



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.passapply.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 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

Correct Answer: AC

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 Suspicious Indicators section of the scan job shown in the exhibit, then answer the following question:

**Suspicious Indicators (6)**

- ● ● ● ● ● ● ● ● collectgetlcon CVE-2009-0972 detected collab.getlcon
- ● ● ● ● ● ● ● ● collectgetlcon CVE-2009-0972 detected Collab.getlcon collab.getlcon
- ● ● ● ● ● ● ● ● collectEmailInfo CVE-2007-5659 detected Collab.collectEmailInfo
- ● ● ● ● ● ● ● ● ShellcodePattern detected
- ● ● ● ● ● ● ● ● Warning detected //warning CVE-NO-MATCH Shellcode Engine Binary Threshold

Which FortiSandbox component identified the vulnerability exploits?

- A. VM scan
- B. Antivirus scan
- C. Static analysis
- D. Cache check

Correct Answer: C

QUESTION 4

Which of the following are FortiWeb's roles when integrated with FortiSandbox? (Choose two.)

- A. Share threat information
- B. Prevent outbreaks
- C. Generate a verdict
- D. Block known threats

Correct Answer: AD

QUESTION 5

Which of the kill chain stages does Fortinet's advanced threat protection solution block? (Choose three.)

- A. Command and control
- B. Delivery
- C. Reconnaissance
- D. Lateral movement
- E. Weaponization

Correct Answer: ACD



VCE & PDF

PassApply.com

https://www.passapply.com/nse7_atp-2-5.html

2024 Latest passapply NSE7_ATP-2.5 PDF and VCE dumps Download

[Latest NSE7 ATP-2.5
Dumps](#)

[NSE7 ATP-2.5 VCE Dumps](#)

[NSE7 ATP-2.5 Exam
Questions](#)