PSE-ENDPOINT Q&As

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.passapply.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

A company discovers through the agent health display in ESM Console that a certain Traps agent is not communicating with ESM Server. Administrators suspect that the problem relates to TLS/SSL. Which troubleshooting step determines if this is an SSL issue?

A. From the agent run the command: telnet (hostname) (port)

B. Check that the Traps service is running

C. From the agent run the command: ping (hostname)

D. Browse to the ESM hostname from the affected agent

Correct Answer: D

QUESTION 2

To ensure that the Traps VDI tool can obtain verdicts for all unknown files what are the things that needs to be checked? Assuming ESM Console and ESM Server are on different servers. (Choose two.)

A. ESM Server can access WildFire Server

B. Endpoint can access WildFire Server

C. ESM Console can access WildFire Server

D. Endpoint can access ESM Server

Correct Answer: AD

QUESTION 3

The administrator has added the following whitelist to the WildFire Executable Files policy.

*\mysoftware.exe

What will be the result of this whitelist?

A. users will not be able to run mysoftware.exe.

B. mysoftware.exe will be uploaded to WildFire for analysis

C. mysoftware.exe will not be analyzed by WildFire regardless of the file location.

D. mysoftware.exe will not be analyzed by WildFire, but only if executed from the C drive.

Correct Answer: B

QUESTION 4

An administrator is testing an exploit that is expected to be blocked by the JIT Mitigation EPM protecting the viewer application in use. No prevention occurs, and the attack is successful. In which two ways can the administrator determine the reason for the missed prevention? (Choose two.)

A. Check in the HKLM\SYSTEM\Cyvera\Policy registry key and subkeys whether JIT Mitigation is enabled for this application

B. Check if a Just-In-Time debugger is installed on the system

C. Check that the Traps libraries are injected into the application

D. Check that all JIT Mitigation functions are enabled in the HKLM\SYSTEM\Cyvera\Policy\Organization \Process\Default registry key

Correct Answer: AC

QUESTION 5

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