**Security+ Bonus Exam 5**

1. Which access control system allows an administrator to choose the level of access to grant to users?

A. RBAC

B. MAC

C. TBAC

D. DAC

2. Kerberos is an example of which of the following security technologies?

A. Physical access control

B. Monitoring system

C. Single sign-on

D. Authentication factor

3. Sensitivity labels are used by which form of access control?

A. DAC

B. MAC

C. RBAC

D. TBAC

4. When CHAP is used for authentication, how are the passwords transmitted from the client to the authentication server?

A. In hashed form

B. In clear text

C. As a ticket

D. Encrypted with AES

5. The most common form of authentication factor is a \_\_\_\_\_\_\_\_\_\_.

A. Password

B. Fingerprint

C. Smart card

D. Token

6. Which of the following authentication actions is generally the strongest?

A. Three passwords consisting of 50 characters each

B. A password, a fingerprint, and a smartcard

C. Two biometrics and a token

D. A token, a handprint, and an iris scan

7. Which of the following represents the most secure system from a best practices perspective?

A. Removing all unneeded services and protocols

B. Using a new operating system right out of the box

C. Installing every available optional component

D. Using a firewall to provide boundary protection

8. As data is transmitted from one system to another across a VPN link, the normal LAN TCP/IP traffic is \_\_\_\_\_\_\_\_\_\_ the VPN protocol.

A. Replaced by

B. Converted into

C. Hashed with

D. Encapsulated in

9. TACACS, a solution similar to RADIUS, is based on what RFC?

A. RFC 1918

B. RFC 2828

C. RFC 1492

D. RFC 1087

10. SSH is considered a secure replacement for \_\_\_\_\_\_\_\_\_\_.

A. TFTP

B. VPN

C. SSL

D. Telnet

.

11. Which of the following is not true in regard to S/MIME?

A. Employs asymmetric cryptography

B. Provides email confidentiality

C. Supports interoperability with a wide range of security solutions

D. Can be used to digitally sign emails

12. Why is Internet email so vulnerable to attack?

A. It uses IP addresses to route messages.

B. Anyone can use email.

C. It requires adherence to standards.

D. It’s sent using SMTP in clear form.

13. You’ve just received an email message that describes a new malicious code threat that’s ravaging the Internet. The message contains detailed information about the threat, describes the damage it can inflict, and provides instructions on how to remove it from your system. The message states that you can easily detect whether you’ve already been a victim of this threat by checking for the presence of three files in the \Windows\System32 folder. As a countermeasure, the message instructs you to delete these three files from your system to prevent further spread of the threat. What should your first action be, based on this message?

A. Locate and delete the identified files.

B. Perform a system backup.

C. Inform your network administrator.

D. Send the message to others in the office.

14. What type of security zone can be positioned so it operates as a buffer network between the secured private network and the Internet and can host publicly accessible services?

A. Honeypot

B. DMZ

C. Extranet

D. Intranet

15. Which of the following technologies enables numerous internal clients to access the Internet over a few leased public IP addresses?

A. SSL

B. L2TP

C. SSH

D. NAT

16. Which of the following is a common example of a host-based IDS that uses signature detection?

A. Firewall

B. Padded cell

C. Virus scanner

D. Penetration testing

17. A honeypot is used to do what?

A. Encourage security policy compliance.

B. Test the security perimeter of a network.

C. Establish a secured communication link across an untrusted network.

D. Lure and detain intruders.

18. Which of the following is not an essential element in locking down a server?

A. Remove unneeded components.

B. Install updates and patches.

C. Perform user awareness training.

D. Configure the system according to company standards and baselines.

19. The basis of application server hardening depends primarily on \_\_\_\_\_\_\_\_\_\_.

A. The function of the server

B. The number of users

C. The size of the average resource transmitted

D. Local versus remote access

20. Which of the following is not a form of asymmetric cryptography?

A. RSA

B. Diffie-Hellman

C. Blowfish

D. ElGamal

21. Certificates operate under the security concept of \_\_\_\_\_\_\_\_\_\_.

A. Principle of least privilege

B. Trusted third party

C. Separation of duties

D. Need to know

22. When will a certificate authority (CA) be likely to revoke a certificate?

A. When the subject profits from the use of the certificate

B. When the subject requests a suspension

C. When the subject obtains certificates from other CAs

D. When the subject changes its identity

23. In order to prevent any one administrator from taking full control over a cryptography system or performing fraud, which of the following solutions should not be implemented?

A. M of N control

B. Job rotation

C. Multiple key pairs

D. Separation of duties

24. Which of the following physical control mechanisms will serve to delay an intruder once their presence is detected?

A. Mantrap

B. Security cameras

C. Fencing

D. Guard dogs

25. The technology used to prevent EMI from entering or leaving a specific room is known as \_\_\_\_\_\_\_\_\_\_.

A. Padded cell

B. TEMPEST

C. Site surveys

D. Directory service

26. The act of falsifying data is also known as \_\_\_\_\_\_\_\_\_\_\_.

A. Impersonation

B. Spoofing

C. Social engineering

D. Replay

27. The purpose of a replay attack is \_\_\_\_\_\_\_\_\_\_\_.

A. Intercepting encrypted data

B. Preventing a server from responding to legitimate resource requests

C. Discovering passwords

D. Gaining access to resources based on a user’s credentials

28. When a cryptography solution uses keys that are easily guessed due to their short length, this allows for a form of attack known as \_\_\_\_\_\_\_\_\_\_\_.

A. Eavesdropping attack

B. Birthday attack

C. Social engineering attack

D. Spoofing attack

29. Birthday attacks can focus on what?

A. Asymmetric keys

B. Digital certificates

C. Hashing

D. Encrypted files

30. The form of password attack that attempts to process every possible combination to discover passwords stored in an accounts database is known as what?

A. Dictionary attack

B. Brute force attack

C. Birthday attack

D. Mathematical attack

31. One of the most common forms of Trojan horse is used to do what?

A. Perform man-in-the-middle attacks.

B. Distribute worms.

C. Plant DoS zombies.

D. Perform dictionary attacks.

32. Which of the following could not be classified as a form of social engineering attack?

A. A user logs in to their workstation and then decides to get a soda from the vending machine in the stairwell. As soon as the user walks away from their workstation, another person sits down at their desk and copies all the files from a local folder onto a network share.

B. You receive an email warning about a dangerous new virus spreading across the Internet. The message tells you to look for a specific file on your hard drive and delete it, since it indicates the presence of the virus.

C. A website claims to offer free temporary access to their products and services but requires that you alter the configuration of your web browser and/or firewall in order to download the access software.

D. A secretary receives a phone call from a person claiming to be a client who is running late to meet the CEO. The caller asks for the CEO’s private cell phone number so she can call him.

33. Which of the following is a form of web security that encrypts web sessions for modern web servers and browsers?

A. SSH

B. S-HTTP

C. TLS

D. IPSec

34. Which of the following is a form of malicious code injection attack where an attacker is able to compromise a web server and inject their own malicious code into the content sent to other visitors?

A. Cross-site scripting

B. Form field manipulation

C. Birthday attack

D. Spoofing attack

35. Cookies pose a risk to \_\_\_\_\_\_\_\_\_\_\_.

A. Network infrastructure

B. Privacy

C. Physical security

D. Access control

36. Which of the following features commonly found on a mobile phone may prevent an unauthorized thief from gaining access to sensitive information?

A. Screen lock

B. Storage device encryption

C. Remote wipe

D. GPS tracking

37. Which of the following is not a benefit of SFTP?

A. It is interoperable with other FTP solutions.

B. It provides logon credential protection.

C. It encrypts data traffic.

D. It uses SSH to provide security.

38. Because FTP doesn’t offer security, what attack is it vulnerable to?

A. Birthday

B. Packet sniffing

C. Replay

D. Social engineering

39. A new wireless access point has been installed in your office. You wish to determine what areas of the office receive the strongest and weakest signals as well as whether the access point can be reached from outside of your office. This activity is known as what?

A. A site survey

B. Penetration testing

C. Risk assessment

D. Business continuity planning

40. The best defense against spoofed network traffic is \_\_\_\_\_\_\_\_\_\_\_.

A. An ingress filter

B. A switch

C. A web server

D. Kerberos

41. Which of the following is not a valid PBX fraud and abuse countermeasure?

A. Change default accounts.

B. Disable maintenance modems.

C. Require photo IDs.

D. Enable logging.

42. The computer systems used by people to interact with a network can be called \_\_\_\_\_\_\_\_\_\_\_.

A. Workstations

B. Proxies

C. Servers

D. Telecoms

43. What hacker technique can be used over a network connection to discover the identity of services active on a computer system?

A. Port scanning

B. Banner grabbing

C. Sniffing

D. ARP poisoning

44. What form of removable media is best suited for backups that are to be used in disaster recovery processes?

A. CD

B. Diskette

C. Flash memory cards

D. Tape

45. Hashing is used for what primary purpose?

A. Integrity verification

B. Digital envelopes

C. Data encryption

D. Authentication

46. What is the size of an SHA-1 hash output?

A. 160 bits

B. 128 bits

C. 192 bits

D. 56 bits

47. Which of the following is not an example of symmetric cryptography?

a. AES

b. Blowfish

c. CAST-128

d. RSA

48. Which symmetric algorithm supports a key size of 0 bits?

A. RC5

B. IDEA

C. Twofish

D. AES

49. The basis of a reliable disaster recovery and business continuity plan is \_\_\_\_\_\_\_\_\_\_\_.

A. User awareness

B. A warm alternate site

C. Backups

D. Redundant hardware

50. Which of the following is not an example of a high-availability solution?

A. Offsite real-time backups

B. RAID

C. Server clustering

D. Switched networking

51. Which of the following is not part of the CIA triad?

A. Confidentiality

B. Integrity

C. Availability

D. Authentication

52. Which of the following is equivalent to the protection of privacy?

A. Confidentiality

B. Integrity

C. Availability

D. Authentication

53. Which of the following describes a community cloud?

A. A cloud environment maintained, used, and paid for by a group of users or organizations for their shared benefit, such as collaboration and data exchange.

B. A cloud service within a corporate network and isolated from the Internet.

C. A cloud service that is accessible to the general public typically over an Internet connection.

D. A cloud service that is partially hosted within an organization for private use and which uses external services to offer recourses to outsiders.

54. After checking into your hotel room, you attempt to connect to the Internet over the free WiFi network. You are prompted by a hotel logo screen to agree to terms of service and provide both your room number and your last name. Once you complete the request, you are able to access the Internet. This procedure is known as?

A. captive portal

B. on-boarding

C. DHCP reservation

D. formal enrollment

55. \_\_\_\_\_\_\_\_\_\_\_\_ are formal contracts (or at least written documents) that define some form of arrangements where two entities agree to work with each other in some capacity. This could be an agreement between a supplier and customer or between equals.

A. Service level agreement

B. Business Partners Agreement

C. Interoperability agreements

D. Memorandum of Understanding

56. Which of the following is not typically a legal agreement or commitment, but rather a more formal form of a reciprocal agreement or gentleman's handshake (neither of which is typically written down), and can be called a "letter of intent"?

A. MOU

B. ISA

C. SLA

D. BPA

57. You attempt to visit Amazon.com but mistakenly type amazin.com. The web site you see is an obvious rip-off of the valid online merchant. This situation can be called?

A. Watering hole attack

B. Typo squatting

C. Rainbow tables

D. Spear phishing

58. By what means can a flaw in WPS be attacked in order for an unauthorized device to be able to connect into an otherwise secure wireless network?

A. Use a deauthorization flood

B. Operate an evil twin

C. Guess the activation PIN

D. Perform war chalking

59. Which of the following is not true in regards to a NoSQL DBMS?

A. NoSQL uses a non-relational database structure, such as hierarchical or multi-level nesting/referencing.

B. NoSQL cannot support structured query language expressions.

C. NoSQL is well suited for managing extremely large collections of data.

D. NoSQL solutions typically does not support ACID.

60. Which of the following is more closely associated with client-side validation rather than server side validation?

A. Protecting a system against input submitted by a malicious user.

B. Filter for known scriptable or malicious content (such as SQL commands or script calls)

C. Block meta-characters

D. Providing better response or feedback to the typical user

61. Data is not always stored statically on a storage device. Thus, a range of security mechanisms are needed to provide reasonable protection over a range of events and circumstances. Which of the following is not a true statement?

A. Data in-transit is data being communicated over a network connection.

B. Session encryption should be used to protect data in-transit.

C. Storage encryption, such as file encryption or whole drive encryption, should be used to protect data at-rest.

D. Data in-use should be protected against disclosure with hashing.

62. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are devices or applications that generate passwords not based on fixed time intervals but instead generates passwords based on a non-repeating one-way function, such as a hash or HMAC (hash message authentication code) (i.e. a type of hash that used a symmetric key in the hashing process) operation.

A. SCADA

B. CHAP

C. HOTP

D. FCoE

63. Why should generic, anonymous, or group accounts be prohibited?

A. No support for multi-factor authentication

B. Not supported by LDAP

C. Inability to hold individuals accountable

D. Requires the use of a TPM

64. Which of the following is considered the least secure?

A. Out-of-band key exchange

B. ECDHE key exchange

C. In-band key exchange

D. One-time pad based keys

65. A cipher suite is?

A. A standardized collection of authentication, encryption, and hashing algorithms used to set or define the parameters for a security network communication.

B. A communication tunnelbetween two entities across an intermediary network.

C. A storage process by which copies of private keys and/or secret keys are retained by a centralized management system.

D. A process by which one communication is hidden inside another communication.

**Security+ Bonus Exam 5  
Answers & Explanations**

1. Which access control system allows an administrator to choose the level of access to grant to users?

A. RBAC

B. MAC

C. TBAC

D. DAC

Answer: D

DAC (discretionary access control) is based on the discretion of a user (that is, the administrator). RBAC (role-based access control), MAC (media/mandatory access control), and TBAC (task-based access control) are based on rules: job descriptions, classifications, and work tasks, respectively.

2. Kerberos is an example of which of the following security technologies?

A. Physical access control

B. Monitoring system

C. Single sign-on

D. Authentication factor

Answer: C

Kerberos is an example of a single sign-on security technology. It isn’t an example of any of the other security technologies listed here. A mantrap is an example of a physical access control device. Auditing is an example of a monitoring system. A password is an example of an authentication factor.

3. Sensitivity labels are used by which form of access control?

A. DAC

B. MAC

C. RBAC

D. TBAC

Answer: B

MAC (media/mandatory access control) uses sensitivity labels. DAC (discretionary access control) uses identity. RBAC (role-based access control) uses job descriptions. TBAC (task-based access control) uses work tasks.

4. When CHAP is used for authentication, how are the passwords transmitted from the client to the authentication server?

A. In hashed form

B. In clear text

C. As a ticket

D. Encrypted with AES

Answer: A

CHAP (Challenge Handshake Authentication Protocol) uses MD5 to hash passwords before transmission. PAP (Password Authentication Protocol) sends passwords in the clear. Kerberos uses tickets. AES (Advanced Encryption Standard) is an encryption algorithm that isn’t used by CHAP.

5. The most common form of authentication factor is a \_\_\_\_\_\_\_\_\_\_.

A. Password

B. Fingerprint

C. Smart card

D. Token

Answer: A

A password is the most common form of authentication. Fingerprints, smart cards, and tokens are widely used, but they aren’t the most widely used forms of authentication.

6. Which of the following authentication actions is generally the strongest?

A. Three passwords consisting of 50 characters each

B. A password, a fingerprint, and a smartcard

C. Two biometrics and a token

D. A token, a handprint, and an iris scan

Answer: B

Multifactor authentication, which uses different factors, is always stronger than using fewer different factors or multiples of one factor.

7. Which of the following represents the most secure system from a best practices perspective?

A. Removing all unneeded services and protocols

B. Using a new operating system right out of the box

C. Installing every available optional component

D. Using a firewall to provide boundary protection

Answer: A

The best solution is to remove all unneeded services and protocols. Using an operating system right out of the box and installing all components are never considered secure options. Adding a firewall to a locked-down system is a security improvement but not a valid replacement for first removing things that aren’t needed on the server.

8. As data is transmitted from one system to another across a VPN link, the normal LAN TCP/IP traffic is \_\_\_\_\_\_\_\_\_\_ the VPN protocol.

A. Replaced by

B. Converted into

C. Hashed with

D. Encapsulated in

Answer: D

As data is transmitted from one system to another across a VPN (virtual private network) link, the normal LAN (large area network) TCP/IP (Transmission Control Protocol/Internet Protocol) traffic is encapsulated in the VPN protocol.

9. TACACS, a solution similar to RADIUS, is based on what RFC?

A. RFC 1918

B. RFC 2828

C. RFC 1492

D. RFC 1087

Answer: C

TACACS (Terminal Access Controller Access Control System) is based on RFC 1492. RFC 1918 defines private IP (Internet Protocol) addresses. RFC 2828 is the Internet security glossary. RFC 1087 is the ethics and the Internet document.

10. SSH is considered a secure replacement for \_\_\_\_\_\_\_\_\_\_.

A. TFTP

B. VPN

C. SSL

D. Telnet

Answer: D

SSH (Secure Shell) is considered a secure replacement for Telnet. SSH isn’t a replacement for TFTP (Trivial File Transfer Protocol). VPN (virtual private network) and SSL (Secure Sockets Layer) are already secure.

11. Which of the following is not true in regard to S/MIME?

A. Employs asymmetric cryptography

B. Provides email confidentiality

C. Supports interoperability with a wide range of security solutions

D. Can be used to digitally sign emails

Answer: C

S/MIME (Secure/Multipurpose Internet Mail Extensions) only works with other S/MIME products. It isn’t interoperable with other cryptographic email solutions. S/MIME employs asymmetric cryptography, provides email confidentiality, and can be used to digitally sign emails.

12. Why is Internet email so vulnerable to attack?

A. It uses IP addresses to route messages.

B. Anyone can use email.

C. It requires adherence to standards.

D. It’s sent using SMTP in clear form.

Answer: D

Email is vulnerable to attack because it uses SMTP (Simple Mail Transfer Protocol) and sends messages in clear form. Email’s use of IP addresses via the domain names found in email addresses, the fact that anyone can use email, and the fact that it requires adherence to standards doesn’t make email any more vulnerable than any other form of TCP/IP application.

13. You’ve just received an email message that describes a new malicious code threat that’s ravaging the Internet. The message contains detailed information about the threat, describes the damage it can inflict, and provides instructions on how to remove it from your system. The message states that you can easily detect whether you’ve already been a victim of this threat by checking for the presence of three files in the \Windows\System32 folder. As a countermeasure, the message instructs you to delete these three files from your system to prevent further spread of the threat. What should your first action be, based on this message?

A. Locate and delete the identified files.

B. Perform a system backup.

C. Inform your network administrator.

D. Send the message to others in the office.

Answer: C

The best first response to a hoax message such as this is to inform your network administrator. Performing a system backup isn’t a bad idea, just not the best choice for your first response. Don’t follow the instructions or send the message to others.

14. What type of security zone can be positioned so it operates as a buffer network between the secured private network and the Internet and can host publicly accessible services?

A. Honeypot

B. DMZ

C. Extranet

D. Intranet

Answer: B

A DMZ (demilitarized zone) is a type of security zone that can be positioned so it operates as a buffer network between the secured private network and the Internet and can host publicly accessible services. A honeypot is a false network used to trap intruders; it isn’t used to host public services. An extranet is for limited partner access, not public. An intranet is the private secured network.

15. Which of the following technologies enables numerous internal clients to access the Internet over a few leased public IP addresses?

A. SSL

B. L2TP

C. SSH

D. NAT

Answer: D

NAT (network address translation) enables numerous internal clients to access the Internet over a few leased public IP addresses. SSL (Secure Sockets Layer) is a security solution often used on web servers. L2TP (Layer 2 Tunneling Protocol) is a VPN (virtual private network) protocol. SSH (Secure Shell) is a secure replacement for Telnet.

16. Which of the following is a common example of a host-based IDS that uses signature detection?

A. Firewall

B. Padded cell

C. Virus scanner

D. Penetration testing

Answer: C

A virus scanner is a common example of a host-based IDS (intrusion detection system) that uses signature detection. Firewalls, padded cells, and penetration testing aren’t forms of IDS.

17. A honeypot is used to do what?

A. Encourage security policy compliance.

B. Test the security perimeter of a network.

C. Establish a secured communication link across an untrusted network.

D. Lure and detain intruders.

Answer: D

A honeypot is used to lure and detain intruders. Awareness training is used to encourage security policy compliance. Penetration testing is used to test the security perimeter of a network. A VPN (virtual private network) is used to establish a secured communication link across an untrusted network.

18. Which of the following is not an essential element in locking down a server?

A. Remove unneeded components.

B. Install updates and patches.

C. Perform user awareness training.

D. Configure the system according to company standards and baselines.

Answer: C

User awareness training is an essential part of security, but it isn’t directly related to locking down a server. Server lockdown should include removing unneeded components, installing updates and patches, and complying with company standards and baselines.

19. The basis of application server hardening depends primarily on \_\_\_\_\_\_\_\_\_\_.

A. The function of the server

B. The number of users

C. The size of the average resource transmitted

D. Local versus remote access

Answer: A

The basis of application server hardening depends primarily on the function of the server. The number of users, the size of transmissions, and whether users access the server locally or remotely are at best secondary issues.

20. Which of the following is not a form of asymmetric cryptography?

A. RSA

B. Diffie-Hellman

C. Blowfish

D. ElGamal

Answer: C

Blowfish is symmetric. RSA (Rivest, Shamir, and Adleman), Diffie-Hellman, and ElGamal are asymmetric.

21. Certificates operate under the security concept of \_\_\_\_\_\_\_\_\_\_.

A. Principle of least privilege

B. Trusted third party

C. Separation of duties

D. Need to know

Answer: B

Certificates operate under the security concept of trusted third party. Certificates aren’t associated with the principle of least privilege, separation of duties, or need to know.

22. When will a certificate authority (CA) be likely to revoke a certificate?

A. When the subject profits from the use of the certificate

B. When the subject requests a suspension

C. When the subject obtains certificates from other CAs

D. When the subject changes its identity

Answer: D

A CA will revoke a certificate when the subject’s identity changes. The CA isn’t likely to revoke when the subject profits, at a request for a suspension, or when the subject obtains certificates from other CAs.

23. In order to prevent any one administrator from taking full control over a cryptography system or performing fraud, which of the following solutions should not be implemented?

A. M of N control

B. Job rotation

C. Multiple key pairs

D. Separation of duties

Answer: B

Job rotation isn’t appropriate in this situation since it trains a single person to perform all administrative tasks and therefore provides each person with the ability to overrun the entire system. M of N controls, multiple key pairs, and separation of duties should be used to prevent a single person from compromising the entire system.

24. Which of the following physical control mechanisms will serve to delay an intruder once their presence is detected?

A. Mantrap

B. Security cameras

C. Fencing

D. Guard dogs

Answer: A

A mantrap will delay an intruder once their presence is detected. Security cameras, fencing, and guard dogs aren’t guaranteed to delay an intruder to keep them from escaping.

25. The technology used to prevent EMI from entering or leaving a specific room is known as \_\_\_\_\_\_\_\_\_\_.

A. Padded cell

B. TEMPEST

C. Site surveys

D. Directory service

Answer: B

TEMPEST is the technology used to prevent EMI (electromagnetic interference) from entering or leaving a specific room. A padded cell is used to delay an intruder with a fake environment while their activities are logged. Site surveys are used to detect where the signal from a wireless access point can be detected. A directory service is a searchable index of network resources.

26. The act of falsifying data is also known as \_\_\_\_\_\_\_\_\_\_\_.

A. Impersonation

B. Spoofing

C. Social engineering

D. Replay

Answer: B

The act of falsifying data is also known as spoofing. Impersonation is the assumption of another user’s identity. Social engineering involves convincing someone to perform a restricted activity or reveal confidential information. Replay attacks occur when authentication traffic is captured and retransmitted.

27. The purpose of a replay attack is \_\_\_\_\_\_\_\_\_\_\_.

A. Intercepting encrypted data

B. Preventing a server from responding to legitimate resource requests

C. Discovering passwords

D. Gaining access to resources based on a user’s credentials

Answer: D

The purpose of a replay attack is to gain access to resources based on a user’s credentials. A replay attack isn’t used to intercept encrypted data, prevent a server from responding to legitimate resource requests, or discover passwords.

28. When a cryptography solution uses keys that are easily guessed due to their short length, this allows for a form of attack known as \_\_\_\_\_\_\_\_\_\_\_.

A. Eavesdropping attack

B. Birthday attack

C. Social engineering attack

D. Spoofing attack

Answer: B

When a cryptography solution uses keys that are short, this allows for a form of attack known as a birthday attack. Eavesdropping, social engineering, and spoofing aren’t directly associated with cryptography attacks.

29. Birthday attacks can focus on what?

A. Asymmetric keys

B. Digital certificates

C. Hashing

D. Encrypted files

Answer: C

Birthday attacks can focus on hashing. Mathematical and social engineering attacks focus on asymmetric keys and encrypted files. Intrusions to certificate authorities (CAs) may be used against digital certificates.

30. The form of password attack that attempts to process every possible combination to discover passwords stored in an accounts database is known as what?

A. Dictionary attack

B. Brute force attack

C. Birthday attack

D. Mathematical attack

Answer: B

A brute force password attack attempts to process every possible combination to discover passwords stored in an accounts database. A dictionary attack is similar but uses a predefined set or list of passwords rather than every possible combination. A birthday attack (reverse hash matching) is a process most password attacks use, but it doesn’t imply that all possible password combinations are tried. A mathematical attack attempts to exploit the algorithm of a cryptography solution; it’s usually not associated with password attacks.

31. One of the most common forms of Trojan horse is used to do what?

A. Perform man-in-the-middle attacks.

B. Distribute worms.

C. Plant DoS zombies.

D. Perform dictionary attacks.

Answer: C

One of the most common forms of Trojan horse is used to plant DoS (denial-of-service) zombies. Trojan horses aren’t often used to perform man-in-the-middle attacks, distribute worms, or perform dictionary attacks.

32. Which of the following could not be classified as a form of social engineering attack?

A. A user logs in to their workstation and then decides to get a soda from the vending machine in the stairwell. As soon as the user walks away from their workstation, another person sits down at their desk and copies all the files from a local folder onto a network share.

B. You receive an email warning about a dangerous new virus spreading across the Internet. The message tells you to look for a specific file on your hard drive and delete it, since it indicates the presence of the virus.

C. A website claims to offer free temporary access to their products and services but requires that you alter the configuration of your web browser and/or firewall in order to download the access software.

D. A secretary receives a phone call from a person claiming to be a client who is running late to meet the CEO. The caller asks for the CEO’s private cell phone number so she can call him.

Answer: A

The activity described in choice A is a form of tailgating or impersonation. The activities described in selections B, C, and D are all examples of social engineering attacks.

33. Which of the following is a form of web security that encrypts web sessions for modern web servers and browsers?

A. SSH

B. S-HTTP

C. TLS

D. IPSec

Answer: C

TLS (transport layer security) is the primary form of security used on modern web servers and browsers to encrypt web sessions. SSH (Secure Shell) and IPSec (Internet Protocol Security) are not directly related to web sessions. S-HTTP (Secure HTTP) is a legacy security protocol that is no longer supported by most web servers and browsers.

34. Which of the following is a form of malicious code injection attack where an attacker is able to compromise a web server and inject their own malicious code into the content sent to other visitors?

A. Cross-site scripting

B. Form field manipulation

C. Birthday attack

D. Spoofing attack

Answer: A

Cross-site scripting is a form of malicious code injection attack where an attacker is able to compromise a web server and inject their own malicious code into the content sent to other visitors. Form field manipulation occurs when an attack changes elements in a web document on the client side, before submitting results back to the web server. A birthday attack is associated with hashing. Spoofing is falsifying source information.

35. Cookies pose a risk to \_\_\_\_\_\_\_\_\_\_\_.

A. Network infrastructure

B. Privacy

C. Physical security

D. Access control

Answer: B

Cookies pose a risk to privacy. They don’t pose a risk to network infrastructure, physical security, or access control.

36. Which of the following features commonly found on a mobile phone may prevent an unauthorized thief from gaining access to sensitive information?

A. Screen lock

B. Storage device encryption

C. Remote wipe

D. GPS tracking

Answer: C

A remote wipe may allow you to remove all device contents once the mobile phone is reported missing or stolen. Screen lock is not a true security measure. Storage device encryption is not a common feature of mobile phones. GPS tracking will not prevent access to sensitive information.

37. Which of the following is not a benefit of SFTP?

A. It is interoperable with other FTP solutions.

B. It provides logon credential protection.

C. It encrypts data traffic.

D. It uses SSH to provide security.

Answer: A

SFTP (Secure FTP) isn’t interoperable with other FTP solutions; only SFTP clients can interact with SFTP servers. SFTP provides logon credential protection, encrypts data traffic, and uses SSH (Secure Shell) to provide security.

38. Because FTP doesn’t offer security, what attack is it vulnerable to?

A. Birthday

B. Packet sniffing

C. Replay

D. Social engineering

Answer: B

FTP is vulnerable to packet sniffing attacks. Birthday attacks focus on hashing. Replay attacks focus on encrypted authentication traffic. Social engineering attacks focus on people rather than technology.

39. A new wireless access point has been installed in your office. You wish to determine what areas of the office receive the strongest and weakest signals as well as whether the access point can be reached from outside of your office. This activity is known as what?

A. A site survey

B. Penetration testing

C. Risk assessment

D. Business continuity planning

Answer: A

This activity is known as a site survey. Penetration testing uses cracking tools to test a security perimeter. Risk assessment evaluates the risks of a secured environment. Business continuity planning is used to support business operations when processes are threatened.

40. The best defense against spoofed network traffic is \_\_\_\_\_\_\_\_\_\_\_.

A. An ingress filter

B. A switch

C. A web server

D. Kerberos

Answer: A

The best defense against spoofed network traffic is an ingress filter. A switch is used to connect individual systems or subnets together. A web server is used to distribute web content. Kerberos is an authentication system. None of these other three items addresses spoofed network traffic.

41. Which of the following is not a valid PBX fraud and abuse countermeasure?

A. Change default accounts.

B. Disable maintenance modems.

C. Require photo IDs.

D. Enable logging.

Answer: C

Requiring photo IDs isn’t a valid countermeasure to PBX (private branch exchange) fraud and abuse. Valid countermeasures are changing default accounts, disabling maintenance modems, and enabling logging.

42. The computer systems used by people to interact with a network can be called \_\_\_\_\_\_\_\_\_\_\_.

A. Workstations

B. Proxies

C. Servers

D. Telecoms

Answer: A

The computer systems used by people to interact with a network are known as workstations. Proxies mediate access to untrusted networks for clients in a private network. Servers host services that are accessed by users from workstations. A telecom is a speaker phone–like feature of some PBX (private branch exchange) systems.

43. What hacker technique can be used over a network connection to discover the identity of services active on a computer system?

A. Port scanning

B. Banner grabbing

C. Sniffing

D. ARP poisoning

Answer: B

Banner grabbing may reveal the identity of a service when used against an open port across a network connection. Port scanning is used to determine whether ports are open or closed. Sniffing is used to collect network traffic to reveal the contents of the headers and non-encrypted payloads. ARP (Address Resolution Protocol) poisoning is used to trick a switch into rerouting traffic.

44. What form of removable media is best suited for backups that are to be used in disaster recovery processes?

A. CD

B. Diskette

C. Flash memory cards

D. Tape

Answer: D

Tape is the best form of removable media for backups that are to be used in disaster recovery processes. CDs, diskettes, and flash memory cards often don’t have sufficient capacity to be suitable for backups.

45. Hashing is used for what primary purpose?

A. Integrity verification

B. Digital envelopes

C. Data encryption

D. Authentication

Answer: A

Hashing is used primarily for integrity verification. Digital envelopes are produced using asymmetric encryption, not hashing. Data encryption is performed using symmetric encryption or asymmetric encryption. Authentication can be provided for by symmetric encryption or asymmetric encryption.

46. What is the size of an SHA-1 hash output?

A. 160 bits

B. 128 bits

C. 192 bits

D. 56 bits

Answer: A

SHA-1’s hash output is 160 bits. MD5, MD4, and MD2 produce 128-bit hash output.

47. Which of the following is not an example of symmetric cryptography?

a. AES

b. Blowfish

c. CAST-128

d. RSA

Answer: D

RSA is asymmetric. AES, Blowfish, and CAST-128 are symmetric.

48. Which symmetric algorithm supports a key size of 0 bits?

A. RC5

B. IDEA

C. Twofish

D. AES

Answer: A

RC5 supports key sizes from 0 to 2048 bits. IDEA supports a key of 128 bits. Twofish supports key sizes from 1 to 256 bits. AES supports key sizes of 128, 192, and 256 bits.

49. The basis of a reliable disaster recovery and business continuity plan is \_\_\_\_\_\_\_\_\_\_\_.

A. User awareness

B. A warm alternate site

C. Backups

D. Redundant hardware

Answer: C

Backups form the basis of a reliable disaster recovery and business continuity plan. User awareness, warm alternate sites, and redundant hardware may improve DRP (disaster recovery planning) and BCP (business continuity planning), but they aren’t essential like backups.

50. Which of the following is not an example of a high-availability solution?

A. Offsite real-time backups

B. RAID

C. Server clustering

D. Switched networking

Answer: D

Switched networking may offer better throughput and bandwidth, and perhaps even some protection against sniffing, but it isn’t a high-availability solution. Offsite real-time backups, RAID (redundant array of independent disks), and server clustering are high-availability solutions.

51. Which of the following is not part of the CIA triad?

A. Confidentiality

B. Integrity

C. Availability

D. Authentication

Answer: D

Authentication is not part of the CIA triad. The CIA triad consists of confidentiality, integrity, and availability.

52. Which of the following is equivalent to the protection of privacy?

A. Confidentiality

B. Integrity

C. Availability

D. Authentication

Answer: A

Confidentiality protection is the equivalent of privacy protection. Integrity, availability, and authentication are all good security concepts, just not equivalent to privacy.

53. Which of the following describes a community cloud?

A. A cloud environment maintained, used, and paid for by a group of users or organizations for their shared benefit, such as collaboration and data exchange.

B. A cloud service within a corporate network and isolated from the Internet.

C. A cloud service that is accessible to the general public typically over an Internet connection.

D. A cloud service that is partially hosted within an organization for private use and which uses external services to offer recourses to outsiders.

Answer: A

A community cloud is a cloud environment maintained, used, and paid for by a group of users or organizations for their shared benefit, such as collaboration and data exchange. A private cloud is a cloud service within a corporate network and isolated from the Internet. A public could is a cloud service that is accessible to the general public typically over an Internet connection. A hybrid cloud is a cloud service that is partially hosted within an organization for private use and which uses external services to offer recourses to outsiders.

54. After checking into your hotel room, you attempt to connect to the Internet over the free WiFi network. You are prompted by a hotel logo screen to agree to terms of service and provide both your room number and your last name. Once you complete the request, you are able to access the Internet. This procedure is known as?

A. captive portal

B. on-boarding

C. DHCP reservation

D. formal enrollment

Answer: A

A captive portal is an authentication technique that redirects a newly connected wireless Web client to a portal access control page. The portal page may require the user to input payment information, provide logon credentials, or input an access code.

55. \_\_\_\_\_\_\_\_\_\_\_\_ are formal contracts (or at least written documents) that define some form of arrangements where two entities agree to work with each other in some capacity. This could be an agreement between a supplier and customer or between equals.

A. Service level agreement

B. Business Partners Agreement

C. Interoperability agreements

D. Memorandum of Understanding

Answer: C

Interoperability agreements are formal contracts (or at least written documents) that define some form of arrangements where two entities agree to work with each other in some capacity. This could be an agreement between a supplier and customer or between equals. A SLA (Service Level Agreement) is a contract between a supplier and a customer. A BPA (Business Partners Agreement) is a contract between two entities dictating their business relationship. A MOU (Memorandum of Understanding) is an expression of agreement or aligned intent, will, or purpose between two entities.

56. Which of the following is not typically a legal agreement or commitment, but rather a more formal form of a reciprocal agreement or gentleman's handshake (neither of which is typically written down), and can be called a "letter of intent"?

A. MOU

B. ISA

C. SLA

D. BPA

Answer: A

A MOU (Memorandum of Understanding) is an expression of agreement or aligned intent, will, or purpose between two entities. An MOU is not typically a legal agreement or commitment, but rather a more formal form of a reciprocal agreement or gentleman's handshake (neither of which is typically written down). An MOU can also be called a "letter of intent".

57. You attempt to visit Amazon.com but mistakenly type amazin.com. The web site you see is an obvious rip-off of the valid online merchant. This situation can be called?

A. Watering hole attack

B. Typo squatting

C. Rainbow tables

D. Spear phishing

Answer: B

Typo squatting or URL hijacking is a practice employed to capture traffic when a user mis-types the domain name or IP address of an intended resource. A squatter will predict URL typos and then register those domain names to direct traffic to their own site.

58. By what means can a flaw in WPS be attacked in order for an unauthorized device to be able to connect into an otherwise secure wireless network?

A. Use a deauthorization flood

B. Operate an evil twin

C. Guess the activation PIN

D. Perform war chalking

Answer: C

WPS (WiFi Protected Setup) is a security standard for wireless networks. It was intended to simply the effort involved in adding new clients to a well-secured wireless network. It operates by auto-connecting the first new wireless client to seek the network once the administrator triggered the feature by pressing the WPS button on the base station. However, the standard also called for a code which could be sent to the base station remotely in order to trigger WPS negotiation without the need to be able to physically press the button on the base station. This led to a brute force guessing attack that could enable a hacker to guess the WPS code in just hours, which in turned enabled the hacker to connect their own unauthorized system to the wireless network.

59. Which of the following is not true in regards to a NoSQL DBMS?

A. NoSQL uses a non-relational database structure, such as hierarchical or multi-level nesting/referencing.

B. NoSQL cannot support structured query language expressions.

C. NoSQL is well suited for managing extremely large collections of data.

D. NoSQL solutions typically does not support ACID.

Answer: B

Some NoSQL DBMS systems support SQL (structured query language) expressions.

60. Which of the following is more closely associated with client-side validation rather than server side validation?

A. Protecting a system against input submitted by a malicious user.

B. Filter for known scriptable or malicious content (such as SQL commands or script calls)

C. Block meta-characters

D. Providing better response or feedback to the typical user

Answer: D

Client-side validation is better suited for providing better response or feedback to the typical user. While, server-side validation is better suited for protecting system against input submitted by a malicious user, such as filtering for known scriptable or malicious content (such as SQL commands or script calls) and blocking meta-characters.

61. Data is not always stored statically on a storage device. Thus, a range of security mechanisms are needed to provide reasonable protection over a range of events and circumstances. Which of the following is not a true statement?

A. Data in-transit is data being communicated over a network connection.

B. Session encryption should be used to protect data in-transit.

C. Storage encryption, such as file encryption or whole drive encryption, should be used to protect data at-rest.

D. Data in-use should be protected against disclosure with hashing.

Answer: D

Data in-use is data being actively processed by an application. Open and active data is only secure if the logical and physical environment is secure. A well established security baseline and physical access control are needed to provide reasonable protection for data in-use. Hashing is an integrity protecting mechanism, not a protection against disclosure.

62. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are devices or applications that generate passwords not based on fixed time intervals but instead generates passwords based on a non-repeating one-way function, such as a hash or HMAC (hash message authentication code) (i.e. a type of hash that used a symmetric key in the hashing process) operation.

A. SCADA

B. CHAP

C. HOTP

D. FCoE

Answer: C

HOTP (HMAC-based One-time Password) tokens or asynchronous dynamic password tokens devices or applications that generate passwords not based on fixed time intervals but instead generates passwords based on a non-repeating one-way function, such as a hash or HMAC (hash message authentication code) (i.e. a type of hash that used a symmetric key in the hashing process) operation.

63. Why should generic, anonymous, or group accounts be prohibited?

A. No support for multi-factor authentication

B. Not supported by LDAP

C. Inability to hold individuals accountable

D. Requires the use of a TPM

Answer: C

Generic account prohibition is the rule that no generic or shared or anonymous accounts should be allowed in private networks or on any system where security is important. Only with unique accounts per subject is it possible to track the activities of individuals and be able to hold them accountable for their actions and any violations of company policy or the law.

64. Which of the following is considered the least secure?

A. Out-of-band key exchange

B. ECDHE key exchange

C. In-band key exchange

D. One-time pad based keys

Answer: C

In-band key exchange is often considered less secure than any other key exchange option because there is greater risk of an eavesdropping or man-in-the-middle attack being able to capture and/or intercept the exchange.

65. A cipher suite is?

A. A standardized collection of authentication, encryption, and hashing algorithms used to set or define the parameters for a security network communication.

B. A communication tunnelbetween two entities across an intermediary network.

C. A storage process by which copies of private keys and/or secret keys are retained by a centralized management system.

D. A process by which one communication is hidden inside another communication.

Answer: A

A cipher suite a standardized collection of authentication, encryption, and hashing algorithms used to set or define the parameters for a security network communication. A VPN is a communication tunnel between two entities across an intermediary network. Key escrow is a storage process by which copies of private keys and/or secret keys are retained by a centralized management system. Steganography is a process by which one communication is hidden inside another communication.