300-215Q&As

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Pass Cisco 300-215 Exam with 100% Guarantee

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

https://www.certbus.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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 2

What is the steganography anti-forensics technique?

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

Correct Answer: A

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

QUESTION 3

```
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 4

```
        function decrypt(crypted, key)
On Error Resume Next

UUf  = crypted
sJs = "" '!!!
 wWLu = ""
 FETw = 1
        for i=1 to len(UUf)
 if ( asc(mid(UUF, i, 1)) > 47 and asc(mid(UUf, i, 1)) < 58) then
 sJs = sJs + mid(UUf, i, 1) '!!!
 FETw = 1
 else
 if FETw = 1 then
 NEL = CInt (sJs) '!!!
 VlxJ = XOR_Func(NEL, key) '!!!
 wWLu = wWLu + Chr(VlxJ) '!!!
 end if
  sJs = ""
 FETw = 0
 end if
 vkB = bEBk or CFc
next
 decrypt = wWLu
 end function
        function XOR_Func(qit, ANF)
 On Error Resume Next
 sCLx = qit xor ANF
 XOR_Func = sCLx

 end function
```

Refer to the exhibit. Which type of code created the snippet?

A. VB Script

B. Python

C. PowerShell

D. Bash Script

Correct Answer: A

QUESTION 5

An attacker embedded a macro within a word processing file opened by a user in an organization\\'s legal department. The attacker used this technique to gain access to confidential financial data. Which two recommendations should a security expert make to mitigate this type of attack? (Choose two.)

A. controlled folder access

B. removable device restrictions

C. signed macro requirements

D. firewall rules creation

E. network access control

Correct Answer: AC

QUESTION 6

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 7

Which information is provided bout the object file by the "-h" option in the objdump line command objdump ? oasys ? vax ? fu.o?

A. bfdname

B. debugging

C. help

D. headers

Correct Answer: D

Reference: https://sourceware.org/binutils/docs/binutils/objdump.html

QUESTION 8

An employee receives an email from a "trusted" person containing a hyperlink that is malvertising. The employee clicks the link and the malware downloads. An information analyst observes an alert at the SIEM and engages the cybersecurity team to conduct an analysis of this incident in accordance with the incident response plan. Which event detail should be included in this root cause analysis?

A. phishing email sent to the victim

B. alarm raised by the SIEM

C. information from the email header

D. alert identified by the cybersecurity team

Correct Answer: B

QUESTION 9

```
<indicator:Observable id= "example:Observable-9c9869a2-f822-4682-bda4-e89d31b18704">
        <cybox:Object id= "example:EmailMessage-9d56af8e-5588-4ed3-affd-bd769ddd7fe2">
         <cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
          <EmailMessageObj:Attachments>
              <EmailMessageObj:File object_reference= "example:File-c182bcb6-8023-44a8-b340-157295abc8a6"/>
          </EmailMessageObj:Attachments>
      </cybox:Properties>
      <cybox:Related_Objects>
        <cybox:Related_Object id= "example:File-c182bcb6-8023-44a8-b340-157295abc8a6"
         <cybox:Properties xsi:type= "FileObj:FileObjectType">
              <FileObj:File_Name condition= "StartsWith">Final Report</FileObj:File_Name>
              <FileObj:File_Extension condition= "Equals">doc.exe</FileObj:File_Extension>
         </cybox:Properties>
        <cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelationshipVocab-1.1">Contains</cybox:Relationship>
      </cybox:Related_Object>
    </cybox:Related_Objects>
  </cybox:Object>
</indicator:Observable>
```

Refer to the exhibit. Which determination should be made by a security analyst?

A. An email was sent with an attachment named "Grades.doc.exe".

B. An email was sent with an attachment named "Grades.doc".

C. An email was sent with an attachment named "Final Report.doc".

D. An email was sent with an attachment named "Final Report.doc.exe".

Correct Answer: D

QUESTION 10

What are YARA rules based upon?

A. binary patterns

B. HTML code

C. network artifacts

D. IP addresses

Correct Answer: A

Reference: https://en.wikipedia.org/wiki/YARA#:~:text=YARA%20is%20the%20name%20of,strings%20and%20a%20boolean%20expression.