Leads4Pass

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.leads4pass.com/210-250.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

After a file disposition changes from unknown to malicious, what is the next step that should be taken?

A. Run the file in a sandbox to verify if it is malicious and to determine the file behaviors.

B. Create a new IPS signature to detect the malicious file.

C. Go back to the system where the file was previously seen and quarantine the malicious file.

D. Run a file retrospective analysis in the cloud using machine learning to determine the file SHA.

Correct Answer: C

QUESTION 2

Which tool is commonly used in a Security Operations Center to aggregate logs sent by endpoint systems, firewalls, intrusion prevention systems, and NetFlow?

A. Cybersecurity Event Management

B. Security Information and Event Management system

C. Firepower Management Center

D. Security Information Management System

Correct Answer: B

QUESTION 3

Which AAA protocol allows for capabilities exchange?

A. RADIUS

B. TACACS+

C. Diameter

D. Kerberos

Correct Answer: C

QUESTION 4

Which evasion method involves performing actions slower than normal to prevent detection?

A. traffic fragmentation

B. tunneling

C. timing attack

D. resource exhaustion

Correct Answer: C

Reference:https://books.google.com/books?id=KIwLSddtAWsCandpg=PA58andlpg=PA58anddq=timing+attack+perform ing+actions+slower+than+normal+to+prevent+detectionandsource=blandots=9qu7ywV-mXandsig=_9lwcDDqWNaYlEe P7VkR0MPAOEandhl=enandsa=Xandved=0ahUKEwiRwo_P8vvRAhVKyoMKHaUlAUQQ6AEIITAB#v=onepageandq=ti ming%20attack%20performing%20actions%20slower%20than%20normal%20to%20prevent%20detectionandf=false

QUESTION 5

What is a Tor exit node?

A. The encrypted Tor network

B. The last Tor node or the "gateways" where the Tor encrypted traffic "exits" to the Internet

C. The Tor node that performs encryption

D. The Tor browser installed in your system in order to "exit" the Internet

Correct Answer: B

Latest 210-250 Dumps   210-250 VCE Dumps   210-250 Exam Questions