

100% Money Back
Guarantee

Vendor:Cisco

Exam Code:210-255

Exam Name:Cisco Cybersecurity Operations

Version:Demo

QUESTION 1

Which incident handling phase is focused on minimizing the impact of the incident?

- A. reporting
- B. remediation
- C. containment
- D. scoping

Correct Answer: C

QUESTION 2

Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.011641	10.0.2.15	192.124.249.9	TCP	76	50588->443 [SYN] Seq=0 Win=0
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588->443 [SYN] Seq=0 Win=0
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443->50588 [SYN, ACK] Seq=0
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588->443 [ACK] Seq=1 Ack=
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443->50586 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586->443 [ACK] Seq=1 Ack=
23	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TCP	56	50588->443 [ACK] Seq=1 Ack=
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443->50588 [ACK] Seq=1 Ack=
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443->50586 [ACK] Seq=1 Ack=
27	0.037413	192.124.249.9	10.0.2.15	TLSv1.2	2792	Server Hello
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586->443 [ACK] Seq=206 Ar

Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)

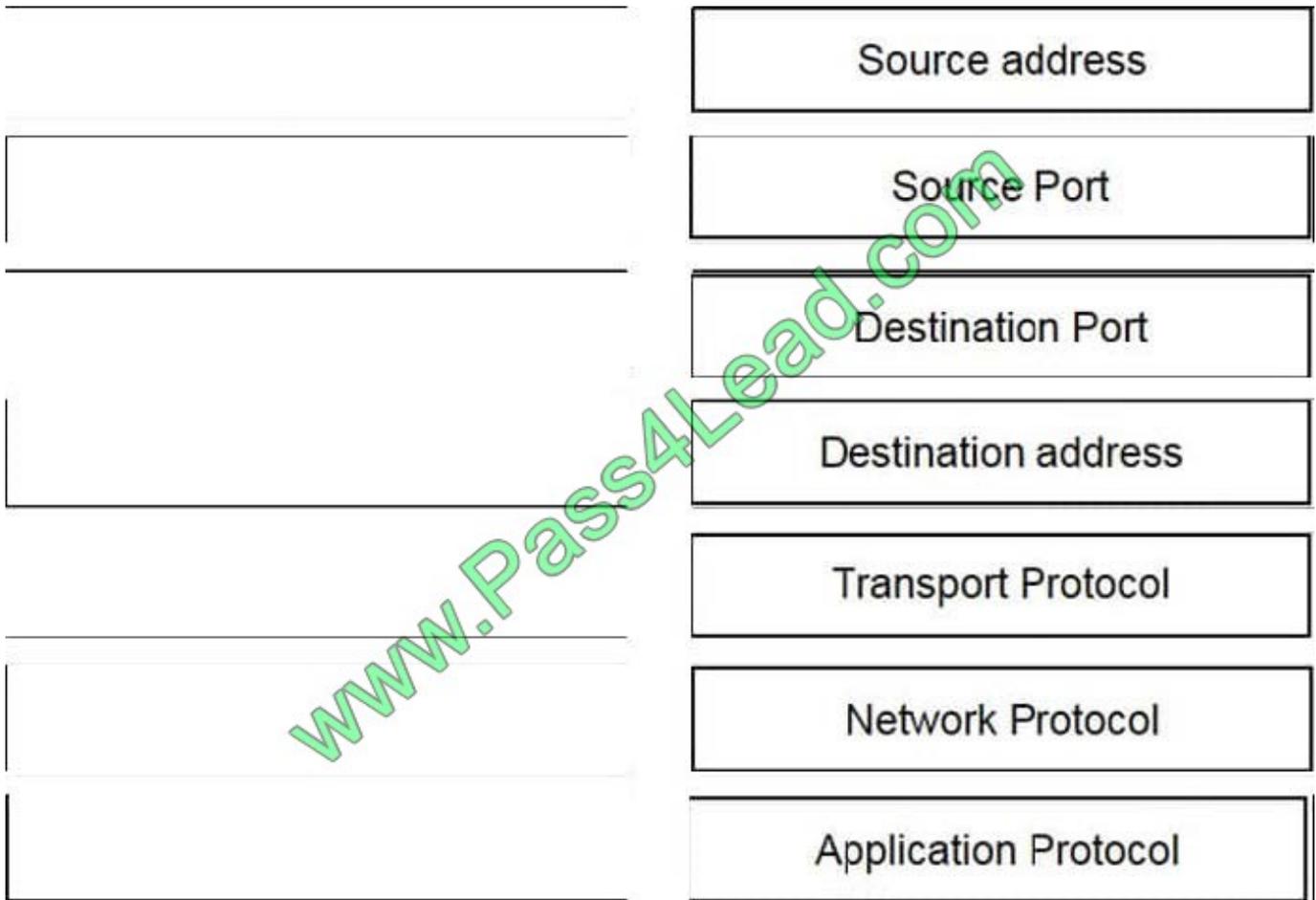
- Linux cooked capture
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.124.249.9 (192.124.249.9)
- Transmission Control Protocol, Src Port: 50588, Dst Port: 443 (443), Seq: 1, Ack: 1,
- Secure Sockets Layer

Offset	Hex	ASCII
0000	00 04 00 01 00 06 08 00 27 00 00 00 00 00 00 00z<.....
0010	45 00 00 f5 eb 3e 40 00 40 00 80 2f 0a 00 02 0f	E.....>@. @./.....
0020	c0 7c f9 09 c5 9c 01 bb 4d 00 7f f7 00 b3 b0 02M.....
0030	50 18 72 10 c6 7c 00 00 06 00 01 00 c8 01 00 00	P.r.
0040	c4 03 03 d1 08 45 78 b7 00 00 04 ee 51 16 f1 82Ex.Q.....
0050	16 43 ec d4 89 60 34 00 00 80 a6 d1 72 d5 11 87	.C... 4] {...r.....
0060	10 57 cc 00 00 1e c0 00 00 c0 2f cc a9 cc a8 c0 2c	.W.....+ /.....
0070	00 35 00 0a 01 00 00 00 00 14 00 33 00 39 00 2f	.@..... 3.9./.....
0080	00 00 00 00 00 00 00 00 00 00 00 16 00 14 00 00	.S.....}.....
0090	11 77 77 77 7e 00 00 00 75 78 6d 69 6e 74 2e 63	.www.lin uxmint.c.....
00a0	6f 6d 00 17 00 00 00 00 00 01 00 00 00 0a 00 08 00	om.....lin uxmint.c.....
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	.3t.....h2.s.....
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

Select and Place:

Source address	10.0.2.15
Destination address	50588
Source Port	443
Destination Port	192.124.249.9
Network Protocol	Transmission control protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

Correct Answer:



QUESTION 3

Which file is allocated with 32 bits?

- A. NTFS
- B. FAT32
- C. FAT
- D. EXT4

Correct Answer: B

QUESTION 4

Which CVSSv3 metric captures the level of access that is required for a successful attack?

- A. attack vector

- B. attack complexity
- C. privileges required
- D. user interaction

Correct Answer: C

Privileges Required The new metric, Privileges Required, replaces the Authentication metric of v2.0. Instead of measuring the number of times an attacker must separately authenticate to a system, Privileges Required captures the level of access required for a successful attack. Specifically, the metric values High, Low, and None reflect the privileges required by an attacker in order to exploit the vulnerability.

QUESTION 5

Which signature type results in a legitimate alert being dismissed?

- A. True negative
- B. False negative
- C. True Positive
- D. False Positive

Correct Answer: B

QUESTION 6

Which two HTTP header fields relate to intrusion analysis? (Choose two).

- A. user-agent
- B. host
- C. connection
- D. language
- E. handshake type

Correct Answer: AB

QUESTION 7

Drag and drop the type of evidence from the left onto the correct description(s) of that evidence on the right.

Select and Place:



Correct Answer:



QUESTION 8

Which option is a misuse variety per VERIS enumerations?

- A. snooping
- B. hacking
- C. theft
- D. assault

Correct Answer: B

QUESTION 9

Which of the following Linux file systems not only supports journaling but also modifies important data structures of the file system, such as the ones destined to store the file data for better performance and reliability?

- A. GRUB
- B. LILO
- C. Ext4
- D. FAT32

Correct Answer: C

QUESTION 10

In addition to cybercrime and attacks, evidence found on a system or network may be presented in a court of law to support accusations of crime or civil action, including which of the following?

- A. Fraud, money laundering, and theft
- B. Drug-related crime
- C. Murder and acts of violence
- D. All of the above

Correct Answer: D

QUESTION 11

What does the CSIRT incident response provider usually do?

- A. provide incident handling services to their parent organization.
- B. provide incident handling services to a country
- C. coordinate and facilitate the handling of incidents across various CSIRTs
- D. focus on synthesizing data from various sources to determine trends and patterns in incident activity
- E. handle reports of vulnerabilities in their software or hardware products
- F. offer incident handling services as a for-fee service to other organizations

Correct Answer: D

QUESTION 12

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

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average **99.9%** Success Rate

More than **800,000** Satisfied Customers Worldwide

Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.