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.pass4itsure.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 advantage does sandboxing provide over traditional virus detection methods?

A. Heuristics detection that can detect new variants of existing viruses.

B. Pattern-based detection that can catch multiple variants of a virus.

C. Full code execution in an isolated and protected environment.

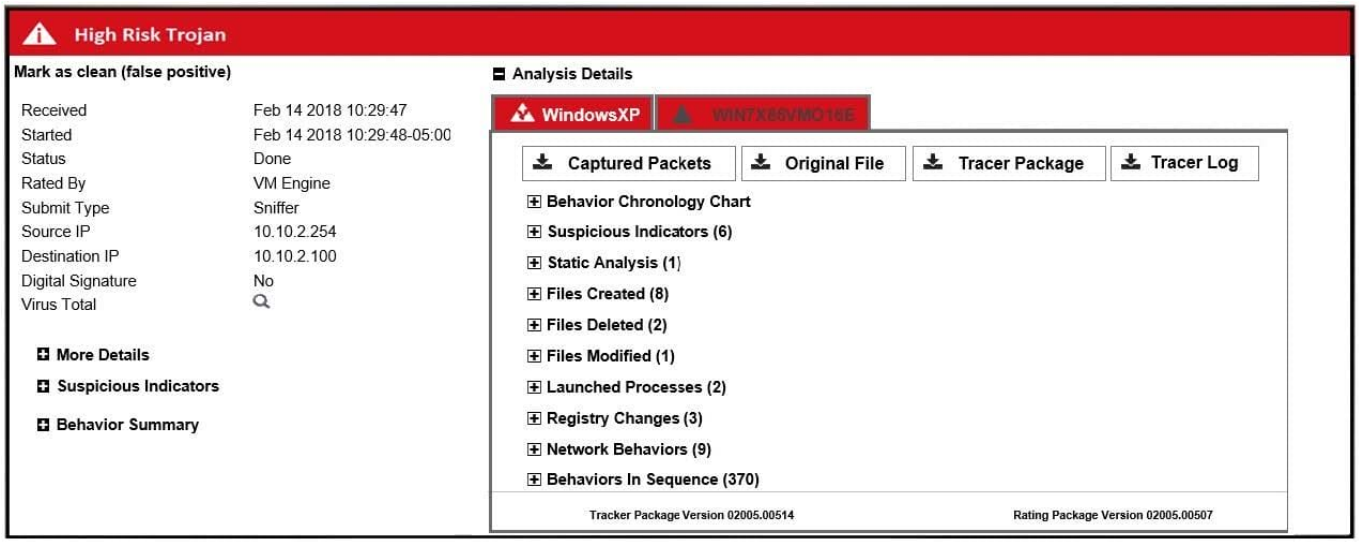
D. Code emulation as packets are handled in real-time.

Correct Answer: A

Heuristic analysis is capable of detecting many previously unknown viruses and new variants of current viruses. However, heuristic analysis operates on the basis of experience (by comparing the suspicious file to the code and functions of known viruses Reference: https://en.wikipedia.org/wiki/Heuristic_analysis

QUESTION 2

Examine the scan job report shown in the exhibit, then answer the following question: Which of the following statements are true regarding this verdict? (Choose two.)



A. The file contained malicious JavaScipt.

B. The file contained a malicious macro.

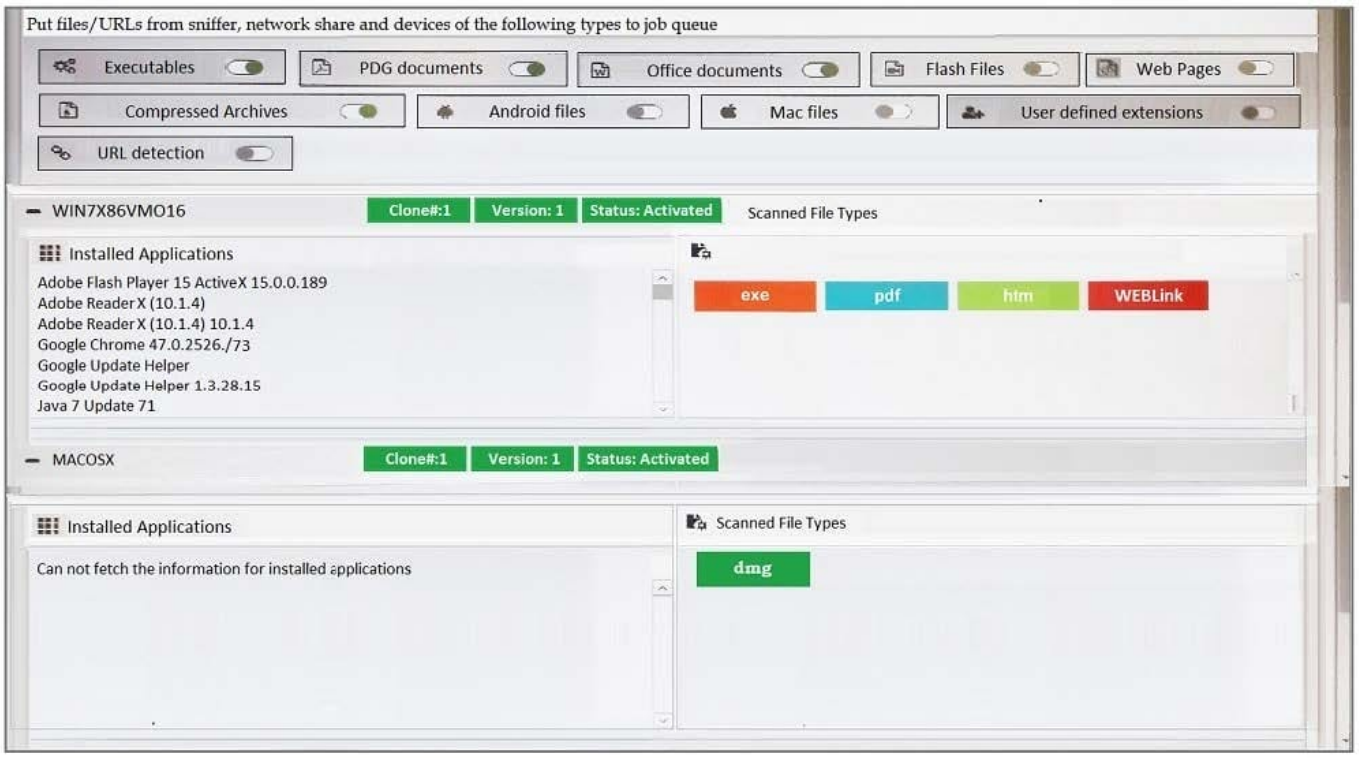
C. The file was sandboxed in two-guest VMs.

D. The file was extracted using sniffer-mode inspection.

Correct Answer: AC

QUESTION 3

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

QUESTION 4

When using FortiSandbox in sniffer-mode, you should configure FortiSandbox to inspect both inbound and outbound traffic.

What type of threats can FortiSandbox detect on inbound traffic? (Choose two.)

A. Botnet connections

B. Malware

C. Malicious URLs

D. Intrusion attempts

Correct Answer: AD

QUESTION 5

Which of the following are features of network share scanning of FortiSandbox? (Choose two.)

A. Move clean files to a separate network share.

B. Replace suspicious files with a replacement message.

C. Detect malicious URLs.

D. Detect network attacks.

Correct Answer: AB

Reference: https://help.fortinet.com/fsandbox/olh/2-5-1/Document/900_Scan%20Input/900_Network%20Share/100_Network%20Share.htm