Free Questions for 300-215 by braindumpscollection

Shared by Hickman on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the transmogrify anti-forensics technique?

Options:

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

B- sending malicious files over a public network by encapsulation

C- concealing malicious files in ordinary or unsuspecting places

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

Answer:

D

Explanation:

https://www.csoonline.com/article/2122329/the-rise-of-anti-forensics.html#:~:text=Transmogrify%20is%20similarly%20wise%20to,a%20file%20from%2C%20say%2C%20.

Question 2

Question Type: MultipleChoice

Which scripts will search a log file for the IP address of 192.168.100.100 and create an output file named parsed_host.log while printing results to the console?

A.
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( "output/parsed_host.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "parsed_host.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

B.
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( "output/parsed_hosts.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "test_log.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

C.
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.10\". *$")
output_filename = os.path.normpath( "output/parsed_host.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "parsed_host.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

D.
```
import os
import re
line_regex = re.compile(r".*fwd=\"192.168.100.100\". *$")
output_filename = os.path.normpath( "output/parsed_host.log")
with open(output_filename, "w") as out_file:
        out_file.write("")
with open(output_filename, "a") as out_file:
        with open( "test_log.log", "r") as in_file"
          for line in in_file:
            if (line_regex.search(line)):
              print line
              out_file.write(line)
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

A

Question 3

Question Type: MultipleChoice

What is a concern for gathering forensics evidence in public cloud environments?

Options:

A- High Cost: Cloud service providers typically charge high fees for allowing cloud forensics.

B- Configuration: Implementing security zones and proper network segmentation.

C- Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.

D- Multitenancy: Evidence gathering must avoid exposure of data from other tenants.

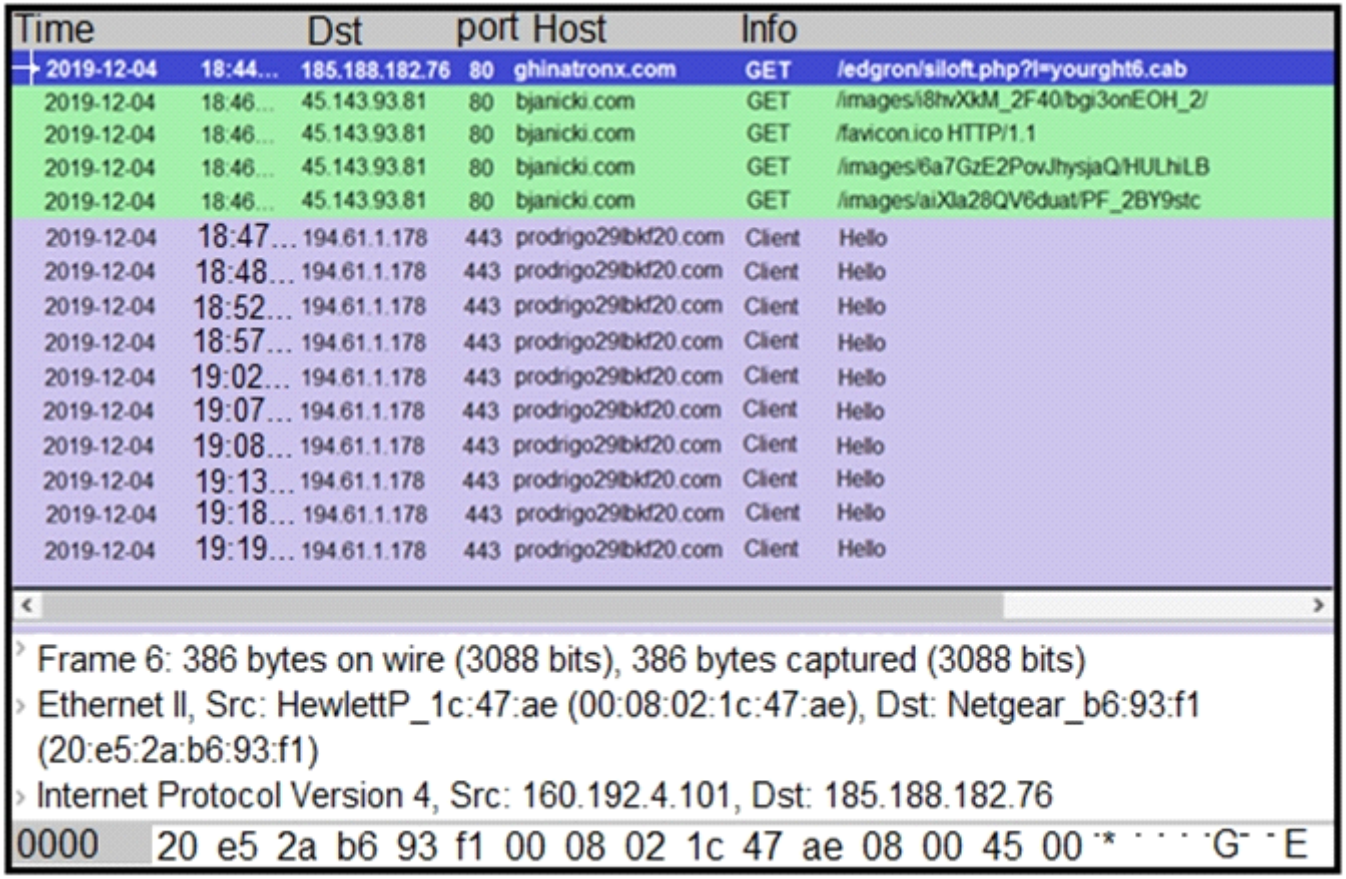
Answer:

D

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit.



A network engineer is analyzing a Wireshark file to determine the HTTP request that caused the initial Ursnif banking Trojan binary to download. Which filter did the engineer apply to sort the Wireshark traffic logs?

Options:

A- http.request.un matches

B- tls.handshake.type ==1

C- tcp.port eq 25

D- tcp.window_size ==0

Answer:

B

Explanation:

https://www.malware-traffic-analysis.net/2018/11/08/index.html https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
2708...	351.613329	167.203.102.117	192.168.1.159	TCP	174	15120 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.614781	52.27.161.215	192.168.1.159	TCP	174	15409 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615356	209.92.25.229	192.168.1.159	TCP	174	15701 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615473	149.221.46.147	192.168.1.159	TCP	174	15969 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.616366	192.183.44.102	192.168.1.159	TCP	174	16247 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.617248	152.178.159.141	192.168.1.159	TCP	174	16532 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618094	203.98.141.133	192.168.1.159	TCP	174	16533 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618857	115.48.48.185	192.168.1.159	TCP	174	16718 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.619789	147.29.251.74	192.168.1.159	TCP	174	17009 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.620622	29.158.7.85	192.168.1.159	TCP	174	17304 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.621398	133.119.25.131	192.168.1.159	TCP	174	17599 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.622245	89.99.115.209	192.168.1.159	TCP	174	17874 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.623161	221.19.65.45	192.168.1.159	TCP	174	18160 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624003	124.97.107.209	192.168.1.159	TCP	174	18448 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624765	140.147.97.13	192.168.1.159	TCP	174	18740 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment

What should an engineer determine from this Wireshark capture of suspicious network traffic?

Options:

A- There are signs of SYN flood attack, and the engineer should increase the backlog and recycle the oldest half-open TCP connections.

B- There are signs of a malformed packet attack, and the engineer should limit the packet size and set a threshold of bytes as a

countermeasure.

C- There are signs of a DNS attack, and the engineer should hide the BIND version and restrict zone transfers as a countermeasure.

D- There are signs of ARP spoofing, and the engineer should use Static ARP entries and IP address-to-MAC address mappings as a countermeasure.

Answer:

A

Question 6

Question Type: MultipleChoice

An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)

Options:

A- Restore to a system recovery point.

B- Replace the faulty CPU.

C- Disconnect from the network.

D- Format the workstation drives.

E- Take an image of the workstation.

Answer:

A, E

Question 7

Question Type: MultipleChoice

A security team is discussing lessons learned and suggesting process changes after a security breach incident. During the incident, members of the security team failed to report the abnormal system activity due to a high project workload. Additionally, when the incident was identified, the response took six hours due to management being unavailable to provide the approvals needed. Which two steps will prevent these issues from occurring in the future? (Choose two.)

Options:

A- Introduce a priority rating for incident response workloads.

B- Provide phishing awareness training for the fill security team.

C- Conduct a risk audit of the incident response workflow.

D- Create an executive team delegation plan.

E- Automate security alert timeframes with escalation triggers.

Answer:

A, E

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

Alert Message

SERVER-WEBAPP LOCK WebDAV Stack Buffer Overflow attempt

Impact:

CVSS base score 7.5

CVSS impact score 6.4

CVSS exploitability score 10.0

Confidentiality Impact PARTIAL

integrity Impact PARTIAL

availability Impact PARTIAL

After a cyber attack, an engineer is analyzing an alert that was missed on the intrusion detection system. The attack exploited a vulnerability in a business critical, web-based application and violated its availability. Which two migration techniques should the engineer recommend? (Choose two.)

Options:

A- encapsulation

B- NOP sled technique

C- address space randomization

D- heap-based security

E- data execution prevention

Answer:

C, E

Question 9

Question Type: MultipleChoice

A security team received an alert of suspicious activity on a user's Internet browser. The user's anti-virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address. Which two actions should be taken by the security analyst with the executable file for further analysis? (Choose two.)

Options:

A- Evaluate the process activity in Cisco Umbrella.

B- Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).

C- Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).

D- Analyze the Magic File type in Cisco Umbrella.

E- Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Answer:

B, C

Question 10

Question Type: MultipleChoice

A security team is discussing lessons learned and suggesting process changes after a security breach incident. During the incident, members of the security team failed to report the abnormal system activity due to a high project workload. Additionally, when the incident was identified, the response took six hours due to management being unavailable to provide the approvals needed. Which two steps will prevent these issues from occurring in the future? (Choose two.)

Options:

A- Introduce a priority rating for incident response workloads.

B- Provide phishing awareness training for the fill security team.

C- Conduct a risk audit of the incident response workflow.

D- Create an executive team delegation plan.

E- Automate security alert timeframes with escalation triggers.

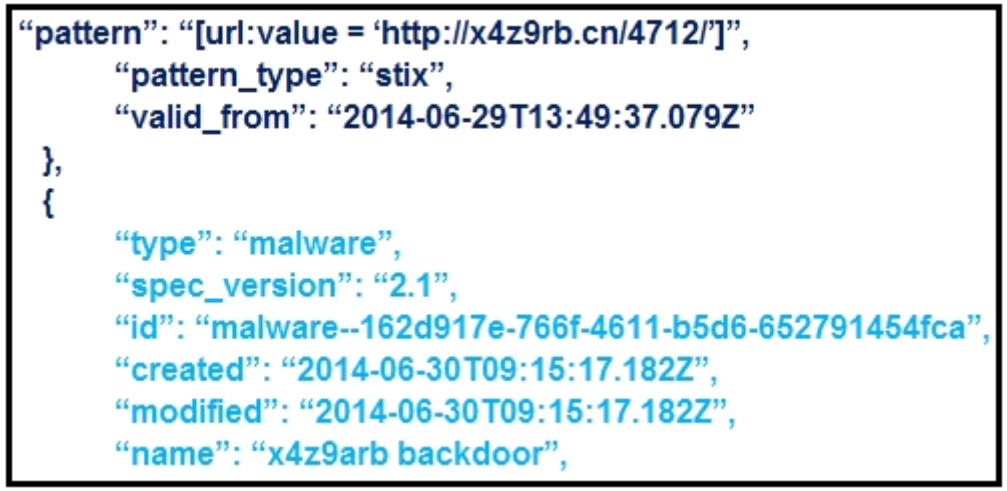
Answer:

A, E

Question 11

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 12

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