NSE7_ATP-2.5 Q&As

Fortinet NSE 7 - Advanced Threat Protection 2.5

Pass Fortinet NSE7_ATP-2.5 Exam with 100% Guarantee

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

QUESTION 1

Which of the advanced threat protection solutions should you use to protect against an attacker may take during the lateral movement stage of the kill chain? (Choose two.)

A. FortiClient and FortiSandbox

B. FortiMail and FortiSandbox

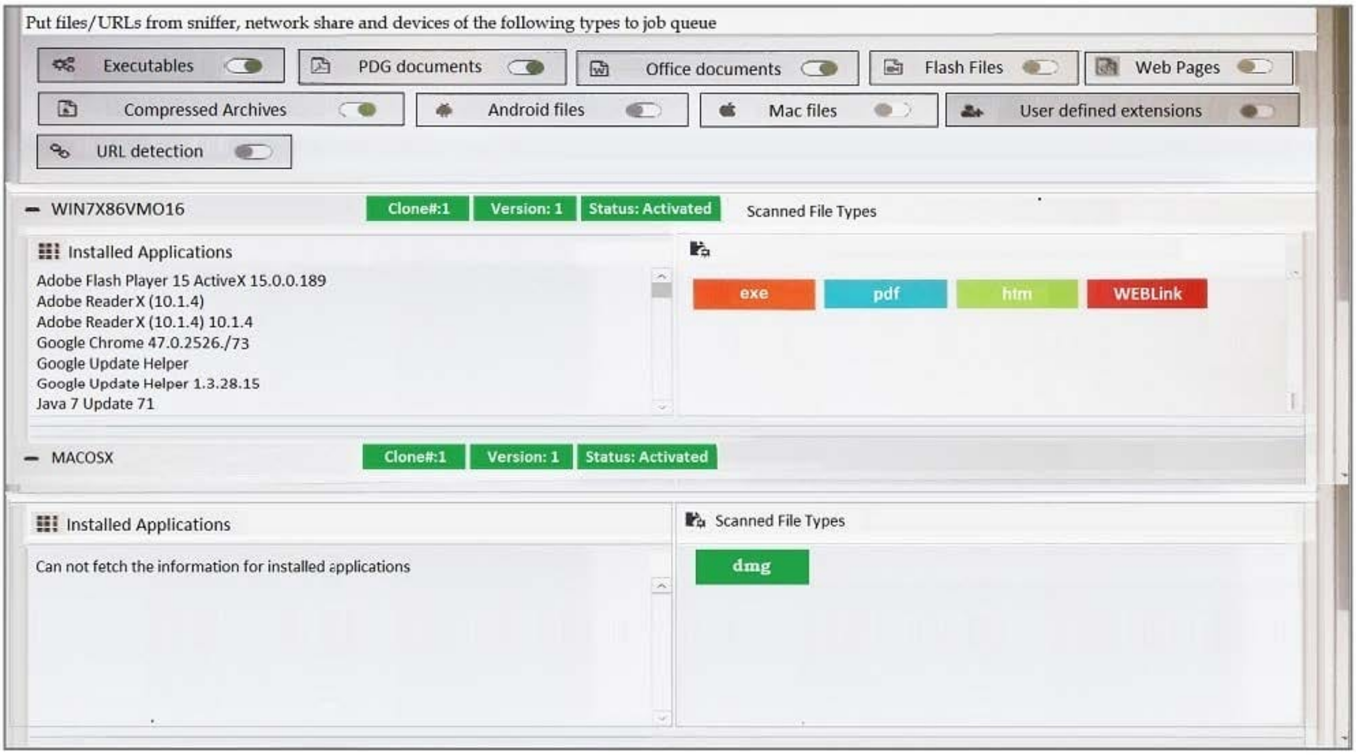
C. FortiGate and FortiSandbox

D. FortiWeb and FortiSandbox

Correct Answer: BD

QUESTION 2

Examine the FortiSandbox Scan Profile configuration shown in the exhibit, and then answer the following question:



Put files/URLs from sniffer, network share and devices of the following types to job queue

Executables
PDG documents
Office documents
Flash Files
Web Pages
Compressed Archives
Android files
Mac files
User defined extensions
URL detection

WIN7X86VMO16 Clone#:1 Version: 1 Status: Activated

Installed Applications
Adobe Flash Player 15 ActiveX 15.0.0.189
Adobe Reader X (10.1.4)
Adobe Reader X (10.1.4) 10.1.4
Google Chrome 47.0.2526./73
Google Update Helper
Google Update Helper 1.3.28.15
Java 7 Update 71

Scanned File Types
exe pdf htm WEBLink

MACOSX Clone#:1 Version: 1 Status: Activated

Installed Applications
Can not fetch the information for installed applications

Scanned File Types
dmg

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 3

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.

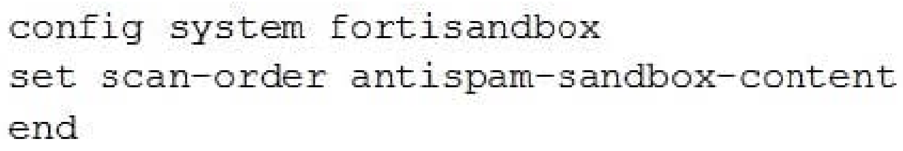
D. Code emulation as packets are handled in real-time.

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 4

Examine the CLI configuration, than answer the following question:



```
config system fortisandbox
set scan-order antispam-sandbox-content
end
```

Which of the following statements is true regarding this FortiMail\\'s inspection behavior?

A. Malicious URLs will be removed by antispam and replaced with a message.

B. Suspicious files not detected by antivirus will be inspected by FortiSandbox.

C. Known malicious URLs will be inspected by FortiSandbox.

D. Files are skipped by content profile will be inspected by FortiSandbox.

Correct Answer: C

QUESTION 5

FortiGate root VDOM is authorized and configured to send suspicious files to FortiSandbox for inspection. The administrator creates a new VDOM, and then generates some traffic so that the new VDOM sends a file to FortiSandbox for the first time.

Which of the following is true regarding this scenario?

A. FortiSandbox will accept the file, but not inspect it until the administrator manually configures the new VDOM on

FortiSandbox.

B. FortiSandbox will inspect all files based on the root VDOM authorization state and configuration.

C. FortiSandbox will accept the file, but not inspect it until the administrator manually authorizes the new VDOM on FortiSandbox.

D. By default, FortiSandbox will autoauthorize the new VDOM, and inspect files as they are received.

Correct Answer: B