

DUMPSBOSS.COM

Fortinet NSE 7 - Advanced Threat Protection 2.5

Fortinet NSE7 ATP-2.5

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

Buy Premium PDF

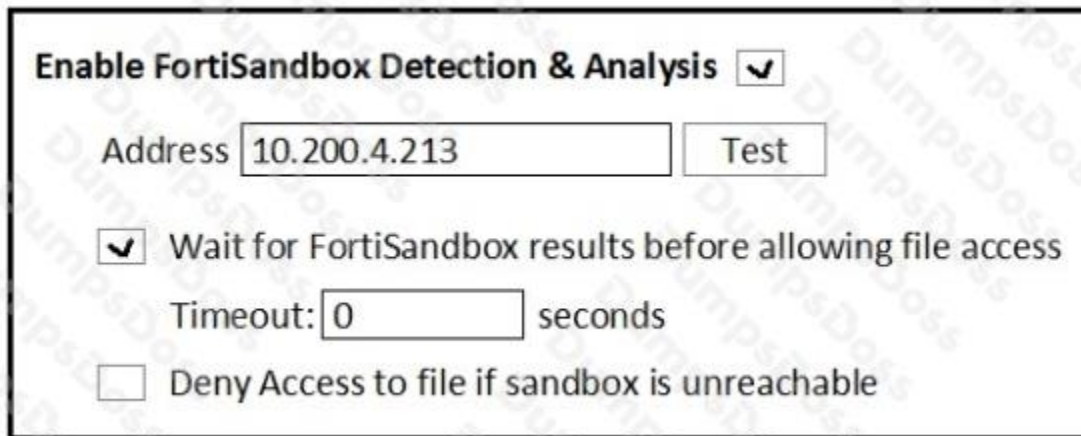
<https://dumpsboss.com>

support@dumpsboss.com

dumpsboss.com

QUESTION NO: 1

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



The screenshot shows the 'Enable FortiSandbox Detection & Analysis' configuration window. It includes a checkbox for 'Enable FortiSandbox Detection & Analysis' which is checked. Below it is an 'Address' field with the value '10.200.4.213' and a 'Test' button. There is also a checkbox for 'Wait for FortiSandbox results before allowing file access' which is checked, followed by a 'Timeout' field with the value '0' and the unit 'seconds'. At the bottom, there is an unchecked checkbox for '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.

ANSWER: C**Explanation:**

:

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

[Admin/800_Sandbox%20Detection/0605_Config%20submission%20and%20remediation.h tm](https://help.fortinet.com/fclient/olh/5-6-6/FortiClient-5.6-Admin/800_Sandbox%20Detection/0605_Config%20submission%20and%20remediation.htm)

QUESTION NO: 2

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

ANSWER: C D**QUESTION NO: 3**

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.

ANSWER: B**QUESTION NO: 4**

At which stage of the kill chain will an attacker use tools, such as nmap, ARIN, and banner grabbing, on the targeted organization's network?

- A. Exploitation
- B. Reconnaissance
- C. Lateral movement

D. Weaponization

ANSWER: B

QUESTION NO: 5

Which samples can FortiClient submit to FortiSandbox for analysis? (Choose two.)

- A. Downloads from emails
- B. URLs from web requests
- C. Command and control traffic
- D. Files from removable storage

ANSWER: A C