

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

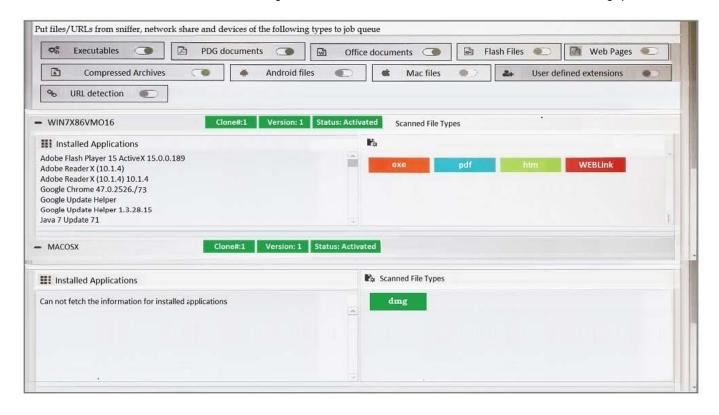
- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers





QUESTION 1

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



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 2

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 90877c1f6e7c97fb11249dc28dd16a3a3ddfac935d4f38c

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

QUESTION 3

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

Enable Fortis	Sandbox Detec	tion & Analy	ysis 🗸	
Address	10.200.4.213		Test	
✓ Wait	for FortiSandb	ox results b	efore allo	owing file access
Time	eout: 0	seconds		
Den	Access to file	if sandbox is	unreach	able



https://www.leads4pass.com/nse7_atp-2-5.html

2024 Latest leads4pass NSE7_ATP-2.5 PDF and VCE dumps Download

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

FortiSandbox generates structured threat information exchange (STIX) packages for which of the following threats? (Choose two.)

- A. Botnet connections
- B. Malware
- C. Intrusion attempts
- D. Malicious URLs

Correct Answer: AC

Reference: https://docs.fortinet.com/document/fortisandbox/3.0.3/administration-guide/170699/ioc-package

QUESTION 5

Which of the following advanced threat protection are capable of preventing patient-zero infections? (Choose two.)

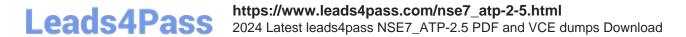
- A. FortiWeb and FortiSandbox
- B. FortiClient and FortiSandbox
- C. FortiMail and FortiSandbox
- D. FortiGate and FortiSandbox

Correct Answer: AD

FortiGate Enterprise Firewall Platform provides the industry\\'s highest- performing firewall capabilities, and Fortinet\\'s FortiGuard Security Subscription Services provide the industry\\'s highest level of threat research, intelligence, and analytics. Reference: https://www.fortinet.com/content/dam/fortinet/assets/alliances/2019/sb-fortinet-alliancesziften.pdf

Latest NSE7 ATP-2.5

NSE7 ATP-2.5 PDF Dumps NSE7 ATP-2.5 VCE Dumps



Dumps