350-701$^{Q\&As}$

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

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

https://www.passapply.com/350-701.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

A. Nexus

B. Stealthwatch

C. Firepower

D. Tetration

Correct Answer: D

QUESTION 2

Which IPS engine detects ARP spoofing?

A. Atomic ARP Engine

B. Service Generic Engine

C. ARP Inspection Engine

D. AIC Engine

Correct Answer: A

QUESTION 3

When using Cisco AMP for Networks which feature copies a file to the Cisco AMP cloud for analysis?

A. Spero analysis

B. dynamic analysis

C. sandbox analysis

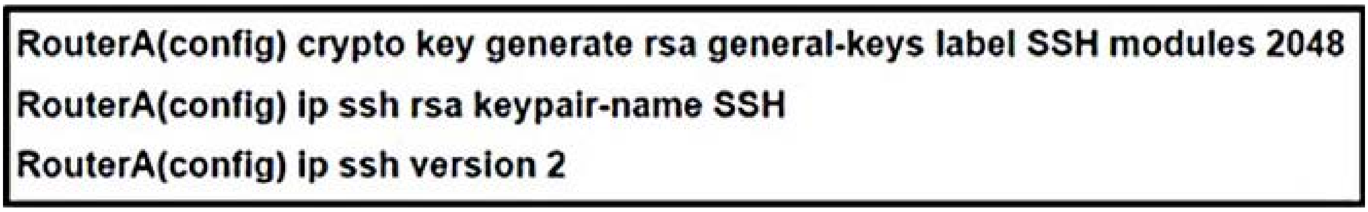
D. malware analysis

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc- config-guidev60/Reference_a_wrapper_Chapter_topic_here.html -> Spero analysis only uploads the signature of the (executable) files to the AMP cloud. It does not upload thewhole file. Dynamic analysis sends files to AMP ThreatGrid.Dynamic Analysis submits (the whole) files to Cisco Threat Grid (formerly AMP Threat Grid). Cisco ThreatGrid runs the file in a sandbox environment, analyzes the file\\'s behavior to determine whether the file ismalicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threatscore, you can view a dynamic analysis summary report with the reasons for the assigned threat score. Youcan also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well asscrubbed reports with limited data for files that your organization did not submit.Local malware analysis allows a managed device to locally inspect executables, PDFs, office documents, andother types of files for the most common types of malware, using a detection rule set provided by the CiscoTalos Security Intelligence and Research Group (Talos). Because local analysis does not query the AMP cloud,and does not run the file, local malware analysis saves time and system resources. -> Malware analysis doesnot upload files to anywhere, it only checks the files locally.There is no sandbox analysis feature, it is just a method of dynamic analysis that runs suspicious files in avirtual machine.

QUESTION 4

Refer to the exhibit.



```
RouterA(config) crypto key generate rsa general-keys label SSH modules 2048
RouterA(config) ip ssh rsa keypair-name SSH
RouterA(config) ip ssh version 2
```

An engineer must enable secure SSH protocols and enters this configuration. What are two results of running this set of commands on a Cisco router? (Choose two.)

A. generates RSA key pairs on the router

B. enables SSHv1 on the router

C. uses the FQDN with the label command

D. labels the key pairs to be used for SSH

E. generates AES key pairs on the router

Correct Answer: AD

QUESTION 5

How is ICMP used an exfiltration technique?

A. by flooding the destination host with unreachable packets

B. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address

C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host

D. by overwhelming a targeted host with ICMP echo-request packets

Correct Answer: C