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.pass2lead.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 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 2

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

Correct Answer: D

QUESTION 3

```
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

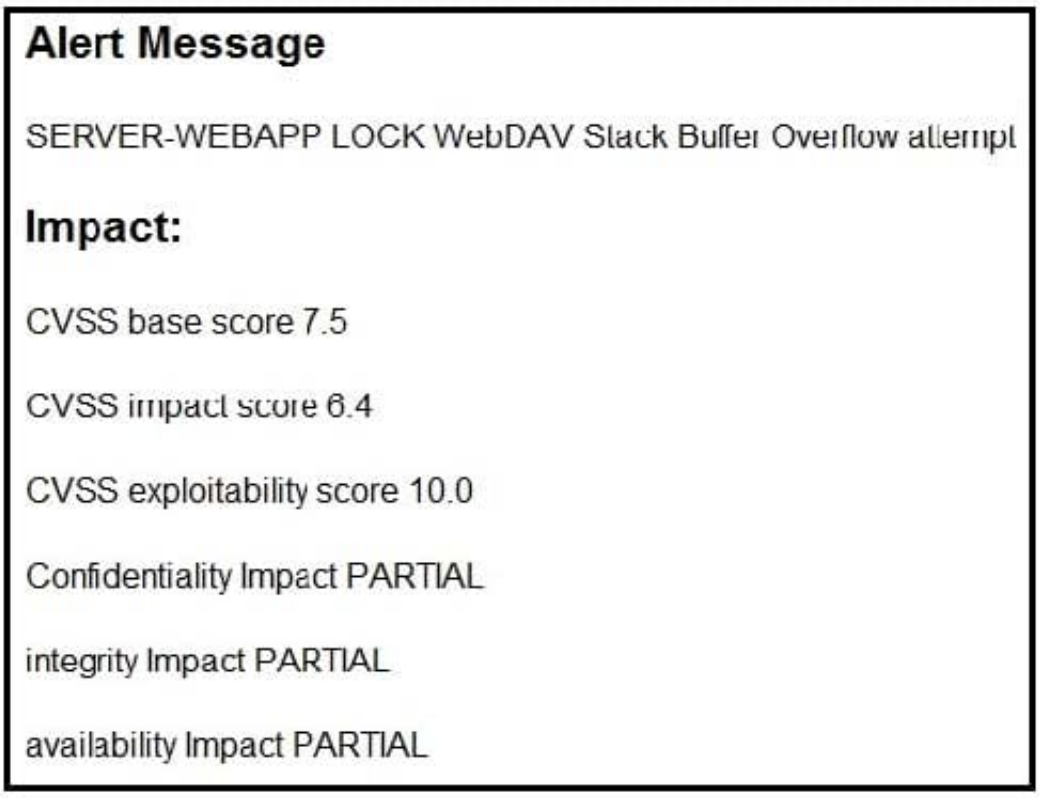
B. False Negative alert

C. False Positive alert

D. True Positive alert

Correct Answer: C

QUESTION 4



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 5

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