

# PSE-ENDPOINT<sup>Q&As</sup>

PSE: Endpoint – Professional

## Pass Palo Alto Networks PSE-ENDPOINT Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/pse-endpoint.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto  
Networks Official Exam Center

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



**QUESTION 1**

An administrator has installed Traps 4.0. The administrator wants to test the malware protections provided. What sample should they use to test the protections provided by Traps?

- A. A sample with a low number of hits in Virus Total
- B. A toolbar package known to be flagged as grayware by Traps
- C. A sample known to generate false positives in the production environment
- D. An MS Office document which contains a ransomware macro

Correct Answer: D

---

**QUESTION 2**

In a scenario where winword.exe, Microsoft Word application, is behaving abnormally, how would the administrator verify if Traps DLLs are injected to the process?

- A. Run `\\cytool policy winword.exe`
- B. Use Process Explore to find Traps DLLs injected to the process
- C. Open the add-ins tab in Word's options to find Traps add-in
- D. Use `\\Ninja mode\\` in the policy editing screen in the ESM to find winword.exe

Correct Answer: B

---

**QUESTION 3**

An administrator has a critical group of systems running Windows XP SP3 that cannot be upgraded. The administrator wants to evaluate the ability of Traps to protect these systems and the word processing applications running on them.

How should an administrator perform this evaluation?

- A. Run a known 2015 flash exploit on a Windows XP SP3 VM, and run an exploitation tool that acts as a listener. Use the results to demonstrate Traps capabilities.
- B. Run word processing exploits in a Windows 7 VM in a controlled and isolated environment. Document indicators of compromise and compare to Traps protection capabilities.
- C. Prepare a Windows 7 VM. Gather information about the word processing applications, determine if some of them are vulnerable, and prepare a working exploit for at least one of them. Execute with an exploitation tool.
- D. Gather information about the word processing applications and run them on a Windows XP SP3 VM. Determine if any of the applications are vulnerable and run the exploit with an exploitation tool.

Correct Answer: A

---

#### QUESTION 4

An administrator has decided to test Traps functionality using malware samples in an isolated nonproduction environment. In order to effectively test Traps, what three types of samples should the administrator avoid? (Choose three.)

- A. A sample with a low number of hits in Virus Total.
- B. An MS Office document which contains a ransomware macro.
- C. A sample known to be flagged as grayware by Traps.
- D. A freeware video application which spawns malicious processes.
- E. A sample known to generate false positives in the production environment.

Correct Answer: ABE

---

#### QUESTION 5

An ESM server's SSL certificate needs two Enhanced Key Usage purposes: Client Authentication and \_\_\_\_\_

- A. Server Authentication
- B. File Recovery
- C. IP Security User
- D. IP Security Tunnel Termination

Correct Answer: A

[PSE-ENDPOINT PDF Dumps](#)

[PSE-ENDPOINT Exam Questions](#)

[PSE-ENDPOINT Braindumps](#)