-

source.

- B. Likelihood is a possible threat-source that may exploit a vulnerability.
- C. Likelihood is the likely source of a threat that could exploit a vulnerability.
- D. Likelihood is the probability that a threat-source will exploit a vulnerability.
- 3. While performing online banking using a web brows- A. Cross-Site Reer, a user receives quest Forgery an email that contains a link to an interesting Web

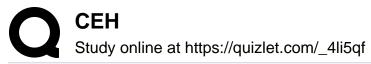
site. When the

user clicks on the link, another web browser session starts and

displays a video of cats playing a piano. The next business day, the

user receives what looks like an email from his bank, indicating that

D. Likelihood is the probability that a threat-source will exploit a vulnerability.



his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.

What web browser-based security vulnerability was exploited to

compromise the user?

- A. Cross-Site Request Forgery
- **B. Cross-Site Scripting**
- C. Web form input validation
- D. Clickjacking
- 4. Which of the following is one of the most effective ways to prevent Cross-site Scripting (X55) flaws in software applications?

C. Validate and escape all information sent over to a server

- A. Verify access right before allowing access to protected information and UI controls
- B. Use security policies and procedures to define and implement proper security settings
- C. Validate and escape all information sent over to a server
- D. Use digital certificates to authenticate a server prior to sending data
- 5. An incident investigator asks to receive a copy of the C. The attack alevent from all tered or erased firewalls, proxy servers, and Intrusion Detection Sysevents from the tems (IDS) on the network logs of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs the sequence of many of the logged events do not match up.

# CEH Study online at https://quizlet.com/\_4li5qf

What is the most likely cause?

- A. The network devices are not all synchronized
- B. The security breach was a false positive
- C. The attack altered or erased events from the logs.
- D. Proper chain of custody was not observed while collecting the logs
- 6. This tool is an 802.11 WEP and WPA-PSK keys crack- D. Aircrack-ng ing program that can recover keys once enough data packets have been captured. It implements the standard FMS attach along with some optimizations like Korek attacks, as well as the PTW attack, thus making the attack much

faster compared to other WEP cracking tools. Which of the following tools is being described?

- A. Wificracker
- B. WLAN crack
- C. Airguard
- D. Aircrack-ng
- 7. Which of the following tools is used to analyze the C. Tcptrace files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?
  - A. Nessus
  - **B.** Tcptraceroute
  - C. Tcptrace
  - D. OpenVAS
- 8. You have compromised a server on a network and successfully open a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the machines in the network using the nmap syntax

D. The nmap syntax is wrong

below, it is not going through.

**QUITTING!** 

What seems to be wrong?

- A. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
- B. This is a common behavior for a corrupted nmap application.
- C. OS Scan requires root privileged.
- D. The nmap syntax is wrong.
- Which of the following is the greatest threat posed by A. An un-encrypt-backups?
   A. An un-encrypted backup can be misplaced or stolen
  - B. A backup is incomplete because no verification was performed.
  - C. A backup is the source of Malware or illicit information.
  - D. A backup is unavailable during disaster recovery.
- 10. An attacker has installed a RAT on a host. The attack- A. Hosts er wants to

ensure that when a user attempts to go to www.MyPersonalBank.com, that the user is directed to a phishing site.

Which file does the attacker need to modify?

- A. Hosts
- **B. Networks**
- C. Boot.ini
- **D. Sudoers**
- Jesse receives an email with an attachment labeled A. Trojan "Court\_Notice\_21206.zip". inside the zip file is a file named

"Court\_Notice\_21ZO6.docx.exe" disguised as a word

document. Upon

execution, a windows appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA\l0cal directory and begins to beacon to a C2 server to download additional

malicious binaries. What type of malware has Jesse encountered?

- A. Trojan
- **B. Worm**
- C. Key-Logger
- **D. Micro Virus**
- 12. In 2007, this wireless security algorithm was rendered A. Wired Equivuseless by alent Privacy capturing packets and discovering the passkey in a (WEP)

matter of seconds. This security flaw led to a network

invasion of TJ Maxx and data

theft through a technique known wardriving.

Which algorithm is this referring to?

- A. Wired Equivalent Privacy (WEP)
- B. Temporal Key Integrity Protocol (TRIP)
- Q. Wi-Fi Protected Access (WPA)
- D. Wi-Fi Protected Access 2 (WPA2)
- 13. What is the best description of SQL Injection?

A. It is a Denial of Service Attack.

B. It is an attack used to modify code in an application.

C. It is and attack used to gain unauthorized access Server and Web to a database.

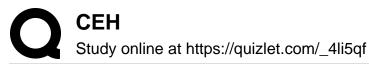
D. It is a Man-in-the-Middle attack between your SQL Server and Web

D. It is

a Man-in-the-Middle attack between your SQL

- 14. Which of the following is the successor of SSL?
  - A. RSA
  - B. GRE
  - C.TLS
  - D. IPSec

C. TLS



- 15. As a Certified Ethical hacker, you were contracted by A. Term of Enaprivate firm to conduct an external security assess- gagement ment through penetration testing. What document describes the specified of the testing, the associated violations, and essentially protects both the organization's interest and your li abilities as a tester?
  - A. Term of Engagement
  - **B. Non-Disclosure Agreement**
  - C. Project Scope
  - **D. Service Level Agreement**
- 16. Which of the following is not a Bluetooth attack?
- B. Bluedriving

- A. Bluejacking
- **B.** Bluedriving
- C. Bluesnarfing
- D. Bluesmaking
- 17. **PGP, SSL, and IKE are all examples of which type of** C. Public Key cryptography?
  - A. Hash Algorithm
  - **B. Secret Key**
  - C. Public Key
  - D. Digest
- 18. Using Windows CMD, how would an attacker list all D. NET VIEW the shares to which

the current user context has access?

- A. NET CONFIG
- **B. NET USE**
- C. NET FILE
- D. NET VIEW
- 19. Which of these options is the most secure procedure A. In a climate controlled facility tapes?
  - A. In a climate controlled facility offsite
  - B. Inside the data center for faster retrieval in a fireproof safe
  - C. In a cool dry environment
  - D. On a different floor in the same building

20. What is the benefit of performing an unannounced **Penetration Testing?** 

A. The tester will have an actual security posture visibility of the target network.

B. The tester could not provide an honest analysis.

C. Network security would be in a "best state" posture.

D. It is best to catch critical infrastructure unpatched.

- 21. What does a firewall check to prevent particular ports A. Transport layer and applications from getting packets into an organi- port numbers and zations? application layer
  - A. Transport layer port numbers and application layer headers headers
  - B. Network layer headers and the session layer port numbers
  - C. Application layer port numbers and the transport layer headers
  - D. Presentation layer headers and the session layer port numbers
- > NMAP —sn 192.168.11.200—215 22. The NMAP command above performs which of the following?

A. A ping scan

- **B.** A trace sweep
- C. An operating system detect
- D. A port scan
- 23. An Internet Service Provider (ISP) has a need to au- D. TACACS+ thenticate users

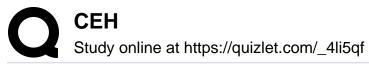
connecting using analog modems, digital Subscriber Line (DSL), wireless data services, and virtual Private Networks (VPN) over a Frame Relay network.

Which AAA protocol is most likely able to handle this requirement?

- A. DIAMETER
- B. Kerberos

A. The tester will have an actual seibility of the target network

A. A ping scan



C. RADIUS D. TACACS+

24. To determine if a software program properly handles C. Puzzing a wide range of

invalid input, a form of automated testing can be used randomly

generate invalid input in an attempt to crash the program.

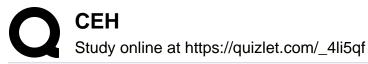
What term is commonly used when referring to this type of testing?

- A. Bounding
- **B.** Mutating
- C. Puzzing
- D. Randomizing
- Which of the following tools can be used for passive C. nmap 25. **OS fingerprinting?** 
  - A. tcpdump
  - B. ping
  - C. nmap
  - D. Tracert
- 26. Your company performs penetration tests and secu- D. Immediately rity assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

- A. Copy the data to removable media and keep it in case you need it.
- B. Ignore the data and continue the assessment until completed as agreed.
- C. Confront the client on a respectful manner and ask her about the data.

stop work and contact the proper legal authorities.



D. Immediately stop work and contact the proper legal authorities.

27. You are the Systems Administrator for a large corpo- C. Network-Based

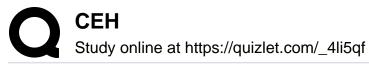
- rate organization.
  You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?
  - A. Host—based IDS
  - **B. Firewall**

the same hash

- C. Network-Based IDS
- D. Proxy
- 28. What is a "Collision attack" in cryptography?
  A. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key B. Collision attacks try to break the hash into three parts to get the plaintext value C. Collision attacks try to find two inputs producing
- C. Collision attacks try to find two inputs producing the same hash

IDS

- D. Collision attacks try to get the public key
- 29. The "Black box testing" methodology enforces which A. Only the exterkind of nal operation of a restriction? system is accessi-
  - A. Only the external operation of a system is accessi- ble to the tester ble to the tester
  - B. The internal operation of a system is completely known to the tester.
  - C. Only the internal operation of a system is known to the tester.
  - D. The internal operation of a system is only partly accessible to the tester.
- 30. You've gained physical access to a Windows 2008 R2 A. John the Ripper server which has as accessible disc drive. When you



attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux tool has the ability to

change any user's password or to activate disabled Windows Accounts?

- A. John the Ripper
- **B. CHNTPW**
- C. Cain & Abel
- D. SET
- 31. While using your bank's online servicing you notice C. Web Parameter the following Tampering

string in the URL bar:

"http://www.MyPersonalBank/Account? Id=368940911028389&Damount=10980&Camount=21" You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

What type of vulnerability is present on this site?

- A. SQL injection
- **B. XSS Reflection**
- C. Web Parameter Tampering
- D. Cookie Tampering
- 32. It is a short-range wireless communication technolo- A. Bluetooth gy intended to

replace the cables connecting portables of fixed devices while

maintaining high levels of security. It allows mobile phones,

computers and other devices to connect and communicate using a short-

range wireless connection.

Which of the following terms best matches the definition?

- A. Bluetooth
- **B.** Radio-Frequency Identification

D. Delegate

- 35. The phase will increase the odds of success in later C. Footprinting phases of the

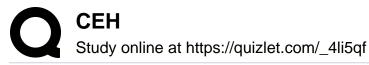
penetration test. It is also the very first step in Information

Gathering, and it will tell you what the "landscape" looks like.

What is the most important phase of ethical hacking in which you need

to spend a considerable amount of time?

- A. Network Mapping
- **B.** Gaining access
- C. Footprinting
- D. Escalating privileges
- Which regulation defines security and privacy con-D. NIST-800-53 36. trols for Federal



information systems and organizations?

A. HIPAA

**B. EU Safe Harbor** 

C. PCI-DSS

D. NIST-800-53

37. Which of the following describes the characteristics C. Moves the MBR of a Boot Sector

to another location on the hard disk

A. Overwrites the original MBR and only executes the and copies new virus code

**MBR** 

B. Modifies directory table entries so that directory entries point to the virus code instead of the actual

itself to the original location of the

program

Virus?

C. Moves the MBR to another location on the hard disk and copies

itself to the original location of the MBR

D. Moves the MBR to another location on the RAM and copies itself to

the original location of the MBR

You are performing information gathering for an im- D. Metagoofil 38. portant penetration

test. You have found pdf, doc, and images in your objective. You

decide to extract metaolata from these files and analvze it.

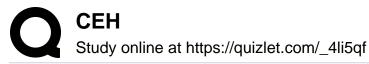
What tool will help you with the task?

- A. Armitage
- **B.** Dimitry
- C. cdpsnarf
- D. Metagoofil

Which of the following is an extremely common IDS C. unicode charac-39. evasion technique in the web world? ters

A. post knocking

**B.** subnetting



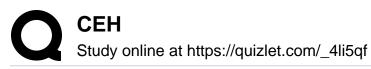
- C. unicode characters
- D. spyware
- 40. When you are testing a web application, it is very A. Burpsuite useful to employ a proxy tool to save every request and response. Nyou can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise

results than if using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?

- A. Burpsuite
- **B.** Dimitry
- C. Proxychains
- D. Maskgen
- 41. It is a kind of malware (malicious software) that crimi- C. Ransomware nals install on your computer so they can lock it from a remote location. This malware generates a pop-up windows, webpage, or email warning from what looks like an official authority. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again.

Which term best matches this definition?

- A. Spyware
- **B.** Adware
- C. Ransomware
- D. Riskware
- 42. Which of the following is assured by the use of a D. Integrity hash?
  - A. Availability
  - **B.** Confidentiality



- C. Authentication
- **D.** Integrity
- 43. When you are getting information about a web server, B. http-git it is very

important to know the HTTP Methods (GET, POST,

**HEAD, PUT, DELETE,** 

TRACE) that are available because there are two critical

methods (PUT and DELETE). PUT can upload a file to the server and

DELETE can delete a file from the server. You can detect all these

methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.

What nmap script will help you with this task?

- A. http enum
- B. http-git
- C. http-headers
- D. http-methods
- 44. **During a blackbox pen test you attempt to pass IRC** C. Application traffic over post

80/TCP from a compromised web enabled host. The traffic gets blocked;

however outbound HTTP traffic is unimpeded.

What type of firewall is inspecting outbound traffic?

- A. Circuit
- **B. Packet Filtering**
- C. Application
- D. Stateful
- 45. A company's security states that all web browsers

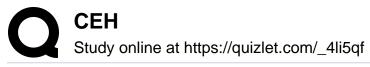
  must automatically

  delete their HTTP browser cookies upon terminating. Web sites that

  What sort of

  security breach is this policy attempting to mitigate? browser user

  A. Attempts by attackers to determine the user's Web by stealing the



browser usage

patterns, including when sites were visited and for how long.

user's authentication credentials.

- B. Attempts by attackers to access passwords stored on the user's
- computer without the user's knowledge.
- C. Attempts by attackers to access Web sites that trust the Web

browser user by stealing the user's authentication credentials.

- D. Attempts by attackers to access the user and password information stores in the company's SQL database.
- You've just been hired to perform a pen test on an 46. organization that has been subjected to a large-scale attack. The CIO is not eliminate all concerned with mitigating threats and vulnerabilities to totally elimi- able to reduce risk nate risk.

C. Explain to the CIO that you canrisk, but you will be to

What Is one of the first thing you should to when the acceptable levels

- A. Start the wireshark application to start sniffing network traffic.
- B. Establish attribution to suspected attackers.
- C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
- D. Interview all employees in the company to rule out possible insider threats.
- Which of the following security operations is used for B. Running a net-47. determining the attack surface of an organization? A. Reviewing the need for a security clearance for each employee

work scan to detect network services in the corpo-

B. Running a network scan to detect network services rate in the corporate

DM7

**DMZ** 

C. Training employees on the security policy regard-

ing social engineering

- D. Using configuration management to determine when and where to apply security patches
- Perspective clients want to see sample reports from B. Share full re-48. previous penetration tests.

ports, with redacted.

What should you do next?

- A. Share full reports, not redacted.
- B. Share full reports, with redacted.
- C. Decline but, provide references.
- D. Share reports, after NDA is signed.
- 49. Which of the following statements is TRUE?
  - A. Sniffers operation on Layer 3 of the OSI model
  - B. Sniffers operation on Layer 2 of the OSI model
  - C. Sniffers operation on the Layer 1 of the OSI model OSI model
  - D. Sniffers operation on both Layer 2 & Layer 3 of the **OSI** model
- Jimmy is standing outside a secure entrance to a 50. facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone. grabs the door as it begins to close.

What just happened?

- A. Masquading
- **B. Phishing**
- C. Whaling
- D. Piggybacking
- The heartland bug was discovered in 2014 and is 51. widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2004-1060. This bug affects the OpenSSL implementation of the transport

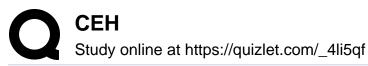
D. Piggybacking

A. Root

D. Sniffers opera-

tion on both Layer

2 & Layer 3 of the



Layer security (TLS) protocols defined in RFC65ZO. What types of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

- A. Root
- **B. Private**
- C. Shared
- D. Public
- 52. You work as a Security Analyst for a retail organiza- A. False Negative tion. In securing

the company's network, you set up a firewall and an IDS. However,

hackers are able to attack the network. After investigating, you

discover that your IDS is not configured properly and therefore is

unable to trigger alarms when needed. What type of alert is the IDS giving?

- A. False Negative
- **B. True Negative**
- **C. True Positive**
- **D. False Positive**
- 53. This international organization regulates billions of transactions

B. International
Security Indus- try Organization
(ISIO)

daily and provides security guidelines to protect per- try Organization sonally identifiable information (PII). These security (ISIO) controls provide a

baseline and prevent low-level hackers sometimes known as script

kiddies from causing a data breach.

Which of the following organizations is being described?

- A. Payment Card Industry (PCI)
- **B. International Security Industry Organization (ISIO)**
- C. Institute of Electrical and Electronics Engineers

### (IEEE)

- D. Center for Disease Control (CDC)
- 54. Which of the following tools performs comprehen- C. Nikto sive tests against web servers, including dangerous files and CGI's?
  - A. Snort
  - **B.** Dsniff
  - C. Nikto
  - D. John the Ripper
- 55. Which of the following is the structure designed to A. PKI verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?
  - A. PKI
  - **B.** biometrics
  - C. SOA
  - D. single sign on
- 56. The chance of a hard drive failure is once every three B. \$146 years. The cost to buy a new hard drive is \$300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns \$10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%). What is the closest approximate cost of this replacement and recovery operation per year?
  - A. \$100
  - B. \$146
  - C. 440
  - D. 1320
- 57. An attacker changes the profile information of a par- A. Cross—Site ticular user on a Request Forgery

target website (the victim). The attacker uses this string to update

the victim's profile to a text file and then submit the data to the

attacker's database.

<frame src=http://www/vulnweb.com/updataif.php</pre>

Style="display:none"></iframe>

What is this type of attack (that can use either HTTP

**GET or HRRP** 

POST) called?

A. Cross—Site Request Forgery

**B. Cross-Site Scripting** 

C. SQL Injection

D. Browser Hacking

You are tasked to perform a penetration test. While D. Social engi-58. you are performing information gathering, you find ab neering employee list in Google. You find receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the

links, and her machine gets infected.

What testing method did you use?

A. Piggybacking

**B.** Tailgating

C. Evesdropping

D. Social engineering

59. Which of the following is a protocol specifically de- C. SYSLOG signed for

transporting event messages?

A. SMS

B. SNMP

- C. SYSLOG
- D. ICMP
- 60. Which of the following is component of a risk assess- C. Administrative ment?
  - A. Logical interface
  - B. DMZ
  - C. Administrative safeguards
  - D. Physical security
- 61. Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?
- B. Service Oriented Architecture

- A. Lean Coding
- **B. Service Oriented Architecture**
- **C.** Object Oriented Architecture
- **D. Agile Process**
- 62. A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants

C. Cross-site Scripting vulnerability

to modify the software requirements to disallow users from entering

HTML as input into their Web application.

What kind of web application vulnerability likely exists in their

software?

- A. Web site defacement vulnerability
- B. SQL injection vulnerability
- C. Cross-site Scripting vulnerability
- D. Cross-site Request Forgery vulnerability
- 63. It is an entity or event with the potential to adversely A. Threat impact a system through unauthorized access destruction disclosures denial of service or modification of data.



### **CEH**

Study online at https://quizlet.com/\_4li5qf

Which of the following terms best matches this definition?

- A. Threat
- B. Attack
- C. Risk
- D. Vulnerability
- 64. Your team has won a contract to infiltrate an organi- D. Reconnaiszation. The company wants to have the attack be a re- sance alistic as possible; therefore, they did not provide any information besides the company name. What should be the first step in security testing the client?
  - A. Scanning
  - **B.** Escalation
  - C. Enumeration
  - D. Reconnaissance
- 65. A penetration tester is conducting a port scan on a A. The host is likespecific host. The tester found several ports opened ly a printer.

that were confusing in concluding

the Operating System (OS) version installed. Considering the NMAP

result below, which of the follow is likely to be installed on the

target machine by the OS?

Starting NMAP 5.21 at 2011-O3-15 11:06 NMAP scan report for

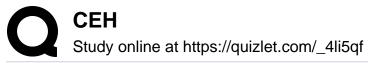
172.16.40.65 Host is up (1.005 latency). Not shown: 993 closed ports

PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tec open ipp 9100/tcp open

MAC Address: OO:00:48:OD:EE:8

- A. The host is likely a printer.
- B. The host is likely a router.
- C. The host is likely a Linux machine.
- D. The host is likely a Windows machine.

A. Botnet Trojan 66.



A hacker has successfully infected an internet-facing server, which he will then use to send junk mail, take part in coordinated attacks, or

hostjunk email content.

Which sort of trojan infects this server?

- A. Botnet Trojan
- **B. Banking Trojans**
- C. Ransomware Trojans
- D. Turtle Trojans
- 67. You have compromised a server and successfully gained a root access.

Telnet to encrypt from this

server.

A. Install and use

You want to pivot and pass traffic undetected over the all outgoing traffic network and

evade any possible Intrusion Detection System.

What is the best approach?

A. Install and use Telnet to encrypt all outgoing traffic from this

server.

- B. Install Cryptcat and encrypt outgoing packets from this server
- C. Use Alternate Data Streams to hide the outgoing packets from this server.
- D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal intrusion **Detection Systems.**
- It is a vulnerability in GNU's bash shell, discovered in A. Shellshock 68. September of

2004, that gives attackers access to run remote commands on a

vulnerable system. The malicious software can take control of an

infected machine, launch denial-of service attacks to disrupt

websites, and scan for other vulnerable devices (including routers).



#### CEH

Study online at https://quizlet.com/\_4li5qf

Which of the following vulnerabilities is being described?

- A. Shellshock
- **B. Rootshock**
- C. Shellbash
- D. Rootshell
- 69. env x= '(){ :;};echo exploit 'bash —c 'cat /etc/passwd B. Display passwd What is the Shellshock bash vulnerability attempting contents to prompt to do on a

vulnerable Linux host?

- A. Add new user to the passwd file
- B. Display passwd contents to prompt
- C. Change all password in passwd
- D. Remove the passwd file.
- 70. Your company was hired by a small healthcare provider to perform a technical assessment on the network.

  What is the best approach for discovering vulnerabil-

tool like Nessus

D. Used a scan

ities on a Windows-based computer?

- A. Use the built-in Windows Update tool
- B. Create a disk image of a clean Windows installation
- C. Check MITRE.org for the latest list of CVE findings
- D. Used a scan tool like Nessus
- 71. To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such as audit?

C. Vulnerability scanner

- A. Port scanner
- **B. Protocol analyzer**
- C. Vulnerability scanner
- **D. Intrusion Detection System**

B. Wireshark

The network administrator contacts you and tells you that she noticed

the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big

conference and she doesn't have time to perform the task.

What tool can you use to view the network traffic being sent and

received by the wireless router?

- A. Netcat
- **B. Wireshark**
- C. Nessus
- D. Netstat
- 73. You are using NMAP to resolve domain names into IP D. >host —t addresses for a a hackeddoping sweep later. main.com

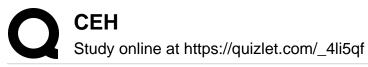
Which of the following commands looks for IP addresses?

- A. >host —t ns hackeddomain.com
- B. >host —t AXFR hackeddomain.com
- C. >host —t soa hackeddomain.com
- D. >host —t a hackeddomain.com
- 74. Which mode of IPSec should you use to assure secu- C. ESP transport rity and con?

dentiality of data within the same LAN?

- A. ESP confidential
- **B. AH Tunnel mode**
- C. ESP transport mode
- D. AH permiscuous
- 75. Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

D. Height and Weight



- A. Iris patterns
- **B.** Voice
- C. Fingerprints
- D. Height and Weight
- 76. When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation. What command will help you to search files using Google as a search engine?

C. site: target.com filetypezxls username password email

- A. site: target.com filezxls username password email
- B. domain: target.com archive:xls username pass-

word email

- C. site: target.com filetypezxls username password email
- D. inurl: target.com filenamezxls username password email
- 77. You have successfully gained access to your client's D. 445 internal network

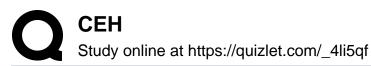
and successfully comprised a linux server which is part of the

internal IP network. You want to know which Microsoft Windows

workstation have the sharing enabled. Which port would you see

listening on these Windows machines in the network?

- A. 1443
- **B.** 3389
- C. 161
- D. 445
- 78. Which of the following parameters describe LM Hash: D. I, II and III I—The maximum password length is 14 characters. II—There are no distinctions between uppercase and lowercase.



III — It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I

B. I and II

C. II

D. I, II and III

- 79. What is the process of logging, recording, and resolv- D. Incident Maning events that agement Process take place in an organization?
  - A. Metrics
  - **B. Security Policy**
  - C. Internal Procedure
  - **D. Incident Management Process**
- 80. A network administrator discovers several unknown D. Directory Trafiles in the root versal directory of his Linux FTP server. One of the files is a tarball, two

are shall script files, and the third is a binary file is named "nc."

The FTP server's access logs show that the anonymous user account

logged in the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP

server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port. Which kind of vulnerability must be

a network port. Which kind of vulnerability must be present to make this remote attack possible?

- A. File system permissions
- **B. Brute Force Login**
- C. Privilege Escalation
- **D. Directory Traversal**
- 81. You are logged in as a local admin on a Windows 7 system and you need

C. c:\compmgmt.msc

### CEH Study online at https://quizlet.com/\_4li5qf

to launch the Computer Management Console from command line.

Which command would you use?

- A. c:\services.msc
- B. c:\ncpa.cp
- C. c:\compmgmt.msc
- D. c:\apedit
- 82. You have successfully comprised a server having an A. Nmap —T4 —F IP address of 10.10.0.0/24

10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best nmap command you will use?

- A. Nmap —T4 —F 10.10.o.o/24
- B. Nmap —T4 —q 10.1o.0.o/24
- c. N map —T4 -o 10.10.0.0/24
- D. Nmap —T4 —r 10.1o.0.0/24
- The "white box testing" methodology enforces what A. The internal opkind of restriction?

A. The internal operation of a system is completely known to the tester.

eration of a system is completely known to the tester.

- B. Only the internal operation of a system is known to the tester.
- C. Only the external operation of a system is accessible to the tester.
- D. The internal operation of a system is only partly accessible to the tester.
- 84. Risk = Threats x Vulnerabilities is referred to as the: D. Risk equation
  - A. Threat assessment
  - B. Disaster recovery formula
  - C. BIA equation
  - D. Risk equation
- 85. An Intrusion Detection System (IDS) has alerted the B. Intrusion Prenetwork administrator to a possibly malicious sequence of

vention System (IPS)

packets went to a

Web server in the network's external DMZ. The packet traffic was

captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

- A. Protocol analyzer
- **B. Intrusion Prevention System (IPS)**
- C. Vulnerability scanner
- D. Network sniffer
- 86. The Open Web Application Security Project (OWASP) A. Injection is the worldwide not-for-profit charitable organization focused on improving the

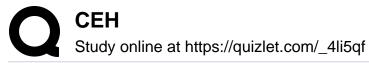
security of software. What item is the primary concern on OWASP's Top

Ten Project most €ritical Web application Security Rules?

- A. Injection
- **B. Cross site Scripting**
- C. Cross site Request Forgery
- **D. Path Disclosure**
- 87. After trying multiple exploits, you've gained root ac- C. Download and cess to a Centos Install Netcat

6 answer. To ensure you maintain access. What would you do first?

- A. Disable IPTables
- **B. Create User Account**
- C. Download and Install Netcat
- D. Disable Key Services
- 88. Which method of password cracking takes the most C. Bruce force time and effect?
  - A. Rainbow Tables
  - B. Shoulder surfing



- C. Bruce force
- D. Directory attack
- 89. Which of the following types of firewalls ensures that B. Stateful inspective the packets are part of the established session?
  - A. Switch-level firewall
  - **B. Stateful inspection firewall**
  - C. Application-level firewall
  - D. Circuit-level firewall
- 90. Which of the following tools is used to detect wireless A. Kismet LANs using the 802.11a/b/g/n WLAN standards on a linux platform?
  - A. Kismet
  - **B.** Netstumbler
  - C. Abel
  - D. Nessus
- 91. Which of the following is the BEST way to defend against network sniffing?

tion protocols to secure network communications

A. Using encryp-

- A. Using encryption protocols to secure network communications
- B. Restrict Physical Access to Server Rooms hosting

**Critical Servers** 

- C. Use Static IP Address
- D. Register all machines MAC Address in a centralized Database
- 92. Session splicing is an IDS evasion technique in which C. Whisker an attacker

delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Which tool can used to perform session splicing attacks?

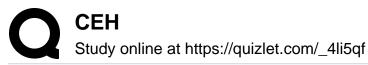
- A. Hydra
- B. Burp
- C. Whisker
- D. Tcpsplice

- 93. During a security audit of IT processes, an IS auditor B. Identify and found that evaluate existing there was no documented security procedures. What practices. should the IS auditor do?
  - A. Terminate the audit.
  - B. Identify and evaluate existing practices.
  - C. Create a procedures document
  - D. Conduct compliance testing
- 94. Which of the following is a low-tech way of gaining B. Social engiunauthorized neering access to systems?
  - A. Sniffing
  - **B. Social engineering**
  - C. Scanning
  - D. Eavesdropping
- 95. Which tool allows analysis and pen testers to exam- B. Maltego ine links between data using graphs and link analysis?
  - A. Metasploit
  - **B.** Maltego
  - C. Wireshark
  - D. Cain & Abel
- 96. You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping but you didn't get any response back. What is happening? A. TCP/IP doesn't support ICMP.

A. TCP/IP doesn't support ICMP.

- B. ICMP could be disabled on the target server.
- C. The ARP is disabled on the target server.
- D. You need to run the ping command with root privileges.
- 97. The security concept of "separation of duties" is most similar to the operation of which type of security device?

C. Firewall



- A. Bastion host
- **B.** Honeypot
- C. Firewall
- **D. Intrusion Detection System**
- The purpose of a is to deny network access to local D. Wireless In-98. area networks and other information assets by unauthorized wireless devices.

trusion Prevention System

- **A. Wireless Access Point**
- **B. Wireless Analyzer**
- C. Wireless Access Control list
- **D. Wireless Intrusion Prevention System**
- 99. You just set up a security system in your network. In C. An Intrusion what kind of **Detection System** system would you find the following string of characters used as a rule within its configuration? alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!";)
  - A. A firewall IPTable
  - **B. A Router IPTable**
  - C. An Intrusion Detection System
  - D. FTP Server rule
- 100. Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening port on the targeted system. If a scanned port is open, what happens? A. The port will ignore the packets.

A. The port will ignore the packets.

- B. The port will send an RST.
- C. The port will send an ACK.
- D. The port will send a SYN.

101. This asymmetry cipther is based on factoring the product of two large prime numbers. What cipher is described above?

C. RSA



### CEH

Study online at https://quizlet.com/ 4li5qf

- A. SHA
- **B. RC5**
- C. RSA
- **D. MD5**
- 102. How does the Address Resolution Protocol (ARP) work?

D. It sends a request packet to all ments, asking for the MAC address

A. It sends a reply packet for a specific IP, asking for the network elethe MAC address.

B. It sends a reply packet to all the network elements, from a specific IP.

asking for the MAC address from a specific IP.

C. It sends a request packet to all the network elements, asking for

the domain name from a specific IP.

D. It sends a request packet to all the network elements, asking for

the MAC address from a specific IP.

103. Which of the following is designed to indentify mali- D. Intrusion Deteccious attempts to penetrate systems?

tion System

- A. Proxy
- **B.** Router
- C. Firewall
- **D. Intrusion Detection System**
- 104. When you return to your desk after a lunch break, you A. Forward the notice a strange email in your inbox. The senders is message to your someone you did business with recently but the subject line has strange characters

company's security response team

in it. What should you do?

permanently

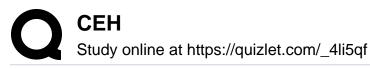
and

A. Forward the message to your company's security delete the response team and

permanently delete the

message from your computer.

- B. Delete the email and pretend nothing happened.
- C. Forward the message to your supervisor and ask



for her opinion on how to handle the situation.

D. Reply to the sender and ask them for more information about the message contents.

105. A common cryptographically tool is the use of XOR. A. 10001011 XOR the following

binary value:

10110001

00111010

A. 10001011

B. 10011101

C. 11011000

D. 10111100

106. A Regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.

A. Move the financial data to another server on the same IP subnet

Based on this information, what should be one of your key

recommendations to the bank?

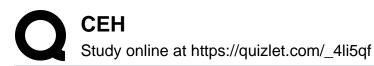
- A. Move the financial data to another server on the same IP subnet
- B. Place a front-end web server in a demilitarized zone that only

handles external web traffic

- C. Issue new certificates to the web servers from the root certificate authority
- D. Require all employees to change their passwords immediately

107. It is a regulation that has a set if guideline, which should be adhered to by anyone who handles any electronic medical data. These

A. HIPAA



guidelines stipulate that all medical practices must ensure that all

necessary measures are in place while saving, accessing, and sharing

any electronic medical data to keep patient data secure.

Which of the following regulations best matches the description?

A. HIPAA

B. COBIT

C. ISO/IEC 27002

D. FISMA

- 108. Which of the following statements regarding ethical B. Ethical hackers hacking is incorrect?
  - A. Testing should be remotely performed offsite.
  - B. Ethical hackers should never use tools that have potential of

exploiting vulnerabilities in the organizations IT sys-nizations IT sys-

C. Ethical hacking should not involve writing to or modifying the target systems.

D. An organization should use ethical hackers who do not sell

hardware/software or other consulting services.

109. Which of the following is considered the best way to A. Use encryptprevent

Personally identifiable information (PII) from web ap- tions protocols to plication

vulnerabilities?

- A. Use encrypted communications protocols to transmit PII
- B. Use full disk encryption on all hard drives to protect PII
- C. Use cryptographic storage to store all PII
- D. Use a security token to log onto into all Web appli-

should never use tools that have potential of exploiting vulnerabilities in the orgatem.

ed communicatransmit PII

## cation that use

110. Under the "Post-attach Phase and Activities," it is the A. III responsibility of the tester to restore the system to a pre-test state.

Which of the following activities should not be included in this

phase?

- I. Removing all files uploaded on the system
- II. Cleaning all registry entries
- III. Mapping of network state
- IV. Removing all tools and maintaining backdoor for reporting
- A. III
- B. IV
- C. III and IV
- D. All should be included.
- 111. Ricardo wants to send secret messages to a competi- B. Steganography tor company. To

secure these messages, he uses a technique of hiding a secret message

within an ordinary message, the technique provides 'security

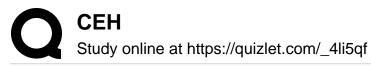
through obscurity'. What technique is Ricardo using?

- A. RSA algorithm
- **B. Steganography**
- C. Encryption
- D. Public-key cryptography
- 112. You have successfully gained access to a linux server B. Encryption and would like

to ensure that the succeeding outgoing traffic from the server will not be caught by a Network Based Intrusion Detection System(NIDS).

Which is the best way to evade the NIDS?

- A. Out of band signaling
- **B.** Encryption



- C. Alternate Data Streams
- D. Protocol Isolation

design problem?

- 113. An attacker gains access to a Web server's database D. insufficient inand display the put validation contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software
  - A. insufficient security management
  - B. insufficient database hardening
  - C. insufficient exception handling
  - D. insufficient input validation
- 114. You are performing a penetration test. You achieved B. Report immediaccess via a buffer overflow exploit and you proceed to find inter- istrator. esting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account. What should you do?
  - A. Do not transfer the money but steal the bitcoins.
  - B. Report immediately to the administrator.
  - C. Transfer money from the administrator's account to another account.
  - D. Do not report it and continue the penetration test.
- 115. Which of the following is a command line packet analyzer similar to **GUI—based Wireshark?**

A. Jack the ripper

B. nessus

C. tcpdump

ately to the admin-

- 116. You are attempting to man-in-the-middle a session. B. TCP Which protocol will allow you to guess a sequence number?
  - A. ICMP
  - B. TCP
  - C. UDP
  - D. UPX
- 117. Which of the following incident handling process phases is responsible for defining rules, creating a back-up plan, and testing the plans for an enterprise?

A. Preparation phase

- A. Preparation phase
- B. Recovery phase
- C. Identification phase
- D. Containment phase
- 118. What term describes the amount of risk that remains B. Residual Risk after the

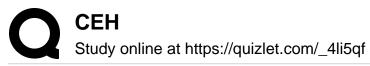
vulnerabilities are classified and the countermeasures have been deployed?

- A. Inherent Risk
- B. Residual Risk
- C. Deferred Risk
- D. Impact Risk
- 119. The "Gray box testing" methodology enforces what D. The internal opkind of restriction?

A. Only the external operation of a system is accessi- tem is only partly ble to the tester.

eration of a sysaccessible to the tester.

- B. Only the internal operation of a system is known to the tester.
- C. The internal operation of a system is completely known to the tester.



- D. The internal operation of a system is only partly accessible to the tester.
- 120. Nation-state threat actors often discover vulnerabili- C. zero-day ties and hold on to them until they want to launch a sophisticated attack. The Stumet attack was an unprecedented style of attack because it used four types of this vulnerability. What is this style of attack called?
  - A. zero-hour
  - B. no-day
  - C. zero-day
  - D. zero-sum
- 121. You are a Network Security Officer. You have two ma- A.
  chines. The first tcp.dstport==514
  machine (192.168.0.99) has snort installed, and the second machine ip.dst==192.168.0.150
  (192.168.0.150) has kiwi syslog installed. You perform

(192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.

What wireshark filter will show the connections from the snort machine to kiwi syslog machine?

- A. tcp.dstport==514 && ip.dst==192.168.0.150
- B. tcp.dstport==514 && ip.dst==192.168.0.99
- C. tcp.srcport==514 && ip.src==192.168.0.99
- D. tcp.srcport==514 && ip.src==192.168.150
- 122. During a recent security assessment, you discover c. Split DNS the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal Network.

  What is this type of DNS configuration commonly called?

  A. DNS Scheme



### CEH

Study online at https://quizlet.com/ 4li5qf

- B. DynDNS
- c. Split DNS
- D. DNSSEC
- 123. A new wireless client is configured to join a 802.11 network. This

C. The WAP does not recognize the

client uses the same hardware and software as many client's MAC adof the other

dre

clients on the network. The client can see the network,

but cannot

connect. A wireless packet sniffer shows that the Wireless Access

Point (WAP) is not responding to the association requests being sent

by the wireless client.

What is a possible source of this problem?

A. The client cannot see the SSID of the wireless network

- B. The wireless client is not configured to use DHCP
- C. The WAP does not recognize the client's MAC address
- D. Client is configured for the wrong channel
- 124. You have several plain-text firewall logs that you must C. Grep review to

evaluate network traffic. You know that in order to do this fast and

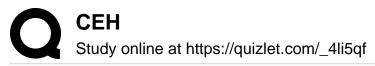
efficiently you must user regular expressions.

Which command-line utility are you most likely to use?

- A. Notepad
- B. MS Excel
- C. Grep
- D. Relational Database
- 125. Initiating an attack against targeted businesses and A. Watering Hole organizations,

Attack

threat actors compromise a carefully selected website by inserting an



exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits. What type of attack is outlined in the scenario?

- A. Watering Hole Attack
- **B. Spear Phishing Attack**
- C. Heartbleed Attack
- D. Shellshock Attack