

200-201^{Q&As}

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

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

https://www.pass4itsure.com/200-201.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

Refer to the exhibit.

alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"BROWSER-CHROME Google Chrome XSSAuditor filter security policy bypass attempt"; flow:to_client,established; file_data; content:"<iframe",nocase; content:"srcdoc",within 20,nocase; content:"<script>",within 10,nocase;

pcre:"/<iframe[^>]*?srcdoc\s?=\s?[\x22\x27]<script>/smi"; metadata:policy max-detectips drop; service:http; reference:bugtrag,65066;

reference:url,googlechromereleases.blogspot.ca/2014/01/stable-channel-update.html; classtype:attempted-user; sid:30252; rev:3;)

A company\\'s user HTTP connection to a malicious site was blocked according to configured policy. What is the source technology used for this measure?

- A. network application control
- B. firewall
- C. IPS
- D. web proxy
- Correct Answer: C

QUESTION 2

How does certificate authority impact a security system?

- A. It authenticates client identity when requesting SSL certificate
- B. It validates domain identity of a SSL certificate
- C. It authenticates domain identity when requesting SSL certificate
- D. It validates client identity when communicating with the se

Correct Answer: B

QUESTION 3



Refer to the exhibit.

			Tin			Sou					inatio				ocol		gth				
				1113								. 249	. 9	a second designed			and the second second			17	seq-u
	_		a susception	any series parts	reconsent in	COLUMN STREET, ST.	Alternation of the	.249.	tion of the	participation in the	104/10/02/05	CONTRACTOR OF STREET, ST.		TCP			Departments and	443-50	and the second second	[SYN,	
				0227				a second a second as a second as				.249	.9					50588-			
			a management of the		and the second se		_	.249.	_	and the second second				TCP			Construction into	443-50	and the second second	[SYN,	
				0229								.249						50586-		[ACK]	
		23		0232	1000		100000000000000000000000000000000000000	20022			1.	.249				2	61	50588-	+443	[PSH,	ACK]
		24	a straight of	0233	and the second second	10.0						.249	. 9	TCP				50586			
								.249.						TCP				443→50		[ACK]	
							100000000000000000000000000000000000000	.249.	1.20	0.0000000000				TCP				443→50			
								.249.	9	10.0).2.	15		TCP				443→50			
a 6		2.8	0.0	0.374	2.6	10.0).2.	15		192.	12.4	.249	.9	TCP	5		56	50586-	+443	[ACK]	Sea=
	-	16	0303	1000	:801	.000	0c4	03030	e0(Sead	1078	d176	76	c13a	ab46	ebf.	•••				
0000	00	04	0.0	01	0.0																
			1000	1000	2002		0.72770	1000	27			93	120.23		-24-26.0	00			*z<		
0010	45	00	1000	01 £5	2002		0.72770	1000	27 40		3c 2b	223.675	120.23	00 00	-24-26.0			.H{@.			
	45 c0	1.255.45	00	1000	48	7b	40	00	40	06	2b	£3	0a		02	0£ 1	Ε		@.+		
0020		1.255.45	00 £9	f5	48 c5	7b 9a	40 01	00 bb	40	06 1f	2b	f3 b4	0a 00	00	02 aa	0£ 1 02	E	.H{@.	@.+	· · · · · ·	
0020 0030	c0 50	7c	00 £9	f5 09 10	48 c5	7b 9a 7c	40 01 00	00 bb 00	40 0e 16	06 1f 03	2b dc 01	f3 b4	0a 00 c8	00 b4 01	02 aa 00	0£ 1 02 00 1	E . . P.r	H{@.	@.+	· · · · · · · · · · · · · · · · · · ·	•
0020 0030 0040	c0 50 c4	7c 18 03	00 f9 72 03	f5 09 10	48 c5 c6 06	7b 9a 7c ea	40 01 00 d0	00 bb 00 78	40 0e 16 d1	06 1f 03 76	2b dc 01 76	f3 b4 00	0a 00 c8 3a	00 b4 01 b4	02 aa 00 6e	0f 1 02 00 1 bf	E . . P.r	.H{@.	@.+ 	· · · · · · · · · · · · · · · · · · ·	•
0020 0030 0040 0050	c0 50 c4	7c 18 03 b8	00 f9 72 03	f5 09 10 0e b2	48 c5 c6 06	7b 9a 7c ea 08	40 01 00 d0 d6	00 bb 00 78 6d	40 0e 16 d1	06 1f 03 76 38	2b dc 01 76 fb	f3 b4 00 c1	0a 00 c8 3a 45	00 b4 01 b4 de	02 aa 00 6e fc	0f 1 02 00 1 bf ee	E P.r	.H{@.	@.+ .vv	 	•
0020 0030 0040 0050 0060	c0 50 c4 e6 8b	7c 18 03 b8 6e	00 f9 72 03 b8	f5 09 10 0e b2 00	48 c5 c6 06 ba	7b 9a 7c ea 08 1e	40 01 00 d0 d6 c0	00 bb 00 78 6d 2b	40 0e 16 d1 0d	06 1f 03 76 38	2b dc 01 76 fb cc	f3 b4 00 c1 91 a9	0a 00 c8 3a 45 cc	00 b4 01 b4 de	02 aa 00 6e fc c0	0f 1 02 00 1 bf 2c	E P.r 	.H{@. 	@.+ .vv 		•
0020 0030 0040 0050 0060 0070	c0 50 c4 e6 8b	7c 18 03 b8 6e	00 f9 72 03 b8 f8	f5 09 10 0e b2 00 0a	48 c5 c6 06 ba 00	7b 9a 7c ea 08 1e 09	40 01 00 d0 d6 c0 c0	00 bb 00 78 6d 2b 13	40 0e 16 d1 0d c0	06 1f 03 76 38 2f	2b dc 01 76 fb cc 00	f3 b4 00 c1 91 a9 33	0a 00 c8 3a 45 cc	00 b4 01 b4 de a8	02 aa 00 6e fc c0	0f 1 02 00 2 bf 2c 2f	E P.r .n.	.H{@. x m +	@.+ .vv .8 ./	n. E. 3.9.,	
0020 0030 0040 0050 0060 0070 0080	c0 50 c4 8b c0	7c 18 03 b8 6e 30	00 f9 72 03 b8 f8 c0	f5 09 10 0e b2 00 0a	48 c5 c6 ba 00 c0 01	7b 9a 7c ea 08 1e 09	40 01 00 d0 d6 c0 c0 00	00 bb 00 78 6d 2b 13 7d	40 0e 16 d1 0d c0 c0 00	06 1f 03 76 38 2f 14 00	2b dc 01 76 fb cc 00	f3 b4 00 c1 91 a9 33 16	0a 00 c8 3a 45 cc 00	00 b4 01 b4 de a8 39 14	02 aa 00 6e fc c0 00 00	0f 1 02 00 2 bf 2c 2f 00	E P.r .n. .5.	.H{@. x m +	@.+ .vv .8 ./.	n. E 3.9.,	
0020 0030 0040 0050 0060 0070 0080 0080	c0 50 c4 e6 8b c0 00	7c 18 03 b8 6e 30 35	00 f9 72 03 b8 f8 c0 00 77	f5 09 10 0e b2 00 0a 0a	48 c5 c6 ba 00 c0 01 2e	7b 9a 7c ea 08 1e 09 00 6c	40 01 00 d0 d0 d6 c0 c0 00 69	00 bb 00 78 6d 2b 13 7d 6e	40 0e 16 d1 0d c0 c0 00	06 1f 03 76 38 2f 14 00	2b dc 01 76 fb cc 00 00	f3 b4 00 c1 91 a9 33 16 69	0a 00 c8 3a 45 cc 00 00 6e	00 b4 01 b4 de a8 39 14 74	02 aa 00 6e fc c0 00 00	0f 1 02 00 5 bf 2c 2f 00 63	E P.r .n. .0. .5.	.H{@. x x m + } wlin	0.+. .vv .8 ./. 	n. E 3.9.,	
0020 0030 0040 0050 0060 0070 0080 0090 00a0	c0 50 c4 e6 8b c0 00 11	7c 18 03 b8 6e 30 35 77	00 f9 72 03 b8 f8 c0 00 77	f5 09 10 0e b2 00 0a 77 17	48 c5 c6 ba 00 c0 01 2e 00	7b 9a 7c ea 08 1e 09 00 6c	40 01 d0 d0 d6 c0 c0 00 69 ff	00 bb 00 78 6d 2b 13 7d 6e 01	40 0e 16 d1 0d c0 c0 00 75	06 1f 03 76 38 2f 14 00 78 01	2b dc 01 76 fb cc 00 00 6d 00	f3 b4 00 c1 91 a9 33 16 69 00	0a 00 c8 3a 45 cc 00 6e 0a	00 b4 01 b4 de a8 39 14 74 00	02 aa 00 6e fc c0 00 00 2e 08	0f 1 02 00 1 bf 2c 2f 00 63 00 0	E P.r .n. .0. .5. .ww	.H{@. x x 	@.+. .vv .8 ./. uxmi	n. E. 3.9., .nt.c	· · · ·
0020 0030 0040 0050 0060 0070 0080 0090 0080 0090 00a0 00b0	c0 50 c4 e6 8b c0 00 11 6f 06	7c 18 03 b8 6e 30 35 77 6d 00	00 f9 72 03 b8 f8 c0 00 77 00 17	f5 09 10 0e b2 00 0a 77 17 00	48 c5 c6 ba 00 c0 01 2e 00 18	7b 9a 7c ea 08 1e 09 00 6c 00 00	40 01 d0 d0 d6 c0 c0 00 69 ff 19	00 bb 00 78 6d 2b 13 7d 6e 01 00	40 0e 16 d1 0d c0 c0 00 75 00 0b	06 1f 03 76 38 2f 14 00 78 01 00	2b dc 01 76 fb cc 00 00 6d 00 02	f3 b4 00 c1 91 a9 33 16 69 00 01	0a 00 3a 45 00 6e 00	00 b4 01 b4 de a8 39 14 74 00 00	02 aa 00 6e fc 00 00 2e 08 23	0f 1 02 00 1 bf 2c 2f 00 63 00 0	E P.r .n. .0. .5. .ww om.	.H{@. x x 	@.+. .vv .8 ./. uxmi		· · · · ·
0020 0030 0040 0050 0060 0070 0080 0090 0090 0080 0090 0080 0050	c0 50 c4 e6 8b c0 00 11 6f 06 00	7c 18 03 b8 6e 30 35 77 6d 00 33	00 f9 72 03 b8 f8 c0 00 77 00 17 74	f5 09 10 0e b2 00 0a 0a 77 17 00 00	48 c5 c6 ba 00 c0 01 2e 00 18 00	7b 9a 7c ea 08 1e 09 00 6c 00 00 00	40 01 00 d0 d6 c0 c0 00 69 ff 19 10	00 bb 00 78 6d 2b 13 7d 6e 01 00 00	40 0e 16 d1 0d c0 c0 00 75 00 0b 17	06 1f 03 76 38 2f 14 00 78 01 00 00	2b dc 01 76 fb cc 00 00 6d 00 02 15	f3 b4 00 c1 91 33 16 69 00 01 02	0a 00 c8 3a 45 cc 00 00 68	00 b4 01 b4 de a8 39 14 74 00 00 32	02 aa 00 6e fc 00 00 2e 08 23 08	0f 1 02 bf ee 2c 2f 00 63 00 73	E P.r .n. .0. .5. .ww om. .3t	.H{@. 	@.+ .vv .8 ./. 	n. .E. 3.9., .nt.c #	· · · · ·
0020 0030 0040 0050 0060 0070 0080 0090 00a0 00b0 00b0 00c0 00d0	c0 50 c4 e6 8b c0 00 11 6f 06 00 70	7c 18 03 b8 6e 30 35 77 6d 00 33 64	00 f9 72 03 b8 f8 c0 00 77 00 17 74 79	f5 09 10 0e b2 00 0a 77 17 00 00 2f	48 c5 c6 ba 00 c0 01 2e 00 18 00 33	7b 9a 7c ea 08 1e 09 00 6c 00 00 00 2e	40 01 d0 d0 c0 c0 c0 69 ff 19 10 31	00 bb 00 78 6d 2b 13 7d 6e 01 00 00 00 08	40 0e 16 d1 0d c0 00 75 00 0b 17 68	06 1f 03 76 38 2f 14 00 78 01 00 74	2b dc 01 76 fb cc 00 6d 00 6d 02 15 74	f3 b4 00 c1 91 a9 33 16 69 00 01 02 70	0a 00 c8 3a 45 cc 00 00 6e 0a 00 68 2f	00 b4 01 b4 de a8 39 14 74 00 00 32 31	02 aa 00 6e fc 00 00 2e 08 23 08 23	0f 1 02 bf ee 2c 2f 00 63 00 73 31	E P.r .n. .0. .5. .ww om. .3t	.H{@. x x 	@.+ .vv .8 ./. 	n. .E. 3.9., .nt.c #	· · · · ·
0020 0030 0040 0050 0060 0070 0080 0090 0080 0090 0080 0080 008	c0 50 c4 e6 8b c0 00 11 6f 06 00 70 00	7c 18 03 b8 6e 30 35 77 6d 00 33 64 05	00 f9 72 03 b8 f8 c0 00 77 00 17 74 79 00	f5 09 10 0e b2 00 0a 77 17 00 02 f 05	48 c5 c6 ba 00 c0 01 2e 00 18 00 33 01	7b 9a 7c ea 08 1e 09 00 6c 00 00 00 2e 00	40 01 d0 d0 d6 c0 c0 69 ff 19 10 31 00	00 bb 00 78 6d 2b 13 7d 6e 01 00 00 08 00	40 0e 16 01 00 c0 00 75 00 0b 17 68 00	06 1f 03 76 38 2f 14 00 78 01 00 00 74 00	2b dc 01 76 fb cc 00 6d 00 02 15 74 0d	f3 b4 00 c1 91 a9 33 16 69 00 01 02 70 00	0a 00 c8 3a 45 cc 00 00 6e 0a 00 68 2f 18	00 b4 01 b4 de a8 39 14 74 00 00 32 31 00	02 aa 00 6e fc 00 00 2e 08 23 08 28 28 26	0f 1 02 bf ee 2c 2f 00 63 00 73 31 1 04	E P.r .n. .0. .5. .ww om. .3t	.H{@. 	@.+ .vv .8 ./. 	n. .E. 3.9., .nt.c #	· · · · ·
0020 0030 0040 0050 0060 0070 0080 0090 0080 0090 0080 0080 008	c0 50 c4 e6 8b c0 00 11 6f 06 00 70 00 01	7c 18 03 b8 6e 30 35 77 6d 00 33 64 05 05	00 f9 72 03 b8 f8 c0 00 77 00 17 74 79 00 01	f5 09 10 0e b2 00 0a 77 17 00 00 2f	48 c5 c6 06 ba 00 c0 01 2e 00 18 00 33 01 01	7b 9a 7c ea 08 1e 09 00 6c 00 00 00 2e 00	40 01 d0 d0 d6 c0 c0 69 ff 19 10 31 00	00 bb 00 78 6d 2b 13 7d 6e 01 00 00 08 00	40 0e 16 d1 0d c0 00 75 00 0b 17 68	06 1f 03 76 38 2f 14 00 78 01 00 74	2b dc 01 76 fb cc 00 6d 00 02 15 74 0d	f3 b4 00 c1 91 a9 33 16 69 00 01 02 70	0a 00 c8 3a 45 cc 00 00 6e 0a 00 68 2f 18	00 b4 01 b4 de a8 39 14 74 00 00 32 31 00	02 aa 00 6e fc 00 00 2e 08 23 08 28 28 26	0f 1 02 bf ee 2c 2f 00 63 00 73 31 1 04 05	E P.r .n. .0. .5. .ww om. .3t	.H{@. x x m + } wlin 	@.+ .vv .8 ./. 	n. .E. 3.9., .nt.c #	· · · · ·

Which application protocol is in this PCAP file?

A. SSH

B. TCP

C. TLS

D. HTTP

Correct Answer: C

QUESTION 4



An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

- A. Run "ps -d" to decrease the priority state of high load processes to avoid resource exhaustion.
- B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.
- C. Run "ps -ef" to understand which processes are taking a high amount of resources.
- D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

Correct Answer: C

Reference: https://unix.stackexchange.com/questions/62182/please-explain-this-output-of-ps-ef-command

QUESTION 5

What describes the concept of data consistently and readily being accessible for legitimate users?

- A. integrity
- B. availability
- C. accessibility
- D. confidentiality
- Correct Answer: B

QUESTION 6

An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

- A. The computer has a HIPS installed on it.
- B. The computer has a NIPS installed on it.
- C. The computer has a HIDS installed on it.
- D. The computer has a NIDS installed on it.

Correct Answer: C

QUESTION 7

A forensic investigator is analyzing a recent breach case. An external USB drive was discovered to be connected and transmitting the data outside of the organization, and the owner of the USB drive could not be identified. Video surveillance shows six people during a two-month period had close contact with the affected asset. How must this type of evidence be categorized?



- A. best evidence
- B. indirect evidence
- C. direct evidence
- D. corroborative evidence
- Correct Answer: B

QUESTION 8

A security incident occurred with the potential of impacting business services. Who performs the attack?

- A. malware author
- B. threat actor
- C. bug bounty hunter
- D. direct competitor
- Correct Answer: B

Reference: https://www.paubox.com/blog/what-is-threatactor/#:~:text=The%20term%20threat%20actor%20refers,CTA)%20when%20referencing%20cybersecurity%20issues

QUESTION 9

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

- A. known-plaintext
- B. replay
- C. dictionary
- D. man-in-the-middle
- Correct Answer: D

QUESTION 10

What is the impact of encryption?

- A. Confidentiality of the data is kept secure and permissions are validated
- B. Data is accessible and available to permitted individuals



- C. Data is unaltered and its integrity is preserved
- D. Data is secure and unreadable without decrypting it

Correct Answer: D

QUESTION 11

Refer to the exhibit.

TCP	10.114.248.74:80	216.36.50.65:60973	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60974	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60975	TIME_VAIT
TCP	10.114.248.74:80	216.36.50.65:60976	TIME WAIT
TCP	10.114.248.74:80	216.36.50.65:60977	TIME WAIT
TCP	10.114.248.74:80	216.36.50.65:60978	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60979	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60980	TIME WAIT
TCP	10.114.248.74:80	216.36.50.65:60981	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60983	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60984	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60985	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60986	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60987	TIME WAIT
TCP	10.114.248.74:80	216.36.50.65:60988	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60989	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60990	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60992	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60993	TIME WAIT
TCP	10.114.248.74:80	216.36.50.65:60994	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60995	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60996	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60997	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60998	TIME_WAIT
TCP	10.114.248.74:80	216.36.50.65:60999	TIME_WAIT
TOP	10.111.210.11.00	610.30.30.03.00777	ATTIC_WHIT

An engineer received a ticket about a slowed-down web application The engineer runs the #netstat -an command. How must the engineer interpret the results?

- A. The web application is receiving a common, legitimate traffic
- B. The engineer must gather more data.
- C. The web application server is under a denial-of-service attack.
- D. The server is under a man-in-the-middle attack between the web application and its database

Correct Answer: C

QUESTION 12

What is indicated by an increase in IPv4 traffic carrying protocol 41 ?

A. additional PPTP traffic due to Windows clients

- B. unauthorized peer-to-peer traffic
- C. deployment of a GRE network on top of an existing Layer 3 network
- D. attempts to tunnel IPv6 traffic through an IPv4 network

Correct Answer: D

QUESTION 13

Which of these is a defense-in-depth strategy principle?

- A. Identify the minimum resource required per employee.
- B. Provide the minimum permissions needed to perform job functions.
- C. Disable administrative accounts to avoid unauthorized changes.
- D. Assign the least network privileges to segment network permissions.

Correct Answer: D

QUESTION 14

Refer to the exhibit.

No.	Time 1 0.000000	Source	Destination 10.128.0.2	Protocol	Length Info	- 80	Isynt	Sega	Win=	512 Le	n=0		
	2 0.003987	10.128.0.2		TCP							Win=29200	Len=0	NSS=1460
	3 0.005514	10.128.0.2	10.0.0.2	TCP							Win=29200		
	4 0.008429	10.0.0.2	10.128.0.2	TCP	54 3342	- 80	[SYN]	Seq=(0 Win=	512 Le	n=0		
	5 0.010233	10.128.0.2	10.0.0.2	TCP	58 80 -	3220	[SYN,	ACK]	Seq=0	Ack=1	Win=29200	Len=0	NSS=1460
	6 0.014072	10.128.0.2		TCP	58 80 -	3342	[SYN,	ACK]	Seq=0	Ack=1	Win=29200	Len=0	NSS=1460
	7 0.016830	10.0.0.2	10.128.0.2	TCP	54 3343	- 80	[SYN]	Seq=(0 Win=	512 Le	n=0		
	8 0.022220	10.128.0.2		TCP				-			Win=29200		
	9 0.023496	10.128.0.2		TCP							Win=29200	Len=0	MSS=1460
	10 0.025243	10.0.0.2		TCP	54 3344								
	11 0.026672			TCP			-	-			Win=29200		
	12 0.028038			TCP							Win=29200		
	13 0.030523	10.128.0.2	10.0.0.2	TCP	58 80 -	3344	[SYN,	ACK]	Seq=0	Ack=1	Win=29200	Len=0	MSS=1460
De [\$	ource Port: 33 estination Por Stream index: CP Segment Le	t: 80 0] en: 0]											
	quence number												
[]	lext sequence	number: 0 (1	elative seque	ence number	:)]								
	cknowledgement												
	$101 \dots = Heade$ lags: 0x002 (3		bytes (5)				ACCRECT ON A						
	indow size val					Statistical and	1000				and the second second second		
	Calculated wir		121										
	necksum: 0x8d5												
	Checksum Statu												
	gent pointer:												
	[imestamps]												
-													

What is occurring in this network traffic?

- A. High rate of SYN packets being sent from a multiple source towards a single destination IP.
- B. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.
- C. Flood of ACK packets coming from a single source IP to multiple destination IPs.
- D. Flood of SYN packets coming from a single source IP to a single destination IP.

Correct Answer: D

QUESTION 15

What is the purpose of a ransomware attack?

- A. to escalate privileges
- B. to make files inaccessible by encrypting the data
- C. to send keystrokes to a threat actor
- D. to decrypt encrypted data and disks

Correct Answer: B

200-201 PDF Dumps

200-201 Practice Test

200-201 Study Guide