Certshared now are offering 100% pass ensure 350-018 dumps!
https://www.certshared.com/exam/350-018/ (872 Q&As)

Cisco

Exam Questions 350-018

CCIE Pre-Qualification Test for Security

Guaranteed success with Our exam guides
visit - https://www.certshared.com
1. A firewall rule that filters on the protocol field of an IP packet is acting on which layer of the OSI reference model?

A. network layer
B. application layer
C. transport layer
D. session layer

Answer: A

2. Which two statements about IPv6 path MTU discovery are true? (Choose two.)

A. If the destination host receives an ICMPv6 Packet Too Big message from a router, it reduces its path MTU.
B. It can allow fragmentation when the minimum MTU is below a configured value.
C. The discovery packets are dropped if there is congestion on the link.
D. If the source host receives an ICMPv6 Packet Too Big message from a router, it reduces its path MTU.
E. During the discovery process, the DF bit is set to 1.
F. The initial path MTU is the same as the MTU of the original node’s link layer interface.

Answer: D,F

Explanation:
IPv6 routers do not support fragmentation or the Don’t Fragment option. For IPv6, Path MTU Discovery works by initially assuming the path MTU is the same as the MTU on the link layer interface where the traffic originates. Then, similar to IPv4, any device along the path whose MTU is smaller than the packet will drop the packet and send back an ICMPv6 Packet Too Big (Type 2) message containing its MTU, allowing the source host to reduce its Path MTU appropriately. The process is repeated until the MTU is small enough to traverse the entire path without fragmentation.

Reference: https://en.wikipedia.org/wiki/Path_MTU_Discovery

3. DRAG DROP

Drag each goal of PCI DS5 on the left to the corresponding PCI DSS requirement on the right.

Answer:
4. Which statement about the fragmentation of IPsec packets in routers is true?

A. By default if the packet size exceeds MTU of ingress physical interface, it will be fragmented and sent without encryption.
B. By default if the packet size exceeds MTU of the egress physical interface, it will be dropped.
C. By default, the router knows the IPsec overhead to add to the packet, performs a lookup if the packet will exceed egress physical interface IP MTU after encryption, then fragments the packet before encrypting and separately encrypts the resulting IP fragments.
D. By default, the IP packets that need encryption are first encrypted with ESP, if the resulting encrypted packet exceeds the IP MTU on the egress physical interface, then the encrypted packet is fragmented before being sent.

Answer: C

5. Which two statements about RFC 2827 are true? (Choose two.)

A. RFC 2827 defines egress packet filtering to safeguard against IP spoofing.
B. A corresponding practice is documented by the IETF in BCP 38.
C. RFC 2827 defines ingress packet filtering for the multihomed network.
D. RFC 2827 defines ingress packet filtering to defeat DoS using IP spoofing.
E. A corresponding practice is documented by the IETF in BCP 84.

Answer: B,D

6. What is the effect of the given command? Refer to the exhibit.

A. It enables CoPP on the FastEthernet 0/0 interface for SSH and SNMP management traffic.
B. It enables MPP on the FastEthernet 0/0 interface for SSH and SNMP management traffic and CoPP for all other protocols.
C. It enables MPP on the FastEthernet 0/0 interface, allowing only SSH and SNMP management traffic.
D. It enables QoS policing on the control plane of the FastEthernet 0/0 interface.
E. It enables MPP on the FastEthernet 0/0 interface by enforcing rate-limiting for SSH and SNMP management traffic.

Answer: C

7. Which two statements about SSL VPN smart tunnels on a Cisco IOS device are true? (Choose two.)

A. They are incompatible with split tunneling.
B. They do not support FTP.
C. They are incompatible with MAPI proxy.

Answer: A,B
D. They support private socket libraries.
E. They can be started in more than one Web browser at the same time.

Answer: A, C

Restrictions for Cisco IOS SSL VPN Smart Tunnels Support

? Smart tunnels do not support split tunneling, Cisco Secure Desktop, private socket libraries, and MAPI proxy.

? Smart tunnels must not be started in two different web browsers simultaneously.

? Applications only with the winsock dll library such as Remote Desktop, VNCviewer, Outlook Express, Outlook Web Access (OWA), Secure Shell (SSH) using Putty, Telnet, FTP, and others are supported.


8. crypto gdoi group gdoi_group identity number 1234

server local

sa receive-only sa ipsec 1 profile gdoi-p

match address ipv4 120

Which statement about the above configuration is true?

A. The key server instructs the DMVPN spoke to install SAs outbound only.
B. The key server instructs the GDOI group to install SAs inbound only.
C. The key server instructs the DMVPN hub to install SAs outbound only.
D. The key server instructs the GDOI spoke to install SAs inbound only.

Answer: B

9. Which statement best describes the concepts of rootkits and privilege escalation?

A. Rootkits propagate themselves.
B. Privilege escalation is the result of a rootkit.
C. Rootkits are a result of a privilege escalation.
D. Both of these require a TCP port to gain access.

Answer: B

10. Refer to the exhibit.

<table>
<thead>
<tr>
<th>Line</th>
<th>User</th>
<th>Host(s)</th>
<th>Idle</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 con 0</td>
<td>admin</td>
<td>idle</td>
<td>00:00:12</td>
<td></td>
</tr>
<tr>
<td>194 vty 0</td>
<td>admin</td>
<td>idle</td>
<td>00:00:02</td>
<td>internal.example.com</td>
</tr>
</tbody>
</table>

What service is enabled on the router for a remote attacker to obtain this information?

A. TCP small services
B. finger
C. maintenance operation protocol
D. chargen
E. Telnet
F. CEF

Answer: B

11. Which three statements about triple DES are true? (Choose three.)
A. For 3DES, ANSI X9.52 describes three options for the selection of the keys in a bundle, where all keys are independent.
B. A 3DES key bundle is 192 bits long.
C. A 3DES keyspace is 168 bits.
D. CBC, 64-bit CFB, OFB, and CTR are modes of 3DES.
E. 3DES involves encrypting a 64-bit block of plaintext with the 3 keys of the key bundle.
Answer: B,C,D

12. Which two statements about the DES algorithm are true? (Choose two)
A. The DES algorithm is based on asymmetric cryptography.
B. The DES algorithm is a stream cipher.
C. The DES algorithm is based on symmetric cryptography.
D. The DES algorithm encrypts a block of 128 bits.
E. The DES algorithm uses a 56-bit key.
Answer: C,E

13. Which spanning-tree mode supports a separate spanning-tree instance for each VLAN and also supports the 802.1w standard that has a faster convergence than 802.1D?
A. PVST+
B. PVRST+
C. PVST
D. CST
E. MST
F. RST
Answer: B

14. Which statement is valid regarding SGACL?
A. SGACL mapping and policies can only be manually configured.
B. Dynamically downloaded SGACL does not override manually configured conflicting policies.
C. SGACL is access-list bound with a range of SGTs and DGTs.
D. SGACL is not a role-based access list.
Answer: C

Explanation:
A role-based access control list bound to a range of SGTs and DGTs forms an SGACL. Reference:

15. Which three LSA types are used by OSPFv3? (Choose three.)
A. Link LSA
B. Intra-Area Prefix LSA
C. Interarea-prefix LSA for ASBRs
D. Autonomous system external LSA
E. Internetwork LSA
Answer: A,B,D

16. Which three statements regarding VLANs are true? (Choose three.)
A. To create a new VLAN on a Cisco Catalyst switch, the VLAN name, VLAN ID and VLAN type must all be specifically configured by the administrator.

B. A VLAN is a broadcast domain.

C. Each VLAN must have an SVI configured on the Cisco Catalyst switch for it to be operational.

D. The native VLAN is used for untagged traffic on an 802.1Q trunk.

E. VLANs can be connected across wide-area networks.

Answer: B,D,E

17. DRAG DROP

Drag each step in the Cisco PSIRT response to incidents and vulnerabilities involving Cisco products on the left in the correct order on the right.

Answer:

18. Which statement about a botnet attack is true?

A. The botnet attack is an attack on a firewall to disable it's filtering ability.

B. The botnet attack is a network sweeping attack to find hosts that are alive behind the filtering device.

C. The botnet attack is a collection of infected computers that launch automated attacks.

D. The owner of the infected computer willingly participates in automated attacks.

E. The botnet attack enhances the efficiency of the computer for effective automated attacks.

Answer: C

19. Refer to the exhibit.
Which message could contain an authenticated initial_contact notify during IKE main mode negotiation?

A. message 3
B. message 5
C. message 1
D. none, initial_contact is sent only during quick mode
E. none, notify messages are sent only as independent message types

Answer: B

20. What entities decrypt a transmission sent by a GDOI group member?

A. all group members
B. the key server only
C. the peer that is indicated by the key server
D. the key server and the peer that is indicated by the key server

Answer: A

21. MACsec, which is defined in 802.1AE, provides MAC-layer encryption over wired networks. Which two statements about MACsec are true? (Choose two.)

A. Only links between network access devices and endpoint devices can be secured by using MACsec.
B. MACsec is designed to support communications between network devices only.
C. MACsec manages the encryption keys that the MKA protocol uses.
D. A switch that uses MACsec accepts either MACsec or non-MACsec frames, depending on the policy that is associated with the client.

Answer: A,D

22. What Context-Based Access Control (CBAC) command sets the maximum time that a muter running Cisco IOS will wait for a new TCP session to reach the established state?

A. ip inspect max-incomplete
B. ip inspect tcp idle-time
C. ip inspect tcp finwait-time
D. ip inspect udp idle-time
E. ip inspect tcp synwait-time

Answer: E

23. What technology can secure DNS information in IP networks?

A. a combination of DNS and SSL/TLS

Certshared now are offering 100% pass ensure 350-018 dumps!
https://www.certshared.com/exam/350-018/ (872 Q&As)
B. a combination of DNS and IPSec
C. DNS encryption
D. DNSSEC
Answer: D
Explanation:
DNSSEC supplements the hierarchical nature of the DNS with cryptographic characteristics that make it possible to verify the authenticity of information stored in the DNS. This validation makes it possible for resolvers to be assured that when they request a particular piece of information from the DNS, that they do in fact receive the correct information as published by the authoritative source.

This assurance is made possible using cryptographic signatures included in the DNS by a source organization. These signatures are calculated on a complete Resource Record set, not individual Resource Records. The signatures are published in a DNSSEC-specific resource record type called RRSIG. For example, setting aside the requisite infrastructure, by publishing the signature for an A record, the source organization makes it possible for resolvers on the Internet to verify that the A record contains authentic data and is correct as published. A DNS server is only signing data for which it is authoritative, for example, the DNS server does not sign NS records that delegate subdomains from its zone.

Reference: http://www.cisco.com/web/about/security/intelligence/dnssec.html#5

24. Which two certificate enrollment methods can be completed without an RA and require no direct connection to a CA by the end entity? (Choose two.)
A. SCEP
B. TFTP
C. manual cut and paste
D. enrollment profile with direct HTTP
E. PKCS#12 import/export
Answer: C,E

25. Which statement about Storm Control implementation on a switch is true?
A. Storm Control does not prevent disruption due to unicast traffic.
B. Storm Control is implemented as a global configuration.
C. Storm Control uses the bandwidth and rate at which a packet is received to measure the activity.
D. Storm Control uses the bandwidth and rate at which a packet is dispatched to measure the activity.
E. Storm Control is enabled by default.
Answer: C

26. Which algorithm is used to generate the IKEv2 session key?
A. Diffie-Hellman
B. Rivest, Shamir, and Adleman
C. Secure Hash Algorithm
D. Rivest Cipher 4
Answer: A

27. What message does the TACACS+ daemon send during the AAA authentication process to request additional authentication information?
A. ACCEPT
B. CONTINUE
C. REJECT
D. ERROR
E. REPLY
Answer: B

28. Which two statements about the IPv6 OSPFv3 authentication Trailer are true (choose two)
A. The AT-bit resides in the OSPFv3 Header field
B. The IPv6 Payload length includes the length of the authentication Trailer
C. It Provide an alternative option to OSPFv3 IPsec authentication
D. The AT-bit must be set only in OSPFv3 Hello packets that include an Authentication Trailer
E. The AT-bit must be set only in OSPFv3 Database Description packets that include an Authentication Trailer
F. The OSPFv3 packet length includes the length of the Authentication Trailer

Answer: D,E

29. An exploit that involves connecting to a specific TCP port and gaining access to an administrative command prompt is an example of which type of attack?
A. botnet
B. Trojan horse
C. privilege escalation
D. DoS

Answer: C

30. Which traffic class is defined for non-business-relevant applications and receives any bandwidth that remains after QoS policies have been applied?
A. scavenger class
B. best effort
C. discard eligible
D. priority queued

Answer: A
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

350-018 Practice Exam Features:

* 350-018 Questions and Answers Updated Frequently
* 350-018 Practice Questions Verified by Expert Senior Certified Staff
* 350-018 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 350-018 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 350-018 Practice Test Here