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.certbus.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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which set of modules must be loaded and configured when using Metasploit?

A. Attacker, payload

B. Exploit, payload

C. Exploit, malware

D. Malware, host

Correct Answer: C

QUESTION 2

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 3

Which is the proper order of tasks that an administrator needs to perform to successfully create and install Traps 4.x for macOS agents?

A. Download ClientUpgradePackage_4.x.x.zip from the support portal. Copy ClientUpgradePackage_4.x.x.zip to target endpoint. Unzip and run traps pkg.

B. Download ClientUpgradePackage.zip from the support portal. Create installation package on ESM using .zip file, download installpackage.zip file. Copy installpackage.zip to target endpoint. Unzip and run traps pkg.

C. Download Traps_macOS_4.x.x.zip from the support portal. Copy Traps_macOS_4.x.x.zip to target endpoint. Unzip and run traps pkg.

D. Download Traps_macOS_4.x.x.zip from the support portal. Create installation package on ESM using .zip file, download installpackage.zip file. Copy installpackage.zip to target endpoint. Unzip and run traps pkg.

Correct Answer: D

QUESTION 4

Which MSI command line parameters will successfully install a Traps agent using SSL and pointed to server ESM?

A. msiexec /i c:\traps.msi /qn TRAPS_SERVER=ESM USE_SSL_PRIMARY=1

B. msiexec /i c:\traps.msi /qn CYVERA_SERVER=ESM USE_SSL_PRIMARY=1

C. msiexec /i c:\traps.msi /qn ESM_SERVER=ESM USE_SSL_PRIMARY=1

D. msiexec /x c:\traps.msi /qn SERVER=ESM USE_SSL_PRIMARY=1

Correct Answer: B

QUESTION 5

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 6

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 7

An administrator is concerned about rogue installs of Internet Explorer. Which policy can be created to assure that Internet Explorer can only run from the \Program Files \Internet Explorer \directory?

A. An execution path policy to blacklist iexplore.exe, and whitelist entry for %programfiles%\iexplore.exe

B. An execution path policy to blacklist *\iexplore.exe. Trusted signers will allow the default iexplore.exe

C. A whitelist of *\iexplore.exe with an execution path restriction, and a blackfirst of %system% \iexplore.exe

D. An execution path policy to blacklist *\iexplore.exe, and a whitelist entry for %programfiles%\Internet Explorer\iexplore.exe

Correct Answer: D

QUESTION 8

In a scenario that macOS Traps logs failed to be uploaded to the forensic folder, where will the user on the macOS host be able to find to collected logs?

A. /ProgramData/Cyvera/Logs

B. /ProgramData/Cyvera/Everyone/Temp

C. /Library/Application Support/Cyvera/BITS Uploads/

D. /Library/Application Support/PaloAltoNetworks/Traps/Upload/

Correct Answer: D

QUESTION 9

Uploads to the ESM Sever are failing.

How can the mechanism for forensic and WildFire uploads be tested from the endpoint?

A. Use BITS commands in PowerShell to send a file to the ESM Server

B. Use curl to execute a POST operation

C. Use SCP commands from a ssh client to transfer a file to the ESM Server

D. Click Check-in now in the agent console

Correct Answer: D

QUESTION 10

Assume a Child Process Protection rule exists for powershell.exe in Traps v 4.0. Among the items on the blacklist is ipconfig.exe. How can an administrator permit powershell.exe to execute ipconfig.exe without altering the rest of the blacklist?

A. add ipconfig.exe to the Global Child Processes Whitelist, under Restriction settings.

B. Uninstall and reinstall the traps agent.

C. Create a second Child Process Protection rule for powershell.exe to whitelist ipconfig.exe.

D. Remove ipconfig.exe from the rule\\'s blacklist.

Correct Answer: A

PSE-ENDPOINT Practice Test PSE-ENDPOINT Study Guide PSE-ENDPOINT Braindumps