100% Money Back Guarantee

**Vendor:**Cisco

**Exam Code:**300-215

**Exam Name:**Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

**Version:**Demo

**QUESTION 1**

An engineer is analyzing a ticket for an unexpected server shutdown and discovers that the web-server ran out of useable memory and crashed.

Which data is needed for further investigation?

A. /var/log/access.log

B. /var/log/messages.log

C. /var/log/httpd/messages.log

D. /var/log/httpd/access.log

Correct Answer: B

---

**QUESTION 2**

```
indicator:Observable id= "example:Observable-Pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
<cybox:Object id= "example:Object-3a7aa9db-d082-447c-a422-293b78e24238">
<cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
<EmailMessageObj:Header>
<EmailMessageObj:From category= "e-mail">
<AddressObj:Address_Value condition= "Contains">@state.gov</AddressObj:Address Value>
</EmailMessageObj:From>
</EmailMessageObj:Header>
</cybox:Properties>
<cybox:Related_Objects>
<cybox:Related_Object>
<cybox:Properties xsi:type= "FileObj:FileObjectType">
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi type= 'cyboxVocabs:HashNameVocab- 1.0">MD5</cyboxCommon:Type>
<cyboxCommn:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelatiobshipVocab-
1.0">Contains</cybox:Relationship>
 </cybox:Related_Object>|
 </cybox:Related_Objects>
 </cybox:Object>
 </indicator:Observable>
```

Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)

A. Update the AV to block any file with hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

B. Block all emails sent from an @state.gov address.

C. Block all emails with pdf attachments.

D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

E. Block all emails with subject containing "cf2b3ad32a8a4cfb05e9dfc45875bd70".

Correct Answer: AB

---

**QUESTION 3**

DRAG DROP

Drag and drop the steps from the left into the order to perform forensics analysis of infrastructure networks on the right.

Select and Place:

Correct Answer:

Reference: https://subscription.packtpub.com/book/networking_and_servers/9781789344523/1/ch01lvl1sec12/network-forensics-investigation-methodology

---

**QUESTION 4**

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)
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

---

**QUESTION 5**

A security team received reports of users receiving emails linked to external or unknown URLs that are non-returnable and non-deliverable. The ISP also reported a 500% increase in the amount of ingress and egress email traffic received. After detecting the problem, the security team moves to the recovery phase in their incident response plan. Which two actions should be taken in the recovery phase of this incident? (Choose two.)

A. verify the breadth of the attack

B. collect logs

C. request packet capture

D. remove vulnerabilities

E. scan hosts with updated signatures

Correct Answer: DE

---

**QUESTION 6**

**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

Refer to the exhibit. 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.)

A. encapsulation

B. NOP sled technique

C. address space randomization

D. heap-based security

E. data execution prevention

Correct Answer: CE

---

**QUESTION 7**

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.)

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).

Correct Answer: BC

---

**QUESTION 8**

```
84.55.41.57 - -[17/Apr/2016:06:57:24 +0100] "GET/wordpress/wp-login.php HTTP/1.1" 200 1568 "-"
84.55.41.57 - -[17/Apr/2016:06:57:31 +0100] "POST/wordpress/wp-login.php HTTP/1.1" 302 1150
"http://www.example.com/wordpress/wp-login.php"


84.55.41.57 - -[17/Apr/2016:06:57:31 +0100] "GET/wordpress/wp-admin/ HTTP/1.1" 200 12905
"http://www.example.com/wordpress/wp-login.php"
84.55.41.57 - -[17/Apr/2016:07:00:32 +0100] "POST/wordpress/wp-admin/admin-ajax.php HTTP/1.1"
200 454 "http://www.example.com/wordpress/wp-admin/"


84.55.41.57 - -[17/Apr/2016:07:11:48 +0100 "GET/wordpress/wp-admin/plugin-install.php HTTP/1.1"
200 12459 "http://www.example.com/wordpress/wp-admin/plugin-install.php?tab=upload"
 84.55.41.57 - -[17/Apr/2016:07:16:06 +0100] "GET /wordpress/wp-admin/update.php? action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca HTTP/1.1" 200 5698


"http://www.example.com/wordpress/wp-admin/plugin install.php?tab-search&s-file+permission"
 84.55.41.57 - -[17/Apr/2016:07:18:19 +0100] "GET /wordpress/wp-
admin/plugins.php?action=activat&plugin=file-manager%2Ffile-manager.php&_wpnonce=bf932ee530
HTTP/1.1" 302.451 "http://www.example.com/wordpress/wp-admin/update.php?action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca"


84.55.41.57 - -[17/Apr/2016:07:21:46 +0100] "GET /wordpress/wp-admin/admin-ajax.php?
action=connector&cmd=upload&target=l1_d3AtY29udGVudA&name%5B%5D=r57.php&FILES
=&_=1460873968131 HTTP/1.1" 200 731 "http://www.example.com/wordpress/wp-admin/admin.php?
page=fie-manager_settings"


84.55.41.57 - -[17/Apr/2016:07:22:53+0100] "GET /wordpress/wp-content/r57.php HTTP/1.1" 200 9036 "-"
84.55.41.57- -[17/Apr/2016:07:32:24 +0100] "POST /wordpress/wp-content/r57.php?14 HTTP/1.1" 200
8030 "http://www.example.com/wordpress/wp-content/r57.php?14"
84.55.41.57 - -[17/Apr/2016:07:29:21 +0100] "GET /wordpress/wp-content/r57.php?29 HTTP/1.1" 200
8391 "http://www.example.com/wordpress/wp-content/r57.php?28"
```

Refer to the exhibit. Which two determinations should be made about the attack from the Apache access logs? (Choose two.)

A. The attacker used r57 exploit to elevate their privilege.

B. The attacker uploaded the word press file manager trojan.

C. The attacker performed a brute force attack against word press and used sql injection against the backend database.

D. The attacker used the word press file manager plugin to upoad r57.php.

E. The attacker logged on normally to word press admin page.

Correct Answer: CD

---

**QUESTION 9**

An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action the engineer should take?

A. Upload the file signature to threat intelligence tools to determine if the file is malicious.

B. Monitor processes as this a standard behavior of Word macro embedded documents.

C. Contain the threat for further analysis as this is an indication of suspicious activity.

D. Investigate the sender of the email and communicate with the employee to determine the motives.

Correct Answer: A

---

**QUESTION 10**

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

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.

Correct Answer: D

Reference: https://www.researchgate.net/publication/307871954_About_Cloud_Forensics_Challenges_and_Solutions

---

**QUESTION 11**

Refer to the exhibit. According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name:iraniansk.com

B. Server: nginx

C. Hash value: 5f31ab113af08=1597090577

D. filename= "Fy.exe"

E. Content-Type: application/octet-stream

Correct Answer: CE

---

**QUESTION 12**

| 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 |

Refer to the exhibit. 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?

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.

Correct Answer: D