Cisco.Premium.210-255.by.VCEplus.126q

Number: 210-255 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 7.3

Exam Code: 210-255
Exam Name: Implementing Cisco Cybersecurity Operations
Certification Provider: Cisco
Corresponding Certification: CCNA Cyber Ops
Website: www.vceplus.com
Free Exam: https://vceplus.com/ccna-exam-210-255-secops/

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in 210-255 exam products and you get latest questions. We strive to deliver the best 210-255 exam product for top grades in your first attempt.

Exam A

QUESTION 1
Which option can be addressed when using retrospective security techniques?

A. if the affected host needs a software update
B. how the malware entered our network
C. why the malware is still in our network
D. if the affected system needs replacement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?

A. local
B. physical
C. network
D. adjacent

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which option is a misuse variety per VERIS enumerations?

A. snooping
B. hacking
C. theft

D. assault

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
In the context of incident handling phases, which two activities fall under scoping? (Choose two.)

A. determining the number of attackers that are associated with a security incident
B. ascertaining the number and types of vulnerabilities on your network
C. identifying the extent that a security incident is impacting protected resources on the network
D. determining what and how much data may have been affected
E. identifying the attackers that are associated with a security incident

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which regular expression matches "color" and "colour"?

A. col[0-9]+our
B. colo?ur
C. colou?r
D.]a-z]{7}

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which kind of evidence can be considered most reliable to arrive at an analytical assertion?

A. direct
B. corroborative
C. indirect
D. circumstantial
E. textual

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
You see 100 HTTP GET and POST requests for various pages on one of your webservers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. delivery
B. reconnaissance
C. action on objectives
D. installation
E. exploitation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which string matches the regular expression r(ege)+x?

A. rx
B. regeegex
C. r(ege)x
D. rege+x

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which statement about threat actors is true?

A. They are any company assets that are threatened.
B. They are any assets that are threatened.
C. They are perpetrators of attacks.
D. They are victims of attacks.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which data element must be protected with regards to PCI?

A. past health condition
B. geographic location
C. full name / full account number
D. recent payment amount

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

What mechanism does the Linux operating system provide to control access to files?

A. privileges required

B. user interaction

C. file permissions

D. access complexity

Correct Answer: C

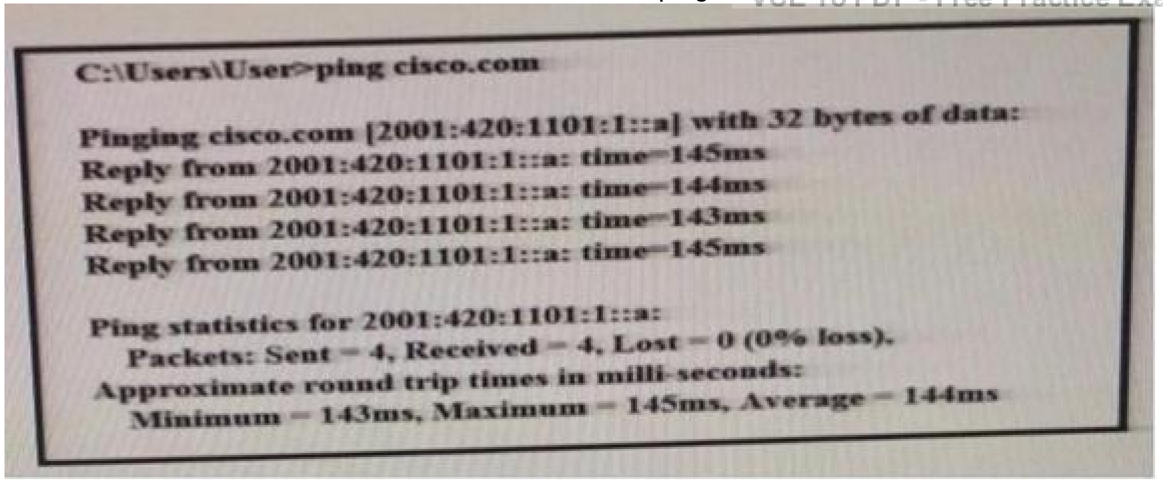
Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Refer to the exhibit. What can be determined from this ping result?



```
C:\Users\User>ping cisco.com

Pinging cisco.com [2001:420:1101:1::a] with 32 bytes of data:
Reply from 2001:420:1101:1::a: time=145ms
Reply from 2001:420:1101:1::a: time=144ms
Reply from 2001:420:1101:1::a: time=143ms
Reply from 2001:420:1101:1::a: time=145ms

Ping statistics for 2001:420:1101:1::a:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 143ms, Maximum = 145ms, Average = 144ms
```

A. The public IP address of cisco.com is 2001:420:1101:1::a.

B. The Cisco.com website is down.

C. The Cisco.com website is responding with an internal IP.
D. The public IP address of cisco.com is an IPv4 address.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which element is part of an incident response plan?

A. organizational approach to incident response
B. organizational approach to security
C. disaster recovery
D. backups

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
What is the correct about listening port?

A. A listening port is a port open by a running application in order to accept inbound connections.
B. A listening port is a port open by a running application in order to accept outbound connections.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

Filtering ports in wireshark?

A. tcp.port = 80
B. tcp.port equals 80
C. tcp.port != 80
D. tcp.port equal 80

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which two statements correctly describe the victim demographics section of the VERIS schema? (Choose two.)

A. The victim demographics section describes but does not identify the organization that is affected by the incident.
B. The victim demographics section compares different types of organizations or departments within a single organization.
C. The victim demographics section captures general information about the incident.
D. The victim demographics section uses geolocation data to identify the organization name of the victim and the threat actor.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
which option is unnecessary for determining the appropriate containment strategy according to NIST.SP80061 r2?

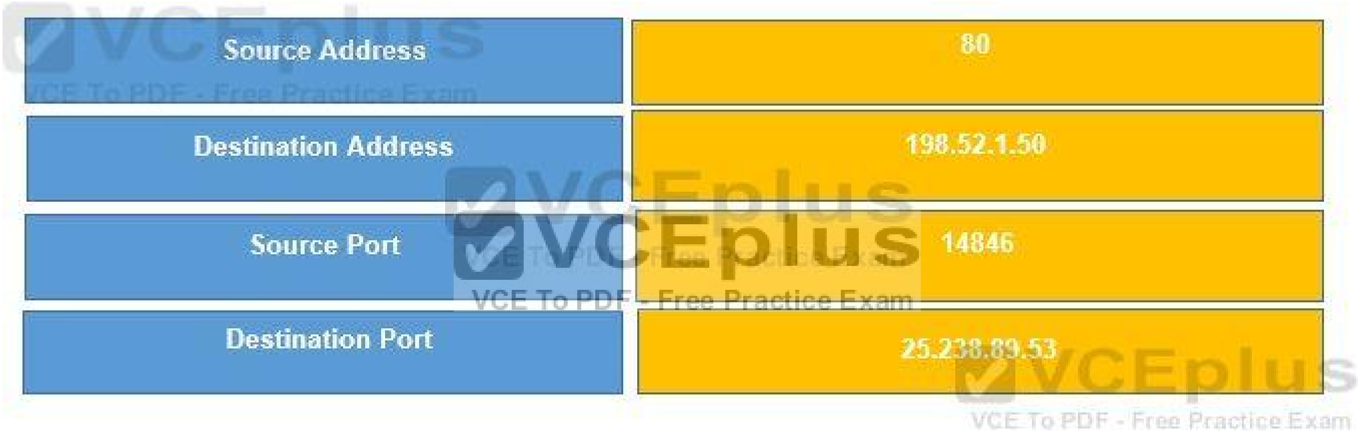
A. attack vector used to compromise the system
B. time and resources needed to implement strategy
C. need for evidence preservation
D. effectiveness of the strategy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

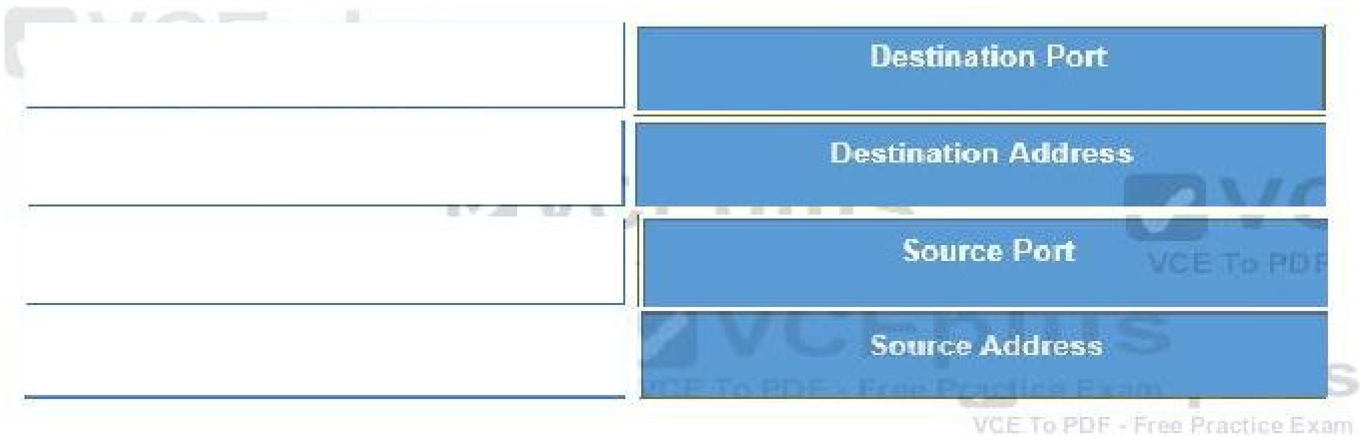
QUESTION 18
Drag and Drop
Built inbound TCP connection 463879 for outside: (25.238.89.53/14846) to DMZ: WWW_Server/80 (198.52.1.50/80)

Select and Place:



Source Address	80
Destination Address	198.52.1.50
Source Port	14846
Destination Port	25.238.89.53

Correct Answer:



Destination Port

Destination Address

Source Port

Source Address

Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which source provides reports of vulnerabilities in software and hardware to a Security Operations Center?

A. Analysis Center
B. National CSIRT
C. Internal CSIRT
D. Physical Security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
What information from HTTP logs can be used to find a threat actor?

A. referer
B. IP address
C. user-agent
D. URL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. Which term defines the initial event in the NIST SP800- 61 r2?

A. instigator
B. precursor
C. online assault
D. trigger

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
You have run a suspicious file in a sandbox analysis tool to see what the file does. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed or required to investigate the callouts? (Choose two.)

A. file size
B. domain names
C. dropped files
D. signatures
E. host IP addresses

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which option filters a LibPCAP capture that used a host as a gateway?

A. tcp|udp] [src|dst] port <port>
B. [src|dst] net <net> [{mask <mask>}|{len <len>}]
C. ether [src|dst] host <ehost>
D. gateway host <host>

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which type of analysis allows you to see how likely an exploit could affect your network?

A. descriptive
B. casual
C. probabilistic
D. inferential

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which network device creates and sends the initial packet of a session?

A. source
B. origination
C. destination
D. network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

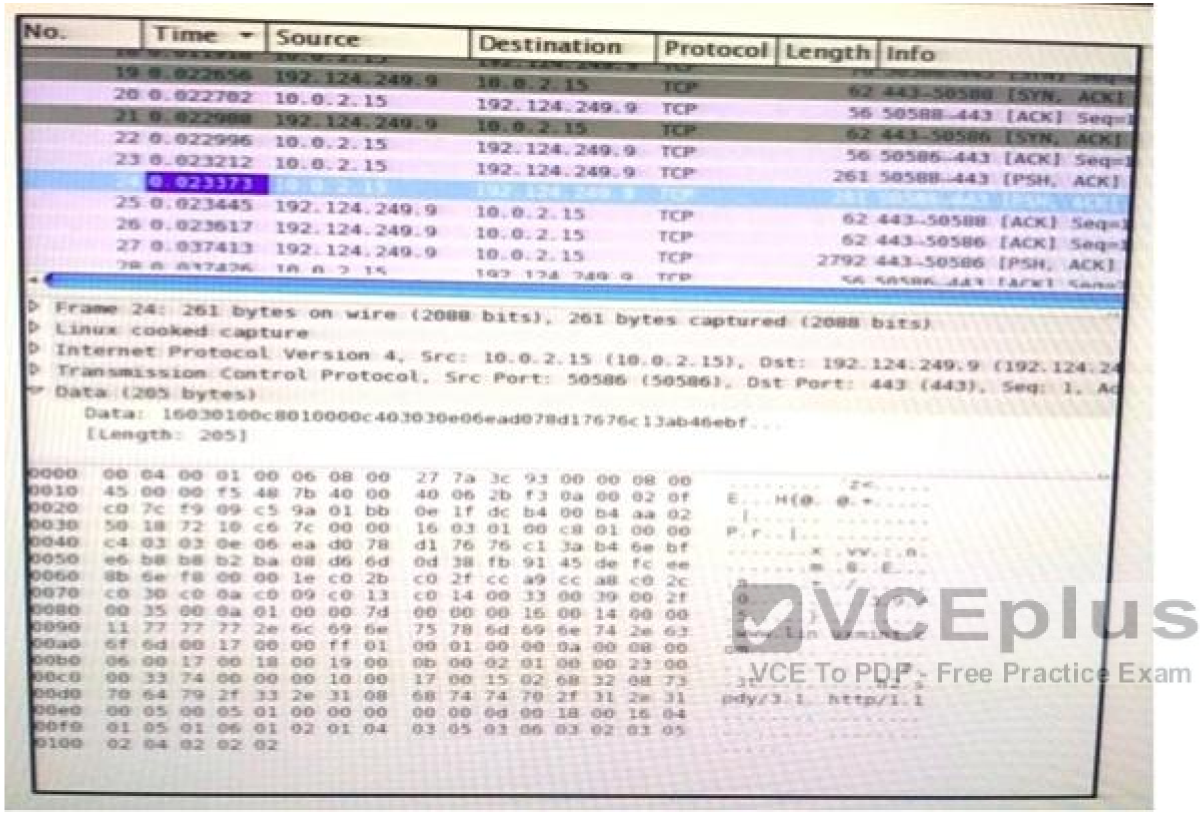
QUESTION 26
When performing threat hunting against a DNS server, which traffic toward the affected domain is considered a starting point?

A. HTTPS traffic
B. TCP traffic
C. HTTP traffic
D. UDP traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Refer to the exhibit. Which application protocol is in this PCAP file?



```
No.   Time      Source          Destination     Protocol Length Info
   19 0.022656  192.124.249.9   10.0.2.15       TCP        62 443-50588 [SYN, ACK]
   20 0.022702  10.0.2.15       192.124.249.9   TCP        56 50588-443 [ACK] Seq=1
   21 0.022988  192.124.249.9   10.0.2.15       TCP        62 443-50586 [SYN, ACK]
   22 0.022996  10.0.2.15       192.124.249.9   TCP        56 50586-443 [ACK] Seq=1
   23 0.023212  10.0.2.15       192.124.249.9   TCP       261 50588-443 [PSH, ACK]
   24 0.023373  10.0.2.15       192.124.249.9   TCP       261 50586-443 [PSH, ACK]
   25 0.023445  192.124.249.9   10.0.2.15       TCP        62 443-50588 [ACK] Seq=1
   26 0.023617  192.124.249.9   10.0.2.15       TCP        62 443-50586 [ACK] Seq=1
   27 0.037413  192.124.249.9   10.0.2.15       TCP      2792 443-50586 [PSH, ACK]
   28 0.037426  10.0.2.15       192.124.249.9   TCP        56 50586-443 [ACK] Seq=
```

```
▷ Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
▷ Linux cooked capture
▷ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.24
▷ Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, Ac
▽ Data (205 bytes)
    Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...
    [Length: 205]
```

```
0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00   ........ 'z<.....
0010  45 00 00 f5 48 7b 40 00  40 06 2b f3 0a 00 02 0f   E...H{@. @.+.....
0020  c0 7c f9 09 c5 9a 01 bb  0e 1f dc b4 00 b4 aa 02   .|...... ........
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00   P.r..|.. ........
0040  c4 03 03 0e 06 ea d0 78  d1 76 76 c1 3a b4 6e bf   .......x .vv.:.n.
0050  e6 b8 b8 b2 ba 08 d6 6d  0d 38 fb 91 45 de fc ee   .......m .8..E...
0060  8b 6e f8 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31   pdy/3.1. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05
0100  02 04 02 02 02
```

A. TCP
B. SSH
C. HTTP
D. SSL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

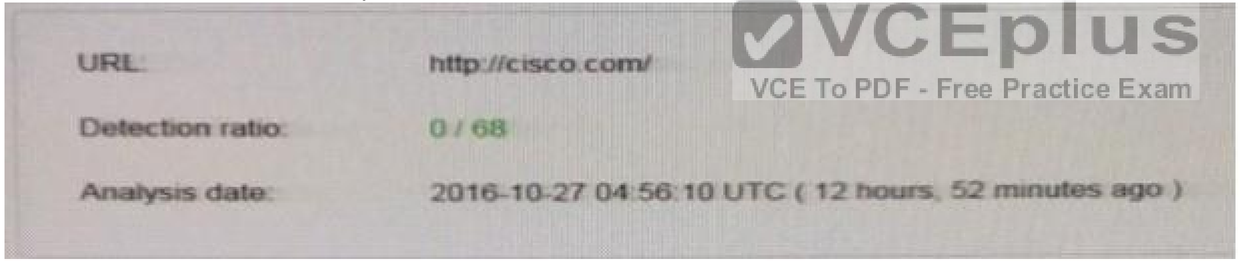
QUESTION 28
You see confidential data being exfiltrated to an IP address that is attributed to a known Advanced Persistent Threat group. Assume that this is part of a real attach and not a network misconfiguration. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. reconnaissance
B. weaponization
C. delivery
D. action on objectives

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Refer to the exhibit. We have performed a malware detection on the Cisco website. Which statement about the result is true?



URL: http://cisco.com/
Detection ratio: 0 / 68
Analysis date: 2016-10-27 04:56:10 UTC (12 hours, 52 minutes ago)

A. The website has been marked benign on all 68 checks.
B. The threat detection needs to run again.
C. The website has 68 open threats.
D. The website has been marked benign on 0 checks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?

A. true positive
B. true negative
C. false positive
D. false negative

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?

A. confidentiality
B. integrity
C. availability
D. complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

A. collection
B. examination
C. reporting
D. investigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which information must be left out of a final incident report?

A. server hardware configurations
B. exploit or vulnerability used
C. impact and/or the financial loss
D. how the incident was detected

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which two components are included in a 5-tuple? (Choose two.)

A. port number
B. destination IP address
C. data packet
D. user name
E. host logs

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference: