Linux Professional Institute Security Essentials Exam

1. What type of malware is specifically designed to conceal its existence and activities on a system?

A. Trojan

B. Cryptominer

C. Rootkit

D. Ransomware

Answer(s): C

---

2. Which term describes the ability to prove that a specific individual or entity performed an action, such as sending a message or conducting a transaction?

A. Confidentiality

B. Integrity

C. Availability

D. Non-repudiation

Answer(s): D

---

3. Which of the following backup types only backs up data that has changed since the last backup of any kind?

A. Full backup

B. Differential backup

C. Mirror backup

D. Incremental backup

Answer(s): D

---

4. Which of the following is a characteristic of Perfect Forward Secrecy (PFS)?

A. It is not used in modern encryption protocols.

B. It uses symmetric encryption for all sessions.

C. It generates a unique session key for each session.

D. It relies on a single long-term private key for all sessions.

Answer(s): C

---

5. Which of the following is used to verify the identity of a website?

A. Diffie-Hellman key exchange

B. X.509 digital certificate

C. Certificate Signing Request (CSR)

D. SSL/TLS

Answer(s): B

---

6. You receive an email from an unknown sender claiming to be from your bank. The email includes a link to a website where you are asked to enter your bank account login information. What type of attack is this?

A. Phishing

B. Social engineering

C. Email spam

D. Scareware

Answer(s): A

---

7. Which of the following devices is used to provide wireless connectivity in a network?

A. Modem

B. Router

C. Switch

D. Access Point

Answer(s): D

---

8. You are setting up a Bluetooth connection between your smartphone and a wireless speaker. What security measure should you take to protect your data?

A. Use a strong and unique password for the Bluetooth connection

B. Enable Bluetooth pairing mode on your smartphone

C. Disable Bluetooth after the connection is established

D. Leave the Bluetooth connection open to all nearby devices

Answer(s): A

---

9. Which of the following types of encryption is typically used to secure data in transit only?

A. Transport encryption

B. Intrusion Detection System (IDS)

C. Firewall

D. End-to-end encryption

Answer(s): A

---

10. Which of the following risk management strategies seeks to minimize risk to an acceptable level?

A. Risk avoidance

B. Risk acceptance

C. Risk mitigation

D. Risk transfer

Answer(s): C

---

11. What is the darknet?

A. Cloud Storage

B. A type of network that is only accessible through TOR

C. A type of network that is not connected to the internet

D. A type of network that is used for illegal activities

Answer(s): B

---

12. Which of the following is a key feature of BitLocker?

A. Integrated with Windows

B. Encrypts only files

C. Cross-platform support

D. Free and open-source

Answer(s): A

---

13. You are concerned about your internet activity being tracked by your ISP. Which of the following solutions would be the most appropriate for protecting your privacy?

A. Disabling your firewall

B. Transfer encryption

C. TOR

D. End-to-end encryption

Answer(s): C

---

14. You are concerned about the security of your internet connection while using a public WiFi network, but you do not want to use a VPN. Which of the following solutions would be the most appropriate for protecting your data?

A. Disabling your firewall

B. Transfer encryption

C. Connecting to an open Wi-Fi network

D. A proxy server

Answer(s): B

---

15. You want to access a website that is blocked in your country. Which of the following solutions would be the most appropriate for accessing the website?

A. Network-attached storage

B. A public VPN provider

C. Using an unencrypted public Wi-Fi network

D. Clearing your browser,s cache

Answer(s): B

---

16. Which of the following is a network of compromised devices used to perform malicious activities?

A. DoS

B. Botnet

C. Man in the Middle

D. Traffic interception

Answer(s): B

---

17. What are browser extensions or add-ons that prevent websites from running scripts, which can be used to collect personal information?

A. Cookies

B. Malware protection

C. Ad blockers

D. Script blockers

Answer(s): D

---

18. You receive an email from what appears to be a legitimate company asking you to verify your login credentials by clicking on a link. What is the most likely security risk associated with providing your login information in response to this email?

A. Your data will be encrypted

B. Updating your software

C. Your data may be intercepted through a phishing scam

D. Your data will be securely stored

Answer(s): C

---

19. What is the purpose of a rootkit?

A. To increase network speed

B. To provide remote access to a system

C. To detect and remove malware

D. To encrypt data on a system

Answer(s): B

---

20. Which of the following devices is an example of an IoT device?

A. Desktop computer

B. Printer

C. Router

D. Smartphone

Answer(s): D
