

210-255^{Q&As}

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/210-255.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Which regex matches on all lowercase letters only?

- A. [a-z]+
- B. a*z+
- C. [a-z]+
- D. a-z+

Correct Answer: C

QUESTION 2

Which description of a retrospective malware detection is true?

- A. You use Wireshark to identify the malware source.
- B. You use historical information from one or more sources to identify the affected host or file.
- C. You use information from a network analyzer to identify the malware source.
- D. You use Wireshark to identify the affected host or file.

Correct Answer: B

QUESTION 3

attacker using robots.txt is under which category?

- A. Reconnaissance
- B. Weaponization
- C. Delivery
- D. Exploitation
- E. Installation
- F. Command and control (C2)
- G. Actions on objectives

Correct Answer: A

QUESTION 4

DRAG DROP

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=
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588->443 [SYN] Seq=0 Win=
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->50588 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50588->443 [ACK] Seq=1 Ack=
23	0.023213	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
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->50588 [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	50588->443 [ACK] Seq=206 Ac

▶ 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 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
 ▶ Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack: 1,
 ▶ Secure Sockets Layer

```

0000 00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00 ..... *z<.....
0010 45 00 00 f5 eb 3e 40 00 40 06 89 2f 0a 00 02 0f E.....>@. @./.....
0020 c0 7c f9 09 c5 9c 01 bb 4d db 7f f7 00 b3 b0 02 .|. .... M.....
0030 50 18 72 10 c6 7c 00 00 16 03 01 00 c8 01 00 00 P.r...|... ..
0040 c4 03 03 d1 08 45 78 b7 2c 90 04 ee 51 16 f1 82 ....Ex. ....0...
0050 16 43 ec d4 89 60 34 4a 7b 80 a6 d1 72 d5 11 87 .C... 4J {...r...
0060 10 57 cc 00 00 1e c0 2b c0 2f cc a9 cc a8 c0 2c .W.....+ ./.....
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 .S.....} .....
0090 11 77 77 77 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63 .www.lin uxmint.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. Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

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:

	Source address
	Source Port
	Destination Port
	Destination address
	Transport Protocol
	Network Protocol
	Application Protocol

QUESTION 5

Refer to the exhibit.

Threat Intelligence:		
IP Address	Reputation (-100 to 100 higher is safer)	
ABC.example.com	25	
DEF.example.com	-75	
FGH.example.com	0	
XYZ.example.com	75	

DNS Information:	
Domain Name	IP Address
ABC.example.com	209.165.201.10
DEF.example.com	209.165.201.130
FGH.example.com	209.165.200.230
XYZ.example.com	209.165.202.25

Session Logs:		
Source	Destination	Protocol
10.0.1.1/5567	209.165.201.130/443	TCP
10.0.1.2/8012	209.165.201.10/80	TCP
10.0.1.10/8125	209.165.200.230/80	TCP
10.0.1.20/9765	209.165.202.25/443	TCP

Which host is likely connecting to a malicious site?

- A. 10.0.1.10
- B. 10.0.1.1
- C. 10.0.1.2
- D. 10.0.1.20

Correct Answer: B

[Latest 210-255 Dumps](#)

[210-255 PDF Dumps](#)

[210-255 VCE Dumps](#)