ENCOR v1.1 (350-401) Video Training Series
Module 5 – Lesson 4 Quiz

Questions

1. Which secure domain found in Cisco's cyber threat defense framework deals with the internal and external security policies, such as HIPAA regulations?

   A. Security Intel
   B. Segmentation
   C. Compliance
   D. Threat Defense

2. Which of the following is not a solution used when achieving endpoint hardening?

   A. Cisco AMP
   B. Cisco Umbrella
   C. Cisco AnyConnect
   D. Cisco Smart Install

3. Which of the following is not an advantage of a next generation firewall (NGFW)?

   A. Zero-touch deployment
   B. Streamlined architecture
   C. Deep packet inspection
   D. Better throughput rates

4. Which mechanism is used by Cisco Identity Services Engine (ISE) to assign security tags for access policy enforcement?

   A. TrustSec
   B. MACsec
   C. NAC
   D. MAB

5. Which security standard is considered to be the wired equivalent of WPA2 protection used in wireless networks?

   A. MACsec
   B. NAC
   C. MAB
   D. TrustSec

6. Which piece of the Network Access Control (NAC) architecture receives extensible authentication protocol (EAP) packets and translates those into RADIUS packets?

   A. Supplicant
   B. Translator
   C. Authentication Server
   D. Authenticator

7. By default, how long does it take a Cisco Catalyst switch to consider 802.1X to be timed out before beginning MAC Authentication Bypass (MAB)?

   A. 30 seconds
   B. 60 seconds
   C. 90 seconds
   D. 120 seconds

Questions and Answers

1. Which secure domain found in Cisco's cyber threat defense framework deals with the internal and external security policies, such as HIPAA regulations?

A. Security Intel
B. Segmentation
C. Compliance
D. Threat Defense

Answer: C
Explanation: The Compliance domain addresses both internal and external security policies. Examples of these include standard regulations such as HIPAA, SOX, and PCI. This would also include any internal policies that are specific to your network.

Video Reference: Cyber Threat Defense

2. Which of the following is not a solution used when achieving endpoint hardening?

A. Cisco AMP
B. Cisco Umbrella
C. Cisco AnyConnect
D. Cisco Smart Install

Answer: D
Explanation: Cisco Smart Install is a method for hardening the network, used for zero-touch deployment of new access layer switches. Cisco AMP, Cisco Umbrella, and Cisco AnyConnect are all used specifically for hardening our endpoints.

Video Reference: Endpoint Hardening

3. Which of the following is not an advantage of a next generation firewall (NGFW)?

   A. Zero-touch deployment
   B. Streamlined architecture
   C. Deep packet inspection
   D. Better throughput rates

Answer: A
Explanation: Next generation firewalls allow for a streamlined architecture by integrating multiple security services into a single appliance, the ability to monitor traffic at OSI layers 2 through 7 with deep packet inspection, and better throughput rates through more robust hardware and streamlined software.

Video Reference: Next Generation Firewall (NGFW)

4. Which mechanism is used by Cisco Identity Services Engine (ISE) to assign security tags for access policy enforcement?

   A. TrustSec
   B. MACsec
   C. NAC
   D. MAB

Answer: A
Explanation: Cisco TrustSec is used by Cisco ISE to assign a security group tag (SGT) to each device at the egress point of a TrustSec capable device. Based on the SGT tag, certain access policies will be enforced elsewhere in the infrastructure. SGTs can be used by routers, switches, and firewalls on Cisco TrustSec capable devices in order to make forwarding decisions.

Video Reference: Cisco TrustSec

5. Which security standard is considered to be the wired equivalent of WPA2 protection used in wireless networks?

   A. MACsec
   B. NAC
   C. MAB
   D. TrustSec

Answer: A
Explanation: MACsec is a Layer 2 protocol that relies on AES to provide confidentiality and integrity, similar to WPA2. However, MACsec operates over a wired Ethernet connection. This is an extension to 802.1X that provides secure key exchange and mutual authentication between MACsec capable devices.

Video Reference: Media Access Control Security (MACsec)

6. Which piece of the Network Access Control (NAC) architecture receives extensible authentication protocol (EAP) packets and translates those into RADIUS packets?

   A. Supplicant
   B. Translator
   C. Authentication Server
   D. Authenticator

Answer: D
Explanation: The Authenticator is the piece of the Network Access Control (NAC) architecture that controls access to the network based on a client's authentication status. This is commonly a switch or wireless LAN controller. The Authenticator receives EAP packets from the client, where Supplicant software is installed in order to send identity credentials to the Authenticator. These are translated into RADIUS packets and forwarded to the Authentication Server in order to validate the client identity.

Video Reference: Network Access Control (NAC) with 802.1X

7. By default, how long does it take a Cisco Catalyst switch to consider 802.1X to be timed out before beginning MAC Authentication Bypass (MAB)?

   A. 30 seconds
   B. 60 seconds
   C. 90 seconds
   D. 120 seconds

Answer: C
Explanation: MAC Authentication Bypass must wait until 802.1X times out before attempting network access. By default, this value is set to 90 seconds on a Cisco Catalyst switch. It's common for administrators to lower this value in order to overcome client access issues caused by the delay, but it's important to be aware that setting the timer interval too low can result in 802.1X bypass happening unnecessarily.

Video Reference: MAC Authentication Bypass (MAB)