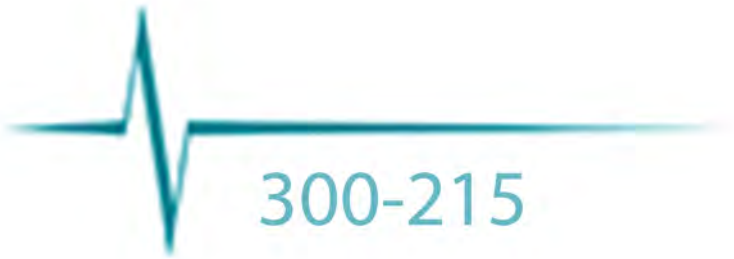
Practice Exam Questions



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

EXAMKILLER

Help Pass Your Exam At First Try

Cisco

Exam 300-215

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

Version: 3.0

[Total Questions: 59]

Question No : 1

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".

Answer: A,B

Question No : 2

What is the function of a disassembler?

A. aids performing static malware analysis
B. aids viewing and changing the running state
C. aids transforming symbolic language into machine code
D. aids defining breakpoints in program execution

Answer: A
Reference:
https://scholar.google.co.in/scholar?q=disassembler+aids+performing+static+malware

+analysis&hl=en&as_sdt=0&as_vis=1&oi=scholart

Question No : 3

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?

A. spoofing
B. obfuscation
C. tunneling
D. steganography

Answer: D
Reference: https://doi.org/10.5120/1398-1887
https://www.carbonblack.com/blog/steganography-in-the-modern-attack-landscape/

Question No : 4

An “unknown error code” is appearing on an ESXi host during authentication. An engineer checks the authentication logs but is unable to identify the issue. Analysis of the vCenter agent logs shows no connectivity errors. What is the next log file the engineer should check to continue troubleshooting this error?

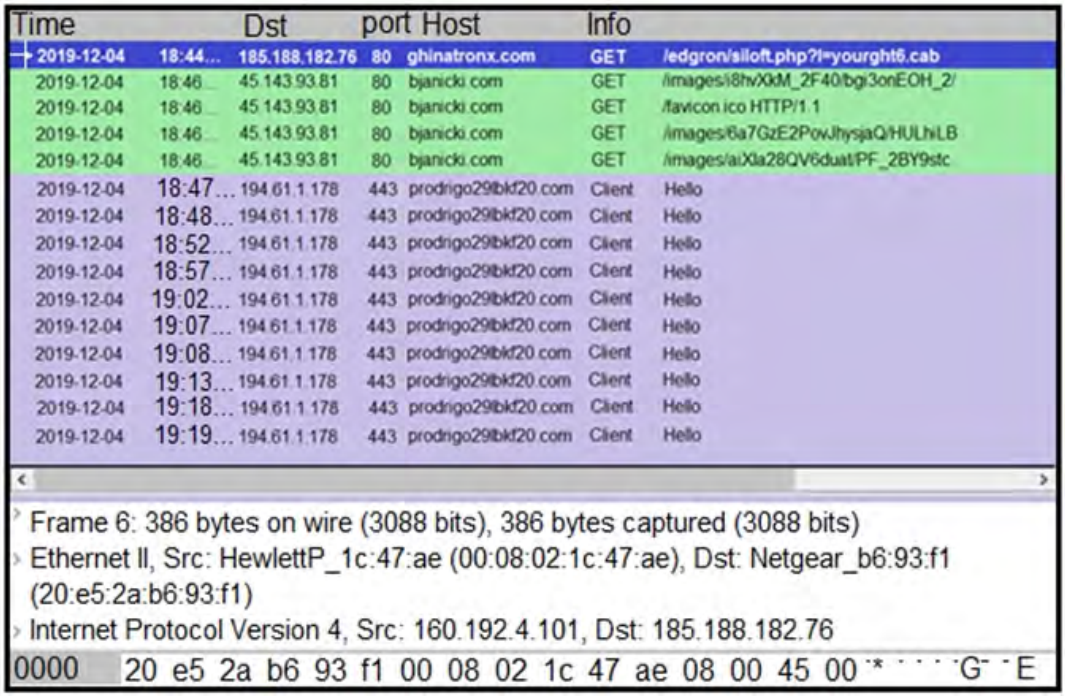
A. /var/log/syslog.log
B. /var/log/vmksummary.log
C. var/log/shell.log
D. var/log/general/log

Answer: A

Reference: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.monitoring.doc/GUID- 832A2618-6B11-4A28-9672-93296DA931D0.html

Question No : 5

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?

A. http.request.un matches
B. tls.handshake.type ==1
C. tcp.port eq 25
D. tcp.window_size ==0

Answer: B

Reference:

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

Question No : 6

Refer to the exhibit.

```
<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>
```

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”.

Answer: D

Question No : 7

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.)

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 No : 8

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).

Answer: B,C

Question No : 9

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.)

A. Inspect registry entries
B. Inspect processes.
C. Inspect file hash.
D. Inspect file type.
E. Inspect PE header.

Answer: B,C
Reference: https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually-d02744f7c43a

Question No : 10

An organization recovered from a recent ransomware outbreak that resulted in significant business damage. Leadership requested a report that identifies the problems that triggered the incident and the security team's approach to address these problems to prevent a reoccurrence. Which components of the incident should an engineer analyze first for this report?

A. impact and flow
B. cause and effect
C. risk and RPN
D. motive and factors

Answer: D

Question No : 11

Refer to the exhibit.

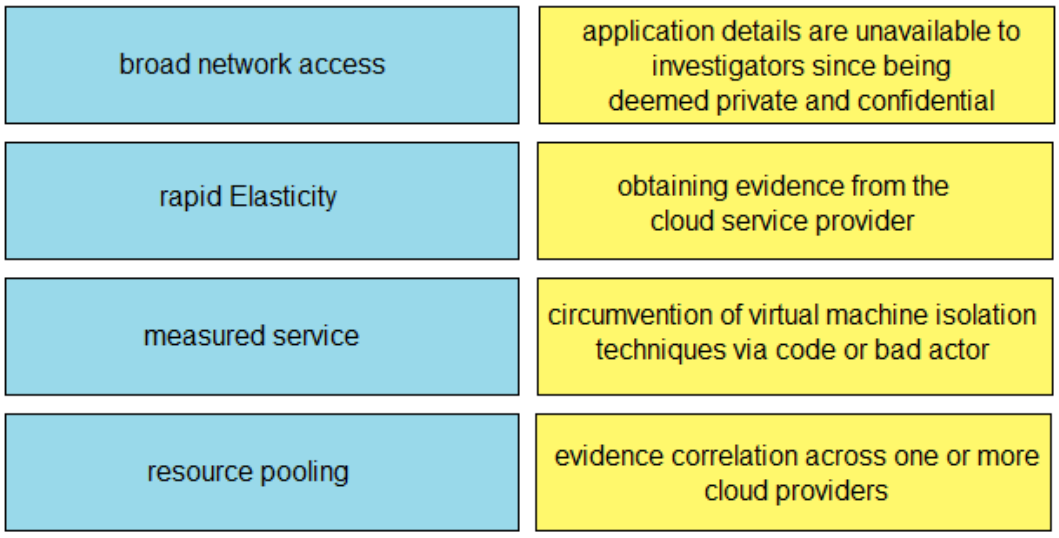
According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name:iraniansk.com
B. Server: nginx
C. Hash value: 5f31ab113af08=1597090577
D. filename= “Fy.exe”
E. Content-Type: application/octet-stream

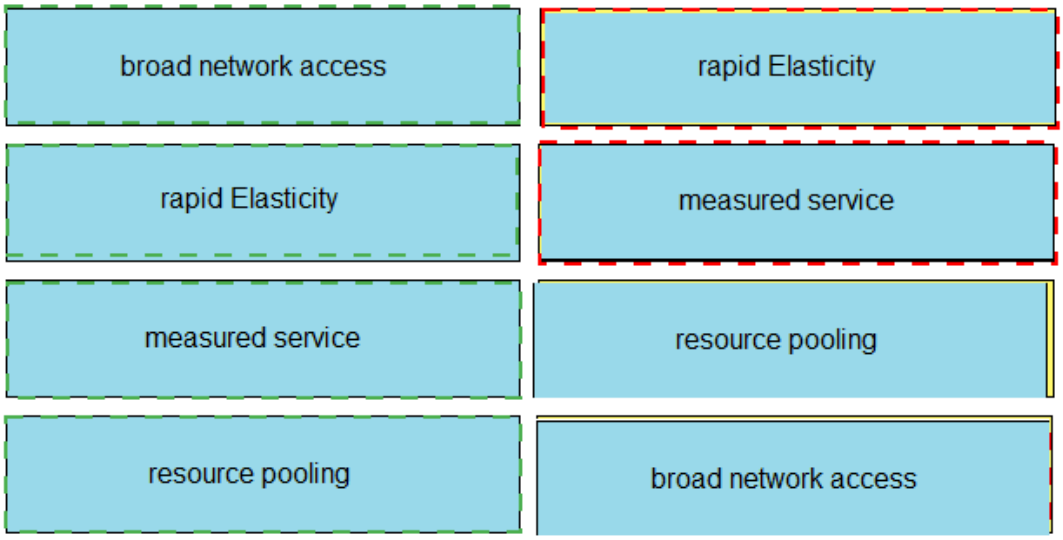
Answer: C,E

Question No : 12 DRAG DROP

Drag and drop the cloud characteristic from the left onto the challenges presented for gathering evidence on the right.



Answer:



Question No : 13

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.)