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.leads4pass.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which tool conducts memory analysis?

A. MemDump

B. Sysinternals Autoruns

C. Volatility

D. Memoryze

Correct Answer: C

Reference: https://resources.infosecinstitute.com/topic/memory-forensics-and-analysis-using-volatility/

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

```
        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 4

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 5

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 6

```
alert tcp $LOCAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg: "WEB-IIS unicode
directory traversal attempt"; flow:to_server, established; content: "/..%c0%af../";
nocase; classtype:web-application-attack; reference:cve, CVE-2000-0884; threshold:
type limit, track_by_dst, count 1, seconds 60; sid: 981; rev6;)
```

Refer to the exhibit. A company that uses only the Unix platform implemented an intrusion detection system. After the initial configuration, the number of alerts is overwhelming, and an engineer needs to analyze and classify the alerts. The highest number of alerts were generated from the signature shown in the exhibit. Which classification should the engineer assign to this event?

A. True Negative alert

B. False Negative alert

C. False Positive alert

D. True Positive alert

Correct Answer: C

QUESTION 7

A scanner detected a malware-infected file on an endpoint that is attempting to beacon to an external site. An analyst has reviewed the IPS and SIEM logs but is unable to identify the file\\'s behavior. Which logs should be reviewed next to evaluate this file further?

A. email security appliance

B. DNS server

C. Antivirus solution

D. network device

Correct Answer: B

QUESTION 8

An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

A. An engineer should check the list of usernames currently logged in by running the command $ who | cut –d' ' -f1| sort | uniq

B. An engineer should check the server\\'s processes by running commands ps -aux and sudo ps -a.

C. An engineer should check the services on the machine by running the command service -status-all.

D. An engineer should check the last hundred entries of a web server with the command sudo tail -100 /var/log/apache2/access.log.

Correct Answer: D

QUESTION 9

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 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.

QUESTION 11

Refer to the exhibit. What is the IOC threat and URL in this STIX JSON snippet?

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/\\'

Correct Answer: D

QUESTION 12

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 13

00386078	64	44	45	33	4C	6A	41	34	4C	6A	4D	78	4C	6B	5A	44
00386088	4D	44	59	78	4E	79	34	31	4E	54	41	32	4C	6A	55	31
00386098	4D	44	59	75	4E	6A	67	7A	4E	77	3D	3D	00	AB	AB	AB

Refer to the exhibit. Which encoding technique is represented by this HEX string?

A. Unicode

B. Binary

C. Base64

D. Charcode

Correct Answer: B

Reference: https://www.suse.com/c/making-sense-hexdump/

QUESTION 14

Over the last year, an organization\\'s HR department has accessed data from its legal department on the last day of each month to create a monthly activity report. An engineer is analyzing suspicious activity alerted by a threat

intelligence platform that an authorized user in the HR department has accessed legal data daily for the last week. The engineer pulled the network data from the legal department\\'s shared folders and discovered above average-size data dumps. Which threat actor is implied from these artifacts?

A. privilege escalation

B. internal user errors

C. malicious insider

D. external exfiltration

Correct Answer: C

QUESTION 15

What is a use of TCPdump?

A. to analyze IP and other packets

B. to view encrypted data fields

C. to decode user credentials

D. to change IP ports

Correct Answer: A