Pass2Lead

https://Pass2Lead.com

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.pass2lead.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 advanced threat protection solutions should you use to protect against an attacker may take during the lateral movement stage of the kill chain? (Choose two.)

A. FortiClient and FortiSandbox

B. FortiMail and FortiSandbox

C. FortiGate and FortiSandbox

D. FortiWeb and FortiSandbox

Correct Answer: BD

QUESTION 2

Which FortiSandbox diagnostic command should you use to diagnose Internet connectivity issues on port3?

A. ping

B. tcpdump

C. test-network

D. traceroute

Correct Answer: D

Reference: https://dokumen.tips/documents/fortios-54-cookbook-fortinet-docs-fortinetknowledgebasetechnicaldocumentation-.html

QUESTION 3

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

Correct Answer: B

QUESTION 4

![Pass2Lead](https://Pass2Lead.com)
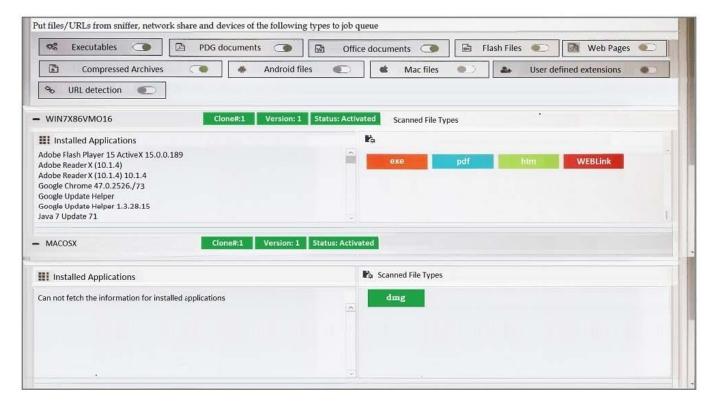When using FortiSandbox in sniffer-mode, you should configure FortiSandbox to inspect both inbound and outbound traffic.

What type of threats can FortiSandbox detect on inbound traffic? (Choose two.)

A. Botnet connections

B. Malware

C. Malicious URLs

D. Intrusion attempts

Correct Answer: AD

QUESTION 5

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