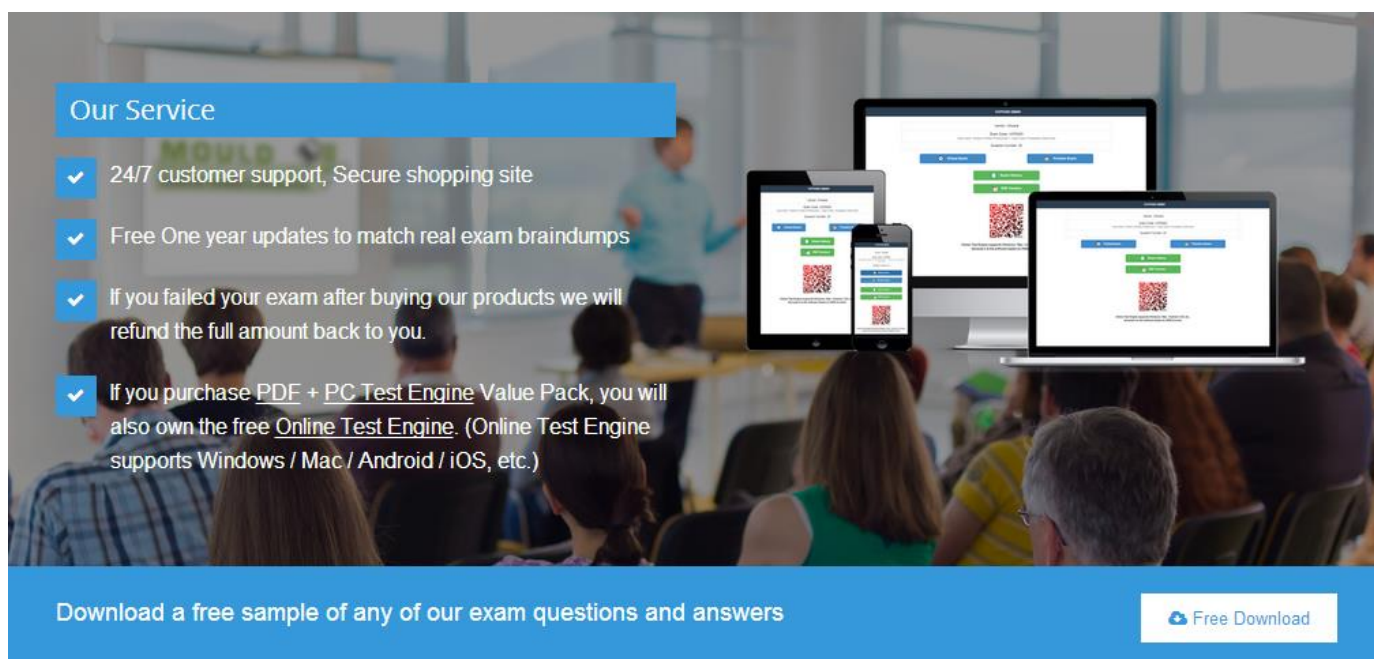


PDF4Test



Our Service

- ✓ 24/7 customer support, Secure shopping site
- ✓ Free One year updates to match real exam braindumps
- ✓ If you failed your exam after buying our products we will refund the full amount back to you.
- ✓ If you purchase PDF + PC Test Engine Value Pack, you will also own the free Online Test Engine. (Online Test Engine supports Windows / Mac / Android / iOS, etc.)

Download a free sample of any of our exam questions and answers [Free Download](#)



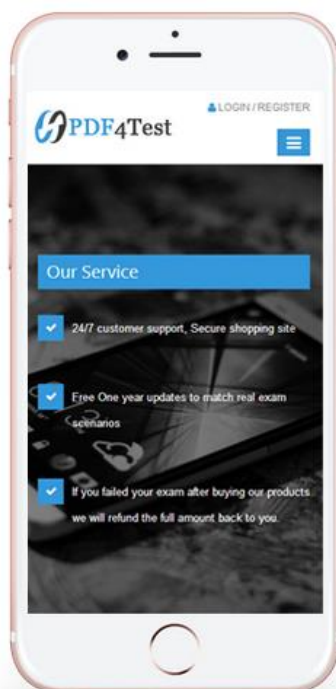
QUALITY AND VALUE

PDF4Test Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.



EASY TO PASS

If you prepare for the exams using our PDF4Test testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.



TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.



TRY BEFORE BUY

PDF4Test offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

<http://www.pdf4test.com>

Free valid test questions and dumps pdf for certification test prep

Exam : **210-255**

Title : Implementing Cisco
Cybersecurity Operations

Vendor : Cisco

Version : DEMO

NO.1 Which stakeholder group is responsible for containment, eradication, and recovery in incident handling?

- A. facilitators
- B. practitioners
- C. leaders and managers
- D. decision makers

Answer: A

NO.2 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

Answer: C

NO.3

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	0.022762	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	50588-443 [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=1

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 (192.124.249.9)

Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, Ack: 443, Win: 0, Len: 205

Data (205 bytes)

Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf... [Length: 205]

```

0000 00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00 .....2.....
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 .n.....+./...
0070 c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f .0.....3.9./
0080 00 35 00 0a 01 00 00 7d 00 00 00 16 00 14 00 00 .5.....}.....
0090 11 77 77 77 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63 .www.linuxmint.c
00a0 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 08 00 om.....
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 .....

```

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

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

Answer: C

NO.4 Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522->80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=1476292607552.28661c
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=6071 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522->80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Which packet contains a file that is extractable within Wireshark?

- A. 1986
- B. 2318
- C. 2542
- D. 2317

Answer: D

NO.5

```
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
```

Refer to the exhibit.

What can be determined from this ping result?

- 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.

Answer: A

NO.6 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

Answer: A