H12-711 HCIA-Security Examination

1. The source socket includes source IP address, source port, and destination IP address. ( )
True **False**

2. The Protocol field of IP packet headers identifies the upper-layer protocol. If the field value is 6, the upper-layer protocol is TCP. If the field value is 17, the upper-layer protocol is UDP. ( )
True False

3. IN SYN flood attacks, an attacker sends a large number of SYN packets to the server but does not acknowledge the SYN-ACK packets. Therefore, the server maintains a lot of half-open TCP connections, exhausting the server resources. ( )
True False

4. Stateful inspection firewalls create and maintain session tables to keep track of TCP and UDP sessions and use security policies to control which sessions can be created. Only the packets associated with the created sessions are forwarded. ( )
True False

5. In network security, attacks can undermine network resources and make them invalid or unavailable. Such attacks are targeted at ( ).
A. Availability B. Confidentiality C. Integrity D. Authenticity

6. Which of the following items is not included in a server map entry of the USG series? ( )
A. Destination IP address
B. Destination port
C. Protocol
D. Source IP address

7. Which of the following zones can be deleted? ( )
A. Security Zone
B. Trust Zone
C. Untrust Zone
D. DMZ Zone

8. Which of the following statements about buffer overflow attacks are correct? ( ) (Select 3 Answers)
A. Buffer overflow attacks use software system memory operation defects with high operating privileges to run attack code.
B. Operating system vulnerabilities and architecture will not cause buffer overflow attacks.
C. The buffer overflow attack is one of the most common methods for attacking software systems.
D. The buffer overflow attack is a type of application-layer attack.

9. Stateful inspection firewalls forward subsequent packets (subsequent packets) mainly based on _____?
A. Route table
B. MAC address table
C. Session table
D. FIB table

10 Which of the following Layer-3 VPN is more secure? ( )
A. GRE
B. PPTP
C. IPSec
D. L2F

11 Which of the following statements about ARP spoofing attacks is incorrect? ( )
A. The ARP mechanism checks only normal packet interactions.
B. ARP spoofing attacks are implemented only through ARP replies.
C. When a host sends a normal ARP request, an attacker responds before the server responds, causing the host to establish an incorrect mapping between the IP and MAC addresses.
D. ARP static binding can be used to defend against ARP spoofing attacks, and it is used mainly on small-scale networks.

12 ACL 2009 is ( )
A. A basic ACL
B. An advanced ACL
C. A MAC-based ACL
D. A time-based ACL

13 Which of the following IP address ranges is the one defined in the rule permit ip source 192.168.11.32 0.0.0.31 command? ( )
A. 192.168.11.0-192.168.11.255
B. 192.168.11.32-192.168.11.63
C. 192.168.11.31-192.168.11.64
D. 192.168.11.32-192.168.11.64

14. Which of the following algorithms uses the same key for encryption and decryption? ( )
A. DES
B. RSA (1024)
C. MD5
D. SHA-1

15. In GRE VPN, which of the following protocols is an encapsulation protocol? ( )
A. GRE
B. IPX
C. IP
D. NetBEUI

16. Which of the following modes is an IKE mode in the second phase? ( )
A. Main mode
B. Aggressive mode
C. Quick mode
D. Passive mode

17 Which one of the following protocols is a multi-channel protocol?（ ）
A. FTP
B. Telnet
C. HTTP
D. SMTP

18. What features does the NAT technology have? ( )
A. NAT hides private IP addresses and improves network security.
B. NAT does not support NAPT for private IP addresses.
C. The IP address translation is transparent for both private and public network users. Users cannot percept the translation process.
D. If bidirectional NAT is configured, external users can access the resources on the private network without any restriction.

19. What does AAA mean?（ ）(Select 3 Answers)
A. Authentication
B. Authorization
C. Accounting

D. Audit

20. Which of the following algorithms are encryption algorithms? （ ）(Select 2 Answers)
A. DES
B. 3DES
C. SHA-1
D. MD5

21. Which of following statements about IDS are correct?（ ） (Select 3 Answers)
A. The IDS dynamically collects a large volume of key information and analyzes and identifies the status of the entire system.
B. The IDS can block detected policy breaches and attacks.
C. The IDS system is comprised of all software and hardware systems for intrusion detection.
D. The IDS system can function with firewalls and switches to better control external access.

22. Which of the following user access and authentication methods are supported by the Policy Center system? （）(Select 3 Answers)
A. Web, identify authentication
B. WebAgent, identify authentication and part of security authentication
C. Agent, identify authentication and security authentication
D. Network access without authentication

23. To enable employees on a business trip to access the intranet file server, which of the following SSL VPN functions is the optimal solution?（ ）
A. Web proxy
B. File sharing
C. Port forwarding
D. Network extension

24. Which of the following protocols are used by SSL? ( ) (Select 3 Answers)
A. Handshake protocol
B. Record protocol
C. Alert protocol
D. Heartbeat protocol

25. Which of the following headers contains a VLAN tag? （ ）
A. Ethernet Frame
B. IP header
C. TCP header
D. UDP header

1.Which of the following is not a major feature of the information security system?（single choice ）
A: **Commonality** B: Controllability C: Non-repudiation D: Integrity

2.Which of the following statements are true about the functions of the "allow l2tp virtual-template 0 remote client" command in L2TP configuration?（multiple choice）
A: This command specifies the virtual interface template to be used.
B: This command specifies the peer tunnel name.
C: This command specifies the local tunnel name.
D: You do not need to specify the tunnel name in certain cases.

3.Checking the system running status, collecting system fault information, and detecting

information security incidents are all actions in cyber security emergency response. Which of the following phases do these actions belong to?（single choice）
A: Preparation phase **B: Detection phase** C: Response phase D: Recovery phase

4.Which of the following statements are true about the signature in certificate content?（multiple choice）
A: It indicates the encryption result of the public key.
B: It indicates the encryption result of the certificate information.
C: It is generated by encrypting the private key of the certificate issuer.
D: It is generated by encrypting the private key of the public key owner.

5.Which of the following statements are false about the IPsec VPN key generation mode?（multiple choice）
A: The key can be manually configured.
B: The key can be generated using IKE.
C: The key generated using IKE can be periodically changed.
D: The key generated during IKE negotiation cannot be used to authenticate identity information.

6.Which of the following is an analysis layer device in the Huawei SDSec solution?（single choice）
A: CIS B: Agile Controller C: Switch **D: Firehunter**

7.Which of the following is not a state of the Huawei Redundancy Protocol (HRP) heartbeat interface?（single choice）
A: Invalid B: Ready C: running **D: full**

8.When a cyber security issue occurs, the severity of the issue must be determined first and immediately reported.（single choice）
A: True **B: False**

9.Which of the following methods can be used by an administrator to log in to Huawei routers for the first time?（single choice）
A: SSH B: Telnet C: Web **D: Console**

10.In the ARP address resolution process, ARP-Reply packets are sent in broadcast mode. All hosts on the same Layer 2 network can receive these packets and learn the mapping between IP and MAC addresses from them.（single choice）
A: True **B: False**

11.When intranet users access the Internet, you can configure a source NAT policy in the easy-ip format.（single choice）
A: True B: False

12.Which of the following password settings is the most secure?（single choice）
A: Digits only
B: Letters only
C: Digits+letters
D: Digits+letters+special characters

13.Which of the following is not a risk identification phase in risk assessment of ISO 27001?（single choice）

A: Risk avoidance
B: Weaknesses identification and assessment
C: Penetration test
D: Network architecture analysis

14.Which of the following statements is false about iptables?（single choice）
A: iptables is a free packet filtering firewall.
B: The table of iptables consists of chains, and a chain consists of rules.
C: A Linux firewall consists of netfilter and iptables.
D: The table processing priority is mangle > raw > nat > filter.

15.A vulnerability is usually called a virus.（single choice）
A: True **B: False**

16.Which layer of the OSI model can encrypt data formats and data?（single choice）
A: Application layer **B: Presentation layer** C: Session layer D: Transport layer

17.Which of the following are included in AAA?（multiple choice）
A: Authentication **B: Authorization** **C: Accounting** D: Audit

18.Which of the following statements are true about penetration test steps?（multiple choice）
A: Collect information and analyze network conditions before a penetration test.
B: Escalate access control rights for implementing a penetration test.
C: After a penetration test is complete, directly output a test report.
D: Provide security suggestions after a test report is output.

19.Which of the following statements is true about antivirus software?（single choice）
A: The virus library of antivirus software usually lags behind computer viruses.
B: Good antivirus software can kill all viruses.
C: Antivirus software can kill all found viruses.
D: Computers that have antivirus software installed will not be infected by viruses.

20.Which of the following actions should be taken in the recovery phase of cyber security emergency response?（multiple choice）
A: Continuously monitor the devices that go online again to learn their running status.
B: Set an isolation zone, summarize data, and estimate loss.
C: Restore the configuration of the damaged network devices and back up all changes.
D: Set up management and technical teams and assign responsibilities to personnel.