HCIA SECURITY REVISION QUESTIONS

1. In hot standby networking, the heartbeat interfaces of the two firewalls must be added to the same security zone.
   A. True
   B. False
2. Employees violating information security may pose security threats to the enterprise networks.
   A. True
   B. False

3. During data encryption, hash algorithms can be used to verify data integrity.
   A. True
   C. False

4. One of the differences between TCP/IP model and the OSI reference model is that the TCP/IP model classifies both the presentation and session layer as the application layer.
   A. True
   B. False
5. In IPsec, AH provides data origin authentication, data integrity check, and anti-replay, but does not provide encryption.
   A. True
   B. False
6. The user organizational structure on a firewall is a mapping of an enterprise's actual organizational structure, and is the basis for use and user organizational structure includes the authentication domain, user group/user, and security group.
   A. True
   B. False

7. All packets constructed and proactively sent by the firewall are considered to be sent from the local zone. All packets requiring the (not only detected and directly forwarded) are considered to be received by the local zone.
   A. True
   B. False

8. There are four default actions for predefined IPS signatures permit, alert, block and blacklist.
   A. True
   B. False

9. A supply chain attack is a cyber attack that targets organizations by focusing on weaker links in their supply chain.
   A. True
   B. False

10. You can run the reset firewall session table command to clear all the session table information. The users then need to re-initiate connection for communication.
    A. True
    B. False

11. Digital signature technology is used in digital certificates.
    A. True
    B. False

12. Before forwarding unicast packets, a layer 2 switch needs to decapsulate their layer 3 header.
    A. True
    B. False

13. SNM3 is a commercial algorithm compiled by the National Cryptography administration. It is used for digital signature and authentication generation and authentication, and random number generation in cryptography applications. It can meet the security requirements of applications.

    A. True
    B. False

14. HTTPS introduces the TLS layer based on HTTP to provide identity authentication, encryption, and integrity check for data transmission.

    A. True
    B. False

15. The DH algorithm is an asymmetric encryption algorithm typically used to negotiate a symmetric encryption key.

    A. True
    B. False

16. SQL injection can be used to perform attack such as authentication bypass, data tampering
    A. True
    B. False
17. A sender a digital signature by encrypting the digital fingerprint using its own public key
    A. True

B. False

18. The keys used for IPsec encryption and authentication can be manually configured or dynamically

    A. True

    B. False

19. The MAC address entries of a layer 2 switch can be dynamically learned or manually configured

    A. True

    B. False

20. Servers that public access are usually placed in the DMZ zone of the firewall.

    A. True

    B. False

Multiple Choice

1. Which of the following are characteristics of viruses and malware?
   - **A. Unauthorized access**
   - **B. Tampering**
   - **C. Damage**
   - D. Unauthorized registration
2. Which of the following statements are correct about the PKI system structure?
   - A. A PKI system consists of three parts: end entity, certificate authority, and certificate registration authority.
   - **B. A PKI entity is an end user of PKI products or services. It can be an individual, an organization, a device (such as a router or firewall).**
   - **C. A CA is a trusted entity that issues and manages digital certificates.**
   - **D. CAs are classified into the root CA and subordinate CAs according to the hierarchy of CAs.**
3. Which of the following measures can be taken to address enterprise network security threats?
   - **A. Egress security.**
   - **B. Terminal security**
   - **C. Transmission security**
   - **D. Device security**
4. Which of the following statements are correct about the firewall DMZ?
   - A. The default priority of the DMZ is 50 and cannot be manually changed.
   - B. The DMZ has a lower priority than the Trust Zone. Therefore, devices in the Trust Zone can directly access the DMZ.
   - **C. Typically, servers that must provide public access services are deployed in the DMZ.**
   - **D. When external network users access the DMZ, both the security policy and NAT policy need to be deployed.**
5. Which of the following statements are correct about SSL VPN?
   - A. Remote office users access intranet web resources through the web proxy service.
   - **B. Remote office users access intranet UDP resources through the port forwarding service.**
   - C. Remote office users access intranet file servers through the file sharing service.
   - **D. Remote office users access intranet IP resources through the network extension service.**
6. Which of the following types of traffic do not trigger authentication even If they match an authentication policy?
   - **A. OSPF traffic**
   - **B. LDP traffic**
   - C. Device access traffic
   - D. Traffic generated when a user accesses the HTTP service

7. Which of the following statements are correct about the differences between firewalls, routers and switches?
    A. Routers and switches are mainly used to forward data, while firewalls are used to control data.
    B. Routers are used to connect different networks and use routing protocols to communicate with each other so that packets can…
    C. A switch is usually used to set up a LAN and is an important network element for LAN communication. It uses layer 2/layer 3.
    D. Firewalls are deployed at the network border to control incoming and outgoing network access. Security protection is the core…..
8. Which of the following statements are correct about the PKI lifecycle?
    A. The PKI manages the entire lifecycle of local certificates, including applying for, issuing, storing, downloading, installing, authentication…
    B. When the certificate of a PKI entity expires, the PKI entity does not need to replace the certificate.
    C. If user services are terminated, users need to revoke their digital certificates.
    D. In order for a download certificate to take effect, it must be installed on the device (specifically, it must be imported into the device).
9. Which of the following statements are correct about RADIUS?
    A. It uses TCP
    B. It encrypts only the password field in an authentication packet.
    C. It applies to accounting.
    D. It supports command authorization.
10. Which of the following statements are correct about IPS signatures?
    A. Predefined signatures are those in the IPS signature database.
    B. Predefined signatures can be created, modified, or deleted.
    C. IPS signature describe the characteristics of attack behaviors on a network.
    D. Incorrect signatures may be useless, cause packet loss, or even interrupt services.
11. Which of the following servers are involved in the DNS system?
    A. Root Server.
    B. Top level DNS Server
    C. Authentication DNS Server
    D. Cache Server
12. Which of the following statements are correct about GRE tunnel interfaces?
    A. GRE tunnel interfaces encapsulate and decapsulate data packets using GRE.
    B. In most cases, the physical interface connecting the local device to the public network is used as the tunnel source interface, and the public network is used as the tunnel destination interface.
    C. A tunnel IP address is used only to enable a tunnel interface to go up and does not need to be configured.

D. When OSPF is enabled on GRE tunnel, the tunnel interfaces at both ends of the must be on the same network segment.

13. Which of the following are characteristics of LDAP?

    A. Supports distributed data storage.
    B. Provides a unified access point for external systems.
    C. Organizes data by directory.
    D. The query is optimized to read data quickly.

14. What are the components of a PKI System?

    A. End entity
    B. Certificate Authority
    C. Certificate Registration Authority
    D. **Certificate/CRL Storage**.

15. Which of the following identity authentication methods are supported by IKEv1?

    A. Pre-shared key
    B. RSA signature.
    C. Digest authentication
    D. Digital envelope authentication

16. Which of the following requirements must be met in setting the administrator password?

    A. The password must be a string of 8 to 64 characters.
    B. The password cannot contain two or more of the same characters consecutively
    C. Admin@123 can be used as the password of a new administrator. However, after the administrator logs in to the system, the administrator…
    D. **To improve security, the password must contain special characters**.

17. Which of the following are application-layer protocols?

    A. HTTP
    B. DNS
    C. Telnet
    D. ARP

18. Which of the following layers in the OSI model correlate to the network interface layer in the standard TCP/IP reference model?

    A. Data link layer
    B. Physical layer
    C. Network layer
    D. Transport layer

19. A message indicating an invalid user name or password is displayed when a user logs in to an SSL VPN gateway. Which of the ….

    A. The account is locked out after incorrect passwords are entered multiple consecutive times.
    B. The authentication server configuration is incorrect
    C. The username or password is incorrect
    D. The authentication mode is incorrect

20. Which of the following statements are correct about the working mechanism and functions of the Huawei Intrusion prevention system?

A. The system parses data protocols, matches the data characteristics against the signature database for identification, and performs further data processing.

B. The signature database needs to be updated frequently to identify the latest attacks, viruses, and unreasonable use of P2P traffic.

C. Intrusion prevention actions include permit, alert, and block.

D. Devices are deployed at the network egress in bypass mode to protect the network in real time without affecting the network topology.

21. Which of the following attacks is initiated by external users to steal local information

A DOS attack

B Trojan horse

C **phishing**

D. Buffer overflow attack

22. which of the following statement is correct about ASPF and server mapping entries

A. ASPF check network-layer information and monitors the network-layer protocol status

B. ASPF determines whether to permit data packets based on the dynamically generated ACLS

C. The server-map generated by ASPF is dynamic

D. All server mapping entry uses a 5-tuple to identify a session

23. Which of the following is incorrect about AH and ESP?

A. AH provide only authentication but not encryption

B. ESP provide both authentication and encryption

C. AH does not check the integrity of the IP header

D. ESP encrypts the valid payload and then encapsulates it into a data packet to ensure data confidentiality

24. Which of the following lists firewall security zones in descending order of priority?

A. Trust >local>DMZ>untrust

B. local>Trust>DMZ>untrust

C. Trust>DMZ>local>untrust

D. Trust>Local>untrust>DMZ

25. Which of the following statement is incorrect about digital certificates?

A. digital certificate contains the owners public key and related identity information.

B. In its simplest form, a certificate contains a public key, name, and digital signature of a CA.

C. A digital signature A digital certificate cannot ensure that one public key is possessed by only one owner in digital signature

D. In most cases, the key of a digital certificate has a validity period.

26. Which of the following is not an advantage of symmetric encryption algorithms

A. High efficiency

B. Low cost

C. Good scalability

D. Suitable for encrypting a large amount of data

27. Which of the following is not an external security threat faced by enterprises?

A. Network scanning

B. DDoS attack

C. Phishing email

D. Terminal vulnerability

28. Which of the following types of packets cannot be filtered by a packet filtering firewall?

A. Non-initial fragments

B. Non-fragmented packets

C. **Forged ICMP error packets**

D. Initial fragments

29. Which of the following statements is incorrect about DOS attacks?

A. DOS attacks stop services or resource access on the target server

B. DOS attacks cause unrecoverable physical damage to the target server.

C. DOS attack forces the target server's buffer to be full and does not receive new requests.

D. DOS attacks use IP spoofing to prevent authorized users from connecting to the target server.

30. Which of the following is not a function of digital envelope?

A. It solves the problem of releasing symmetric keys.

B. It solve the problem of slow symmetric keys encryption

C. It improve security, scalability, and efficiency

D. It ensures the security of symmetric keys.

11. What is the protocol number of ESP?

A**. 50**

B.51

C. 53

D.54

31. Which of the following is not a function of public key technologies

A. Identity Authentication

B. Data integrity

C. **public key security**

D. data privacy

32. Which of the following is not a layer 2 VPN

A. **IPsec**
B. PPTP
C. L2TP
D. QinQ

33. If the VRRP group ID is 2, which of the following is the MAC address of the virtual router?
A. 00-00-5E-01-02
B. 00-00-5E-00-00-02
C. 00-10-5E-00-01-01
D. 00-01-5E-00-01-02

34. Which of the following statement is correct about HTTP?
A. HTTP is used to access various pages on the www server
B. HTTP is used to convert host domain names to IP addresses
C. HTTP resolves known IP addresses into MAC addresses
D. HTTP provide a way to transfer files. It allows data to be transferred from one host to another

35. .How many types of digital certificates are defined by Huawei
A. 1
B. 2
C. 3
D. 4

36. Which of the following are covered in the basic implementation of intrusion prevention?
A. Application data reassembly
B. protocol identification and parsing
C. Signature matching
D. Response and handling

37. Which of the following are the default zones of Huawei firewalls?
A. Untrust
B. DMZ
C. Trust
D. local

38. Which items are contained in a digital certificate
A. Public key
B. Certificate serial number
C. Digital signature
D. Key validity period

39. which of the following attacks are single –packet attacks?
A Smurf attack
B IP spoofing attack

C IP sweep attack
D ICMP redirect attack

40 which of the following operation can be performed on data in the security situational awareness
A Data cleaning
B Data classification
C Data association and supplementation
D Data labelling

41 Which of the following statement are correct about SSL VPN access users?
A Visitors can log in to the authentication page provided by the SSL VPN module to trigger the authentication
B HTTPS is an application of SSL VPN
C SSL VPN works between the transport layer and application layer
D SSL VPN provides services such as web proxy and network extension

42 Which of the following statement are correct about SSL VPN?
A Remote office users access intranet web resources through the web proxy service
B Remote office users access intranet UDP resources through the port forwarding services
C Remote office users access intranet file servers through the file sharing service
D Remote office users access intranet IP resources through the network extension service

43 which of the following layers in the OSI model correlate to the network interface layers
A Data link layer
B Physical layers
C Network layer
D Transport

44 Which of the following are the characteristics of viruses and malware
A **Unauthorized access**
B Tampering
C Damage
D Unauthorized registration

45. Which of the following algorithms can be used by digital envelope?
A Symmetric encryption algorithm
B Hash algorithm
C Asymmetric encryption algorithm
D MD5 algorithm

46 which of the following are included in the framework of the IPsec VPN protocol?
A Security association
B Security protocol
C Encapsulation mode
D Key exchange

Single choice questions

1. Which of the following statements is correct about HTTP?
   a. **HTTP is used to access various pages on the WWW server.**
   b. HTTP is used to convert host domain names into IP addresses.
   c. HTTP resolves known IP addresses into MAC addresses.
   d. HTTP provides a way to transfer files. It allows data to be transferred from one host to another
2. Which of the following statements is incorrect about packet processing on a stateful inspection firewall?
   a. **When the firewall stateful detection mechanism is enabled, only SYN packets in TCP packets can be used to establish sessions.**
   b. When stateful inspection is enabled, the firewall checks both the first packet and subsequent packets against security policies.
   c. When receiving a packet, the firewall searches for a matching entry in the session table. If no match is found, the firewall processes the packet…
   d. When receiving a packet, the firewall searches for a matching entry in the session table. If match is found, the firewall processes the packet…
3. Which of the following statements is incorrect about DoS attacks?
   a. DoS attacks stop services or resource access on the target server.
   b. **DoS attacks cause unrecoverable physical damage to the target server.**
   c. DoS attack forces the target server's buffer to be full and does not receive new requests.
   d. DoS attacks use IP spoofing to prevent authorized users from connecting to the target server.
4. Which of the following attacks is initiated by external users to steal local information or obtain control rights?
   a. DoS attack
   b. Trojan horse
   c. **Phishing**
   d. Buffer overflow attack
5. SMTP is a simple mail transfer protocol that provides internet email services. Which of the following is the SMTP port number?
   a. 80
   b. 23
   c. 21
   d. **25**
6. Which of the following statements is correct about ASPF and sever mapping entries?
   a. ASPF checks network-layer information and monitors the network-layer protocol status.
   b. ASPF determines whether to permit data packets based on the dynamically generated ACLs
   c. **The server-map generated by the ASPF is dynamic**
   d. All sever mapping entry uses a 5-tuple to identify a session.

7. Which of the following statements is incorrect about AH in IPsec VPN?
    a. It supports data origin authentication
    b. It supports data integrity check
    c. It supports anti-replay
    d. It supports packet encryption
8. Which of the following problems cannot be solved using PKI?
    a. The transaction parties cannot verify the identities of each other.
    b. Data may be eavesdropped and tampered with during transmission, and information security cannot be ensured.
    c. No paper receipt is used in transaction, making arbitration difficult
    d. The network is congested due to heavy traffic. As a result, the server cannot provide services properly.
9. Which of the following is an example of a strong password?
    a. Admin321
    b. Huawei!3S5#2%
    c. Hell0world
    d. 1001
10. Which of the following is not an asymmetric encryption algorithm?
    a. DH
    b. DES
    c. RSA
    d. DSA
11. Which of the following lists firewall security zones in descending order of priority?
    a. Trust > Local > DMZ > Untrust
    b. Local > Trust > DMZ > Untrust
    c. Trust > DMZ > Local > Untrust
    d. Trust > Local > Untrust > DMZ
12. Which of the following is not a function of security awareness?
    a. Security data processing
    b. Security element collection
    c. Security data analysis and result display
    d. Automatic security locating
13. Which of the following is not an external security threat faced by enterprises?
    a. Network Scanning
    b. DDoS attack
    c. Phishing email
    d. Terminal Vulnerability
14. A basic ACL rule is configured as follows:

    ```
    #
    Rule permit source 1.1.1.0 0.0.0.255
    #
    ```

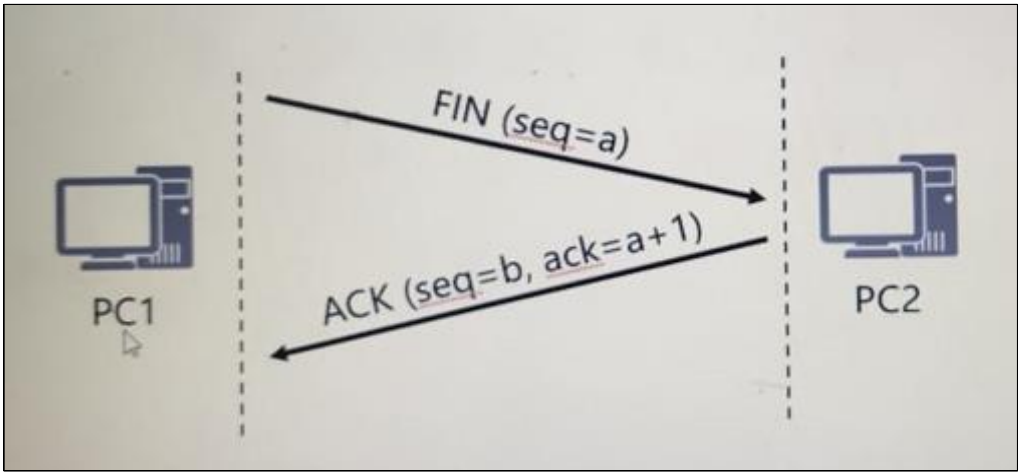
    Given this, which of the following statements is correct?
    a. Packets with source address 1.1.1.1 and destination address 2.2.2.2 are discarded.

b. Packets with source address 1.1.1.10 and destination address 2.2.2.2 are discarded
c. Packets with source address 1.1.200.200 and destination address 2.2.2.2 are allowed to pass through.
d. **Packets with source address 1.1.1.200 and destination address 2.2.2.2 are allowed to pass through**.

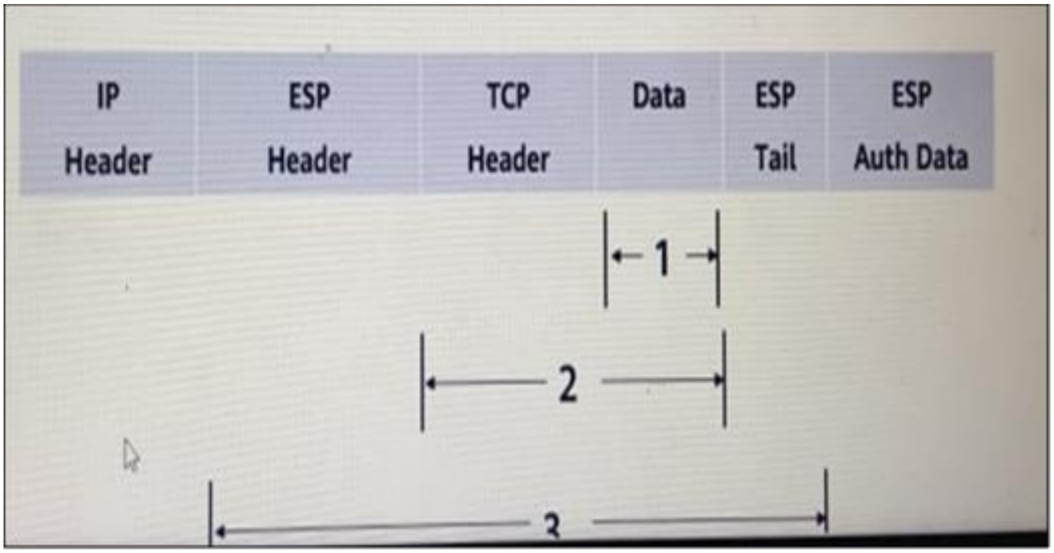
15. What is the protocol number of ESP?
    a. 50
    b. 51
    c. 53
    d. 54
16. Which of the following is not a layer 2 VPN?
    a. IPsec
    b. PPTP
    c. L2TP
    d. QinQ
17. Which of the following statements is incorrect about GRE over IPsec?
    a. GRE over IPsec encapsulates packets using GRE and the IPsec.
    b. GRE over IPsec supports encapsulation in both tunnel and transport modes.
    c. GRE over IPsec combines the advantages of GRE and IPsec to securely transmit broadcast and multicast services between a company's head…
    d. IPsec protects the data flows originated from the GRE tunnel source address to the GRE tunnel destination address.
18. Which of the following statements is correct about the heartbeat link and heartbeat interface of a firewall?
    a. An interface configured with the vrrp virtual-mac enable command can be used as a heartbeat interface.
    b. An interface whose MTU value is less than 1500 can be used as a heartbeat interface.
    c. The heartbeat interface of two firewalls can be added to different security zones.
    d. The management interface (Meth0/0/0) cannot be used as a heartbeat interface.
19. Which of the following items is not included in an IPsec SA?
    a. Security Parameter Index(SPI)
    b. Destination IP address
    c. Security protocol number
    d. Port number
20. Which of the following technologies can hide the internal network while preventing external attacks on an internal server?
    a. IP Spoofing
    b. NAT
    c. ACL
    d. VRRP
21. Which of the following statements is incorrect about digital certificates?
    a. In its simplest form, a certificate contains a public key, name, and digital signature of a CA.

b. Issuer name in the digital certificate, which can be different from the principal name in the issuer certificate.
c. The certificate structure complies with X 509v3.
d. A signature is obtained after the issuer uses a private key to encrypt the hash digest of the certificate information.

22. Which of the following statements is correct about the default zones of Huawei firewalls?
    a. Default security zones can be deleted.
    b. Four default security zones are available
    c. Default security zones cannot be deleted, but their security level can be modified.
    d. The level of a default security zone can be customized.
23. As shown in the figure, a TCP connection is set up between PC1 NAD PC2. PC1 sends a FIN request for this connection, and PC2…. Which of the following statements is correct?



    a. The TCP connection between PC1 and PC2 is closed.
    b. The TCP connection between PC1 and PC2 is in the half-closed state and cannot be used to send data.
    c. The TCP connection between PC1 and PC2 is in the half-closed state, and PC1 can still send data to PC2.
    d. The TCP connection between PC1 and PC2 is in the half-closed state, and PC2 can still send data to PC1.
24. As shown in the figure, which of the following shows the authentication range of ESP in transport mode?


IP Header
ESP Header
TCP Header
Data
ESP Tail
ESP Auth Data
1
2
3