

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.leads4pass.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

Which of the following scan job report sections are generated by static analysis? (Choose two.)

- A. Office Behaviors
- B. Launched Processes
- C. Registry Changes
- D. Virtual Simulator

Correct Answer: CD

QUESTION 2

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 3

Examine the FortiClient configuration shown in the exhibit. then answer the following question:

Enable FortiSandbox Detection & Analysis

Address

Wait for FortiSandbox results before allowing file access
Timeout: seconds

Deny Access to file if sandbox is unreachable

What is the general rule you should follow when configuring the Timeout value for files submitted to FortiSandbox?

- A. It should be long enough for FortiSandbox to complete an antivirus scan of files.
- B. It should be long enough for FortiSandbox to complete a cloud query of file hashes.
- C. It should be long enough for FortiSandbox to complete sandbox analysis of files.
- D. It should be long enough for FortiSandbox to complete a static analysis of files.

Correct Answer: C

Reference https://help.fortinet.com/fclient/olh/5-6-6/FortiClient-5.6-Admin/800_Sandbox%20Detection/0605_Config%20submission%20and%20remediation.htm

QUESTION 4

Which advanced threat protection integration solution should you use to protect against out-of-band attack vectors, such as USB drives, used during the delivery stage of the kill chain?

- A. FortiGate and FortiSandbox
- B. FortiMail and FortiSandbox
- C. FortiWeb and FortiSandbox
- D. FortiClient and FortiSandbox

Correct Answer: B

Reference: <https://www.infosecpartners.com/fortimail-fortisandbox-perfect-partners/>

QUESTION 5

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	90877c1f6e7c97fb11249dc28dd16a3a3ddfacc935d4f38c
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

[NSE7_ATP-2.5 Practice Test](#)

[NSE7_ATP-2.5 Exam Questions](#)

[NSE7_ATP-2.5 Braindumps](#)