200-201$^{\text{Q\&As}}$

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

QUESTION 1

What is the difference between inline traffic interrogation and traffic mirroring?

A. Inline interrogation is less complex as traffic mirroring applies additional tags to data.

B. Traffic mirroring copies the traffic rather than forwarding it directly to the analysis tools

C. Inline replicates the traffic to preserve integrity rather than modifying packets before sending them to other analysis tools.

D. Traffic mirroring results in faster traffic analysis and inline is considerably slower due to latency.

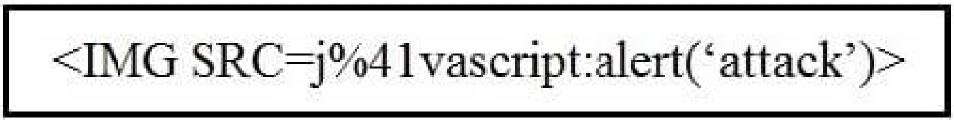
Correct Answer: B

Inline inspection - Inline traffic interrogation is a technique in which traffic flows through a device that inspects the traffic and makes decisions about how to handle it. The inspection takes place in real-time and in-line with the traffic flow.

Traffic mirroring - Traffic mirroring, also known as port mirroring or SPAN (Switched Port Analyzer), is a technique for forwarding a copy of network traffic to a monitoring device. The copy of the traffic is sent to a separate tool for analysis, security or other purposes.

QUESTION 2

Refer to the exhibit.



```
<IMG SRC=j%41vascript:alert('attack')>
```

Which kind of attack method is depicted in this string?

A. cross-site scripting

B. man-in-the-middle C. SQL injection

D. denial of service

Correct Answer: A

QUESTION 3

Which element is included in an incident response plan as stated in NIST.SP800-617

A. security of sensitive information

B. individual approach to incident response

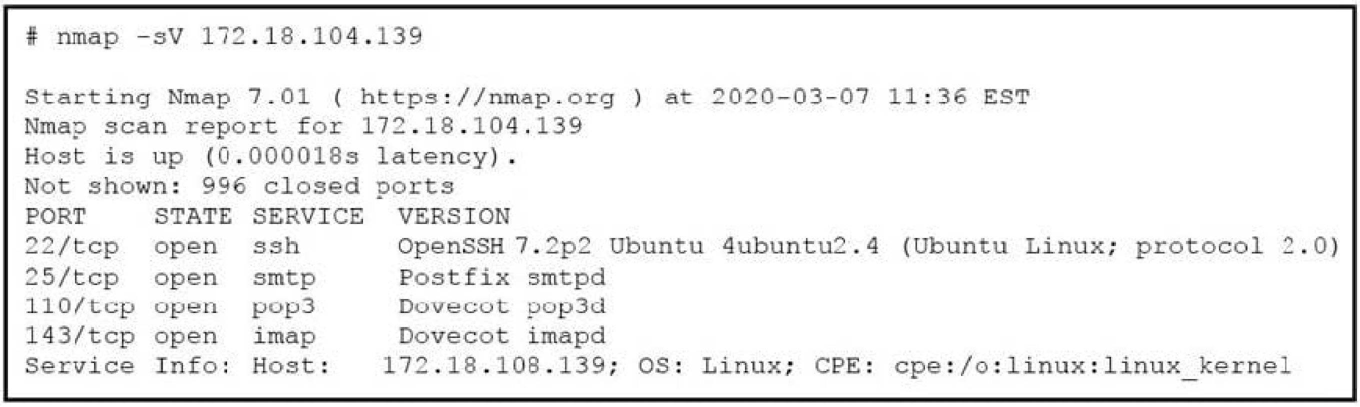
C. consistent threat identification

D. approval of senior management

Correct Answer: D

QUESTION 4

Refer to the exhibit.



```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp   open   smtp     Postfix smtpd
110/tcp  open   pop3     Dovecot pop3d
143/tcp  open   imap     Dovecot imapd
Service Info: Host:   172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

What does the output indicate about the server with the IP address 172.18.104.139?

A. open ports of a web server

B. open port of an FTP server

C. open ports of an email server

D. running processes of the server

Correct Answer: C

QUESTION 5

An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?

A. digital certificates

B. static IP addresses

C. signatures

D. cipher suite

Correct Answer: A