www.CertBus.com

CERTBUS

NSE7_ATP-2.5^{Q&As}

Fortinet NSE 7 - Advanced Threat Protection 2.5

Pass Fortinet NSE7_ATP-2.5 Exam with 100% Guarantee

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

https://www.certbus.com/nse7_atp-2-5.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

What information does a scan job report include? (Choose two.)

A. Updates to the antivirus database

B. Summary of the file activity

C. Details about system files deleted of modified

D. Changes to the FortiSandbox configuration

Correct Answer: BC

QUESTION 2

FortiSandbox generates structured threat information exchange (STIX) packages for which of the following threats? (Choose two.)

A. Botnet connections

B. Malware

C. Intrusion attempts

D. Malicious URLs

Correct Answer: AC

Reference: https://docs.fortinet.com/document/fortisandbox/3.0.3/administration-guide/170699/ioc-package

QUESTION 3

Examine the FortiSandbox configuration on FortiMail shown in the exhibit, then answer the following question:

What does the Scan result expires in value specify?

A. How often the local scam results cache will expire on FortiMail.

B. How long FortiMail will wait to send a file or URI to FortiSandbox.

C. How long FortiMail will wait for a scan result from FortiSandbox.

D. How long FortiMail will query FortiSandbox for a scan result.

Correct Answer: B

QUESTION 4

Examine the FortiGate antivirus log detail shown in the exhibit, then answer the following question:

AntiVirus

|	
Profile Name	AV-AcmeCorp
Virus/Botnet	FSA/RISK_HIGH
Virus ID	8
Reference	http://www.fortinet.com/ve?vn=FSA%2FRISK_HIGH
Detection Type	Virus
Direction	incoming
Quarantine Skip	File-was-not-quarantined.
FortiSandbox Checksum	90877c1f6e7c97fb11249dc28dd16a3a3ddfac935d4f38c
Submitted for FortiSandbox	false
Message	File reported infected by Sandbox.

Which of the following statements is true?

A. FortiGate quarantined the file as a malware.

B. The file matched a FortiSandbox-generated malware signature.

C. The file was downloaded from www.fortinet.com.

D. The FSA/RISK_HIGH verdict was generated by FortiSandbox.

Correct Answer: C

QUESTION 5

Examine the FortiSandbox Scan Profile configuration shown in the exhibit, and then answer the following question:
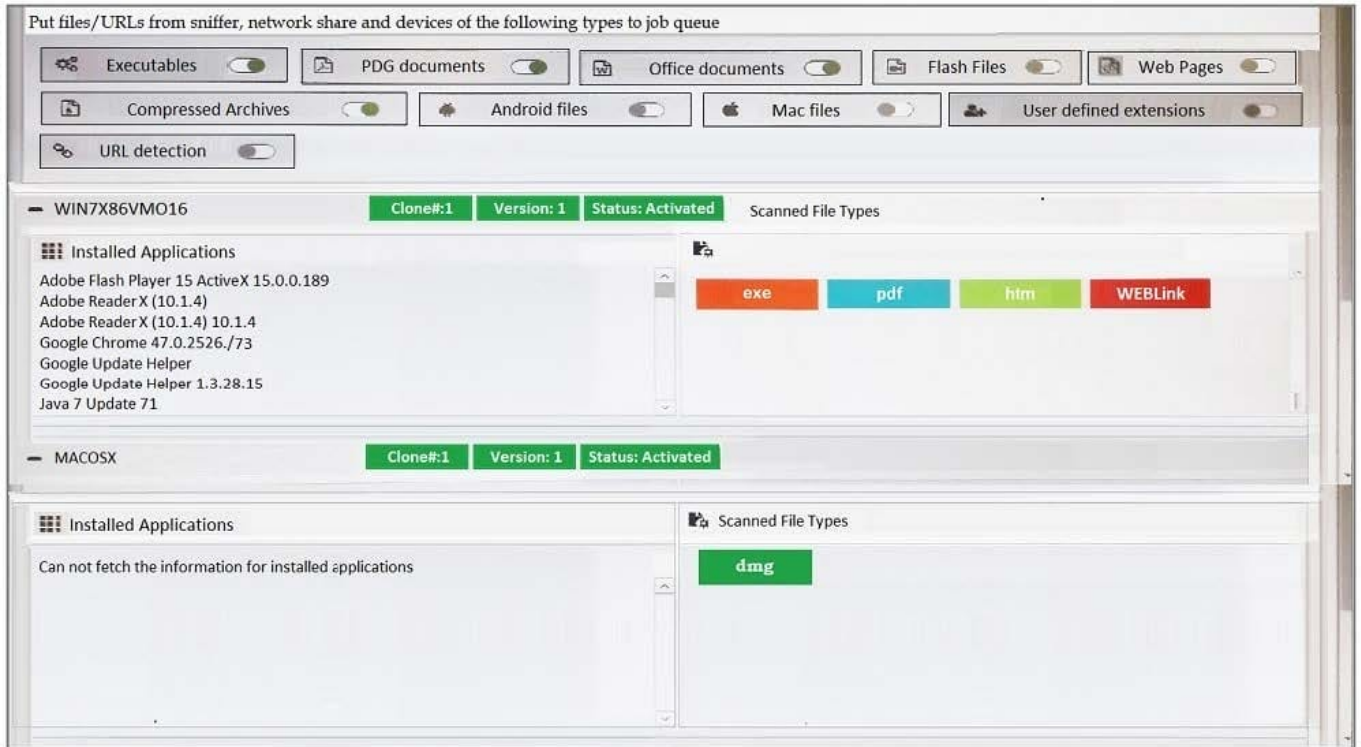
Based on the configuration, which of the following statements are true? (Choose two.)

A. PDF files will be inspected in the WIN7X86VM)16 VM.

B. URLs submitted using JSON API will not be inspected.

C. HTM files submitted using the management GUI will be inspected.

D. DMG files will be inspected in the MACOSX VM.

Correct Answer: CD

Latest NSE7_ATP-2.5
Dumps

NSE7_ATP-2.5 Practice
Test

NSE7_ATP-2.5 Braindumps