Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

300-215 Dumps
300-215 Braindumps
300-215 Real Questions
300-215 Practice Test
300-215 Actual Questions

Cisco

300-215

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

Question: 51 Section 1

```
<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".

Answer: D

Question: 52 Section 1

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

Answer: DE

Question: 53 Section 1

An organization uses a Windows 7 workstation for access tracking in one of their physical data centers on which a guard documents entrance/exit activities of all personnel. A server shut down unexpectedly in this data center, and a security specialist is analyzing the case. Initial checks show that the previous two days of entrance/exit logs are missing, and the guard is confident that the logs were entered on the workstation. Where should the security specialist look next to continue investigating this case?

- A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
- B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList
- C. HKEY_CURRENT_USER\Software\Classes\Winlog
- D. HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentUser

Answer: A
Reference:
https://www.sciencedirect.com/topics/computer-science/window-event-log

Question: 54 Section 1

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.

Answer: A

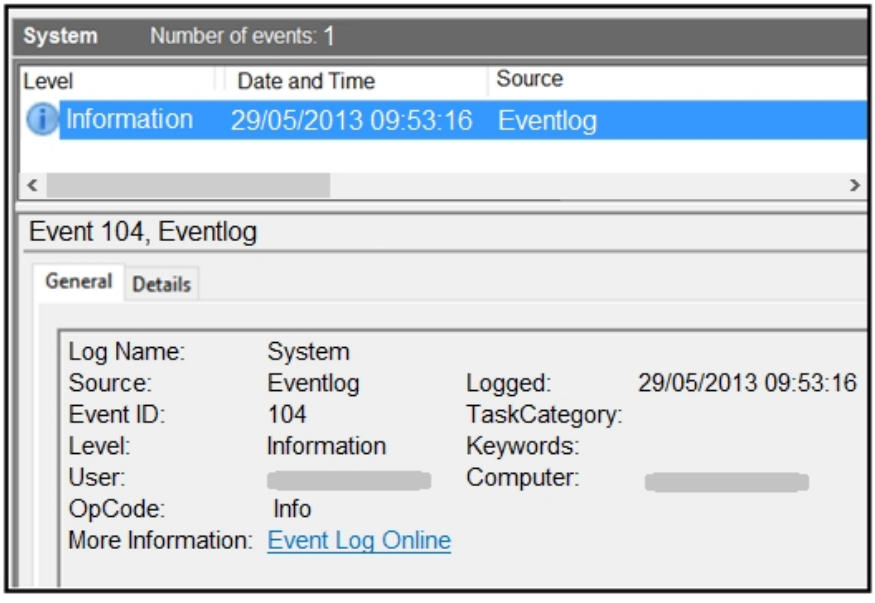
Question: 55 Section 1

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

Answer: B

Question: 56 Section 1



Refer to the exhibit. An employee notices unexpected changes and setting modifications on their workstation and creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

- A. data obfuscation
- B. reconnaissance attack
- C. brute-force attack
- D. log tampering

Answer: B

Question: 57 Section 1

```
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

Answer: C

Question: 58 Section 1

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

Answer: CE

Question: 59 Section 1

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

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*