NSE7_ATP-2.5$^{Q\&As}$

Fortinet NSE 7 - Advanced Threat Protection 2.5

Pass Fortinet NSE7_ATP-2.5 Exam with 100% Guarantee

QUESTION 1

Which FortiWeb feature supports file submission to FortiSandbox?

A. Attack signature

B. Credential stuffing defense

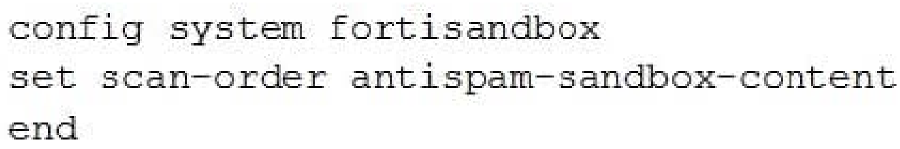
C. IP reputation

D. File security

Correct Answer: C

QUESTION 2

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 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.

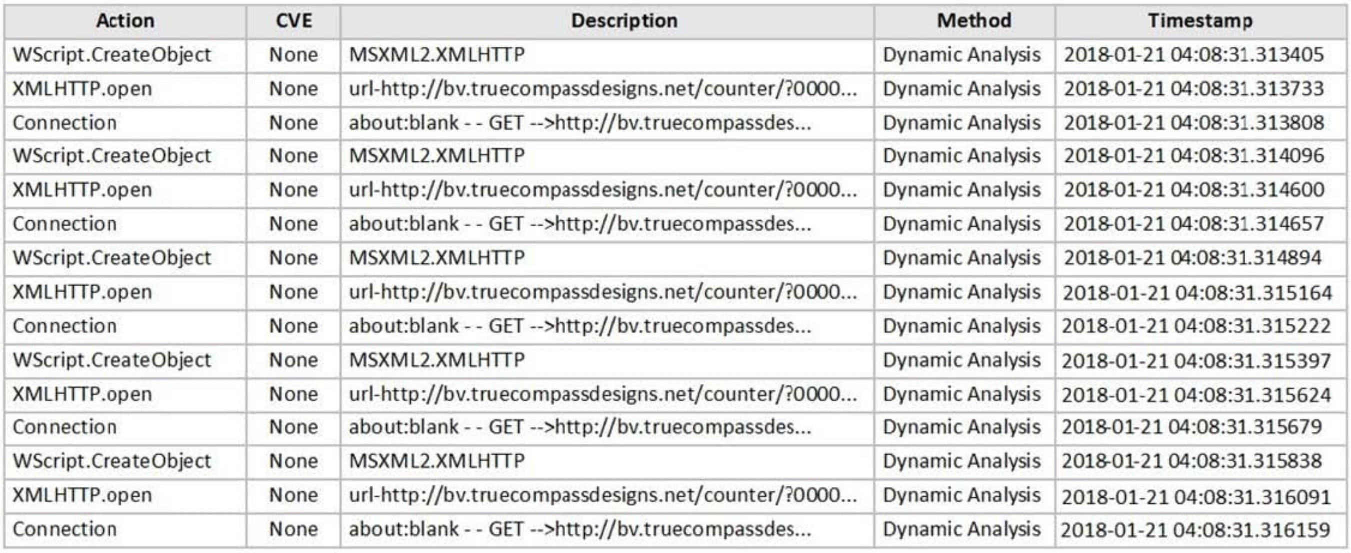
Correct Answer: A

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 virtual Simulator section of the scan job report shown in the exhibit, then answer the following question:



Action	CVE	Description	Method	Timestamp
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.313405
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.313733
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.313808
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.314096
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.314600
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.314657
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.314894
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.315164
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.315222
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.315397
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.315624
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.315679
WScript.CreateObject	None	MSXML2.XMLHTTP	Dynamic Analysis	2018-01-21 04:08:31.315838
XMLHTTP.open	None	url-http://bv.truecompassdesigns.net/counter/?0000...	Dynamic Analysis	2018-01-21 04:08:31.316091
Connection	None	about:blank - - GET -->http://bv.truecompassdes...	Dynamic Analysis	2018-01-21 04:08:31.316159

Based on the behavior observed by the virtual simulator, which of the following statements is the most likely scenario?

A. The file contained a malicious image file.

B. The file contained malicious JavaScript.

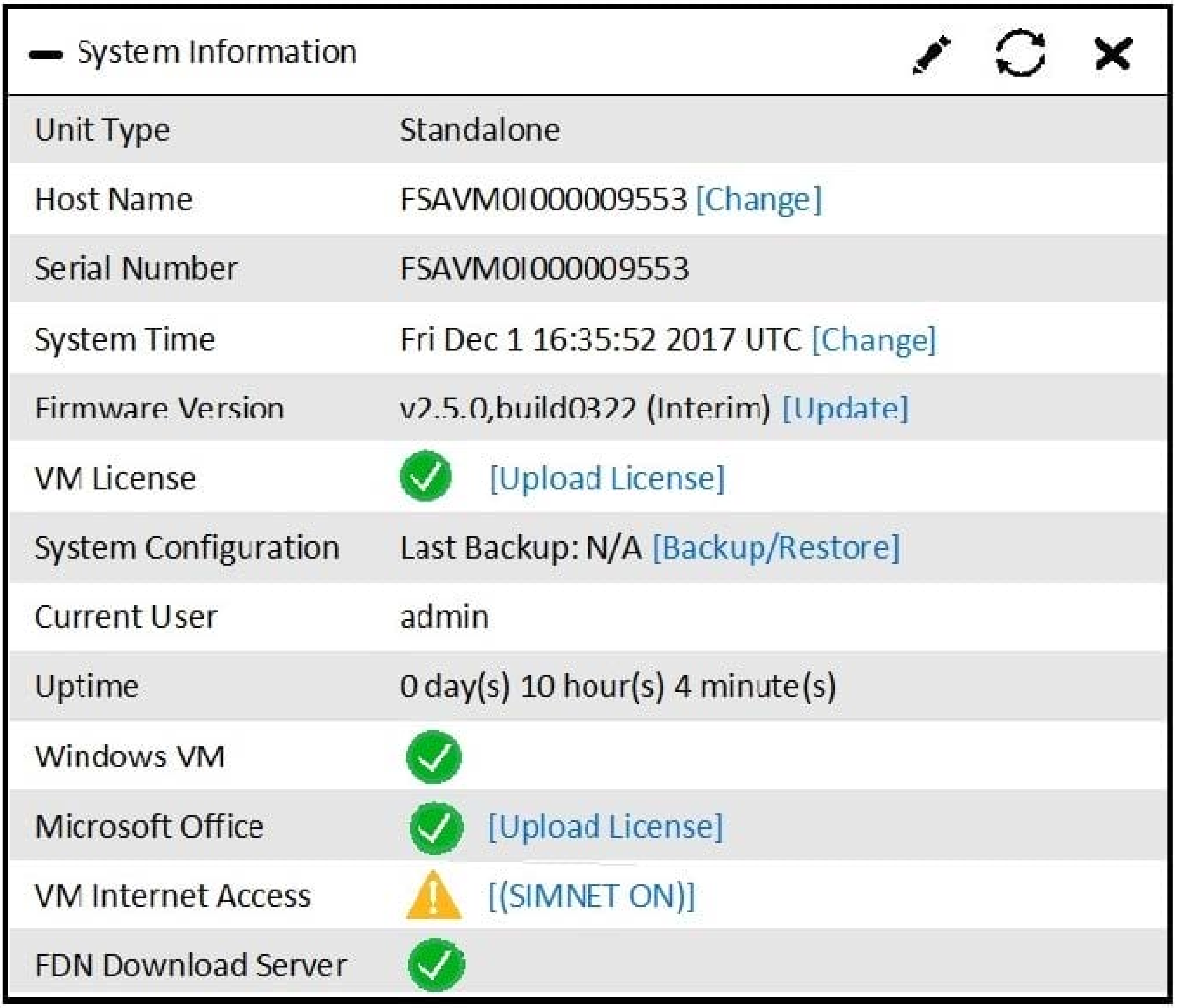
C. The file contained a malicious macro.

D. The file contained a malicious URL.

Correct Answer: B

QUESTION 5

Examine the System Information widget shown in the exhibit, then answer the following question:



System Information

Unit Type	Standalone
Host Name	FSAVM0I000009553 [Change]
Serial Number	FSAVM0I000009553
System Time	Fri Dec 1 16:35:52 2017 UTC [Change]
Firmware Version	v2.5.0,build0322 (Interim) [Update]
VM License	✓ [Upload License]
System Configuration	Last Backup: N/A [Backup/Restore]
Current User	admin
Uptime	0 day(s) 10 hour(s) 4 minute(s)
Windows VM	✓
Microsoft Office	✓ [Upload License]
VM Internet Access	⚠ [(SIMNET ON)]
FDN Download Server	✓

Which of the following inspections will FortiSandbox perform on samples submitted for sandboxing? (Choose two.)

A. URL rating on FQDN seen in DNS requests

B. IP reputation check on callback connections

C. Antivirus inspection on downloaded files

D. URL rating on HTTP GET requests

Correct Answer: CD