210-250 Q&As

Cisco Cybersecurity Fundamentals

Pass Cisco 210-250 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/210-250.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which one of the following statements is true regarding the CAPWAP tunneling protocol?

A. It is used to encapsulate data between the LWAP and the WLC.

B. It is used to encapsulate data between different standalone APs.

C. It is used to encapsulate data between the standalone AP and the wireless clients.

D. It is used to encapsulate data between the LWAP and the wireless clients.

Correct Answer: A

QUESTION 2

Which IDS system can detect attacks using encryption?

A. Network IDS deployed in inline mode

B. Network IDS deployed in promiscuous mode

C. Host-based IDS

D. Network IPS deployed in inline mode

Correct Answer: C

QUESTION 3

Stateful and traditional firewalls can analyze packets and judge them against a set of predetermined rules called access control lists (ACLs). They inspect which of the following elements within a packet? (Choose two.)

A. Session headers

B. NetFlow flow information

C. Source and destination ports and source and destination IP addresses

D. Protocol information

Correct Answer: CD

QUESTION 4

What is an advantage when deploying the Talos Intelligence Group security intelligence feed?

A. updated virus signatures for IT administrators to deploy on user end-stations.

B. updated geo-location database updates, to track malicious activities origins.

C. regular updates to ensure that the system uses up-to-date information to filter your network traffic.

D. archival intelligence feeds that are only obtained from the Internet storm center.

E. real-time cyber analytics feeds from leading governments around the globe.

Correct Answer: C

QUESTION 5

What is the main advantage of an SIEM compared to a normal log collector?

A. It provides log storage.

B. It provides log correlation.

C. It provides a GUI.

D. It provides a log search functionality

Correct Answer: B

QUESTION 6

Which of the following is an open source feed for threat data?

A. Cyber Squad ThreatConnect

B. BAE Detica CyberReveal

C. MITRE CRITs

D. Cisco AMP Threat Grid

Correct Answer: C

QUESTION 7

Which option is a purpose of port scanning?

A. Identify the Internet Protocol of the target system.

B. Determine if the network is up or down.

C. Identify which ports and services are open on the target host.

D. Identify legitimate users of a system.

Correct Answer: C

QUESTION 8

Malicious Windows operating system codes that share a single virtual address space, and can manage the system CPU and memory resources directly are running in which mode?

A. safe

B. user

C. kernel

D. privileged

Correct Answer: C

QUESTION 9

Which two statements about client-side web-based attacks are true? (Choose two.)

A. Attackers use clear and plain text to access the resources they desire to access.

B. Attackers use obfuscation to hide a URL within a message so the user will not notice the true URL.

C. Attackers rarely perform client-side web-based attacks because they have found easier and more effective ways to perform attacks.

D. Attackers use many tricks to fool the user into clicking on a URL link to a nefarious website.

Correct Answer: BD

QUESTION 10

Which one of the following statements best describes the purpose of a default route?

A. A default route sets the preferred path for multicast packets.

B. A default route is an optional entry that is used when no explicit path to a destination is found in the routing table.

C. A default route will flood the packet out of all connected ports.

D. A default route is just a placeholder in the route table until a new route is found.

Correct Answer: B

QUESTION 11

What is the purpose of the switched virtual interface on a multilayer switch?

A. enables the switch to perform QoS functions such as CBWFQ, LLQ, and traffic shaping

B. allows the multiprotocol switch to load balance traffic across trunk ports

C. provides basic Layer 3 functions for the Layer 2 switch ports assigned to a VLAN

D. prevents routing and bridge loops by creating broadcast and collision domains

Correct Answer: C

QUESTION 12

What is the Common Vulnerabilities and Exposures (CVE)?

A. An identifier of threats

B. A standard to score vulnerabilities

C. A standard maintained by OASIS

D. A standard for identifying vulnerabilities to make it easier to share data across tools, vulnerability repositories, and security services

Correct Answer: D

QUESTION 13

What are three goals of OpenSOC? (Choose three.)

A. to provide a collaborative open source community for development of an extensible and scalable advanced security analytics tool

B. to provide a collaborative open communication platform for network outages and performance monitoring

C. to encourage open communication for additional features and identification of deficiencies for a stable and functionally usable tool

D. to identify key feature enhancements to drive technology efforts around efficient security analytics

E. to identify key performance indicators for network device analysis and capacity planning

Correct Answer: ACD

QUESTION 14

What is an amplification attack?

A. An amplification attack is a form of directed DDoS attack in which the attacker\\'s packets are sent at a much faster rate than the victim\\'s packets.

B. An amplification attack is a form of reflected attack in which the response traffic (sent by the unwitting participant) is made up of packets that are much larger than those that were initially sent by the attacker (spoofing the victim).

C. An amplification attack is a type of man-in-the-middle attack.

D. An amplification attack is a type of data exfiltration attack.

Correct Answer: B

QUESTION 15

The Cisco OpenDNS dashboard page provides useful and important security information for security analysts. In which section of the dashboard are threats of malware or botnets displayed?

A. activity volume

B. message center

C. top identities

D. top domains

Correct Answer: B