# Braindump2go Guarantee All Exams 100% Pass One Time!

Vendor: Cisco

> Exam Code: 200-201

- **Exam Name: 200-201 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)**
- ➤ New Updated Questions from <u>Braindump2go</u> (Updated in <u>Sep/2020</u>)

### Visit Braindump2go and Download Full Version 200-201 Exam Dumps

#### **QUESTION 16**

**Drag and Drop Question** 

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.			Tin	1e		Sour	ce			Dest	inatio	on		Prot	tocol	Leng	th I	nfo				
		17	0.0	116	41	10.0	).2.	15		192.	124	.249	.9	TCP		1	76 5	0586-	443	[SYN]	Seq=0	Win=
		18	0.0	119	18	10.0	).2.	15		192.	124	.249	.9	TCP	1	1 5	76 5	0588-	443	[SYN]	Seq=0	Win=
		19	0.0	226	56	192	124	.249	9.9	10.0	.2.	15		TCP	)		52 4	43-50	588	[SYN,	ACK]	Seq=(
				30-21H375		10.0	CONTRACTOR OF STREET					.249	.9	TCP	)						Seq=1	
			HINDONES	0000000000	INFOORIS E		RESCHOOLSE	.249						TCP				434200004400	00000000	MATERIAL PROPERTY.	ACK]	DODGET AND
						10.0						.249									Seq=1	Ack:
						10.0									v1.2			Lient				
						10.0							.9		v1.2			lient				123110
								.249						TCP						The state of the s	Seq=1	
								.249						TCP						The second second	Seq=1	ACK
								.249							v1.2			erver				
4		28	0.0	13/4	2.6_	10.0	1./.	1.5		19%.	124	.249	. 9	TECH	,		16 5	11586-	443	LACKI	Sea=2	()6 A
> Tran	nsmis	sio	n Co			Prot	oco.	1, S	rc P	ort:	. 50	300	(50	,500				110 (	,445/	, seq	. 1, A	CK.1,
> Inte > Tran > Secu	nsmis ure S	ssio	n Co ets	Lay	er	Prot 06																CK.1,
> Tran	nsmis ure S	ssio Sock	n Co ets 00	Lay	er 00		08	00	27	7a	3с		00	0.0	08	00 .			*z<	, seq		CK.1)
> Tran > Section 0000 0010	nsmis ure S 00 45	ock 04 00	n Co ets 00	Lay 01 f5	er 00 eb	06	08 40	00	27 40	7a 06	3c 89	93 2f	00 0a	00	08	00 . 0f F			*z<			CK.1,
> Tran > Section 0000 0010 0020	nsmis ure s 00 45 c0	ock 04 00 7c	n Co ets 00 00 f9	01 f5 09	00 eb c5	06 3e	08 40 01	00	27 40 4d	7a 06 db	3c 89	93 2f f7	00 0a 00	00 00 b3	08 02	00 . 0f F	  I	.>@.	*z<	· · · · · · · · · · · · · · · · · · ·		CK.1,
0000 0010 0020 0030	00 45 c0 50	04 00 7c 18	00 00 00 f9	01 f5 09	00 eb c5 c6	06 3e 9c	08 40 01 00	00 00 bb 00	27 40 4d 16	7a 06 db 03	3c 89 7f 01	93 2f £7 00	00 0a 00 c8	00 00 b3 01	08 02 b0	00 . 0f H 02 .	   	.>@.	*z<	····		CK.1,
> Tran > Section 0000 0010 0020 0030 0040	00 45 c0 50 c4	04 00 7c 18	00 00 00 f9 72 03	01 f5 09 10 d1	00 eb c5 c6	06 3e 9c 7c	08 40 01 00 78	00 00 bb 00 b7	27 40 4d 16 2c	7a 06 db 03 90	3c 89 7f 01 04	93 2f f7 00 ee	00 0a 00 c8 51	00 00 b3 01 16	08 02 b0 00	00 . 0f H 02 . 00 H	   	 .>@. 	*z<	/		CK.1,
0000 0010 0020 0030 0040 0050	00 45 c0 50 c4 16	04 00 7c 18 03 43	00 00 00 f9 72 03 ec	01 f5 09 10 d1 d4	00 eb c5 c6 08	06 3e 9c 7c 45	08 40 01 00 78 34	00 00 bb 00 b7 4a	27 40 4d 16 2c	7a 06 db 03 90 80	3c 89 7f 01 04 a6	93 2f f7 00 ee d1	00 0a 00 c8 51 72	00 00 b3 01 16 d5	08 02 b0 00 f1	00 . 0f H 02 . 00 H 82 .	   	 .>@.  .l .Ex.	*z<	/		CK.1,
0000 0010 0020 0030 0040 0050 0060	00 45 c0 50 c4 16	04 00 7c 18 03 43	00 00 00 f9 72 03 ec	01 f5 09 10 d1 d4	00 eb c5 c6 08 89	06 3e 9c 7c 45 60	08 40 01 00 78 34 c0	00 00 bb 00 b7 4a	27 40 4d 16 2c 7b	7a 06 db 03 90 80 2f	3c 89 7f 01 04 a6	93 2f f7 00 ee d1 a9	00 0a 00 c8 51 72 cc	00 00 b3 01 16 d5	08 02 b0 00 f1 11 c0	00 . 0f H 02 . 00 H 82 . 87 .	     	 .>@. .I .Ex. +	*z<	/ /		CK.1,
> Tran > Section 0000 0010 0020 0030 0040 0050	00 45 c0 50 c4 16 10	04 00 7c 18 03 43 57	00 00 f9 72 03 ec	01 f5 09 10 d1 d4	00 eb c5 c6 08 89 00 c0	06 3e 9c 7c 45 60 1e	08 40 01 00 78 34 c0	00 00 bb 00 b7 4a 2b	27 40 4d 16 2c 7b c0	7a 06 db 03 90 80 2f	3c 89 7f 01 04 a6 cc	93 2f f7 00 ee d1 a9 33	00 0a 00 c8 51 72 cc	00 00 b3 01 16 d5	08 02 b0 00 f1 11 c0	00 . 0f H 02 . 00 H 82 . 87 . 2c .	         C   W	 .>@.  .Ex. 4J	*z< @ M {			CK.1,
0000 0010 0020 0030 0040 0050 0060 0070 0080	00 45 c0 50 c4 16 10	04 00 7c 18 03 43 57 30	00 00 f9 72 03 ec cc	01 f5 09 10 d1 d4 00 0a	00 eb c5 c6 08 89 00 c0	06 3e 9c 7c 45 60 1e 09	08 40 01 00 78 34 c0 c0	00 00 bb 00 b7 4a 2b 13 7d	27 40 4d 16 2c 7b c0 c0	7a 06 db 03 90 80 2f 14	3c 89 7f 01 04 a6 cc 00	93 2f f7 00 ee d1 a9 33 16	00 0a 00 c8 51 72 cc 00	00 00 b3 01 16 d5 a8 39	08 02 b0 00 f1 11 c0	00 . 0f H 02 . 00 H 82 . 87 . 2c . 2f .	       C   W   5	 .>@. .  .Ex. 4J +	*z< @ M {	/ .0 .r		CK.1,
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090	00 45 c0 50 c4 16 10 c0	04 00 7c 18 03 43 57 30	00 00 f9 72 03 ec cc	01 f5 09 10 d1 d4 00 0a	00 eb c5 c6 08 89 00 c0	06 3e 9c 7c 45 60 1e 09	08 40 01 00 78 34 c0 c0 00 69	00 00 bb 00 b7 4a 2b 13 7d	27 40 4d 16 2c 7b c0 c0	7a 06 db 03 90 80 2f 14	3c 89 7f 01 04 a6 cc 00 00 6d	93 2f f7 00 ee d1 a9 33 16	00 0a 00 c8 51 72 cc 00 00 6e	00 00 b3 01 16 d5 a8 39 14 74	08 02 b0 00 f1 11 c0 00	00 . 0f H 02 . 00 H 82 . 87 . 2c . 2f . 00 .	         C   W   5	 .>@. .  .Ex. 4J + }	*z< @ M { ./.	.0		CK.1,
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 00a0	00 45 c0 50 c4 16 10 c0	04 00 7c 18 03 43 57 30 35 77	00 00 f9 72 03 ec c0 00 77	01 f5 09 10 d1 d4 00 0a 0a 77	00 eb c5 c6 08 89 00 c0 01 2e 00	06 3e 9c 7c 45 60 1e 09 00 6c	08 40 01 00 78 34 c0 c0 00 69 ff	00 00 bb 00 b7 4a 2b 13 7d 6e	27 40 4d 16 2c 7b c0 c0 00 75	7a 06 db 03 90 80 2f 14 00 78	3c 89 7f 01 04 a6 cc 00 00 6d	93 2f f7 00 ee d1 a9 33 16 69 00	00 0a 00 c8 51 72 cc 00 00 6e 0a	00 00 b3 01 16 d5 a8 39 14 74	08 02 b0 00 f1 11 c0 00 2e	00 . 0f H 02 . 00 H 82 . 87 . 2c . 2f . 00 . 63 .	C W 0 www	 .>@. .I .Ex. 4J +	*z< @ M {	.0 .0 3.9.,		CK.1,
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 00b0	00 45 c0 50 c4 16 10 c0 00 11 6f 06	04 00 7c 18 03 43 57 30 35 77 6d 00	00 00 69 72 03 ec cc c0 00 77	01 f5 09 10 d1 d4 00 0a 77 17	00 eb c5 c6 08 89 00 c0 01 2e 00 18	06 3e 9c 7c 45 60 1e 09 00 6c 00	08 40 01 00 78 34 c0 c0 00 69 ff	00 00 bb 00 b7 4a 2b 13 7d 6e 01	27 40 4d 16 2c 7b c0 c0 00 75 00 0b	7a 06 db 03 90 80 2f 14 00 78 01 00	3c 89 7f 01 04 a6 cc 00 00 6d 00	93 2f f7 00 ee d1 a9 33 16 69 00	00 0a 00 c8 51 72 cc 00 00 6e 0a	00 00 b3 01 16 d5 a8 39 14 74 00	08 02 b0 00 f1 11 c0 00 00 2e 08	00 .00 in 02 .00 in 82 .00 .00 .00 .00 .00 .00 .00 .00 .00 .0	C W O 5	 .>@. .I .Ex. 4J +	*z< @ M {	.0 .0 3.9.,		
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0000	00 45 c0 50 c4 16 10 c0 00 11 6f 06	04 00 7c 18 03 43 57 30 35 77 6d 00 33	00 00 f9 72 03 ec cc c0 00 77 74	01 f5 09 10 d1 d4 00 0a 77 17 00 00	00 eb c5 c6 08 89 00 c0 01 2e 00 18 00	06 3e 9c 7c 45 60 1e 09 00 6c 00	08 40 01 00 78 34 c0 c0 69 ff 19	00 00 bb 00 b7 4a 2b 13 7d 6e 01 00	27 40 4d 16 2c 7b c0 c0 00 75 00 0b 17	7a 06 db 03 90 80 2f 14 00 78 01 00	3c 89 7f 01 04 a6 cc 00 00 6d 00 02 15	93 2f f7 00 ee d1 a9 33 16 69 00 01 02	00 0a 00 c8 51 72 cc 00 6e 0a 00 68	00 00 b3 01 16 d5 a8 39 14 74 00 00 32	08 02 b0 00 f1 11 c0 00 2e 08 23	00 .00 in 02 .00 in 82 .00 .00 .00 .00 .00 .00 .00 .00 .00 .0	0 W 0 5 www	 .>@. .I .Ex. 4J + }	*z< @ M {	.0 .0 3.9.,	, , , , , , , , , , , , , , , , , , , ,	
> Trai > Section 0000 0010 0020 0030 0040 0050 0060 0070	00 45 c0 50 c4 16 10 c0 00 11 6f 06	04 00 7c 18 03 43 57 30 35 77 6d 00 33 64	00 00 f9 72 03 ec cc 00 00 17 74 79	01 f5 09 10 d1 d4 00 0a 77 17 00 00 2f	00 eb c5 c6 08 89 00 c0 01 2e 00 18 00 33	06 3e 9c 7c 45 60 1e 09 00 6c 00 00 00	08 40 01 00 78 34 c0 c0 69 ff 19 10 31	00 00 bb 00 b7 4a 2b 13 7d 6e 01 00	27 40 4d 16 2c 7b c0 c0 00 75 00 0b 17 68	7a 06 db 03 90 80 2f 14 00 78 01 00 00	3c 89 7f 01 04 a6 cc 00 6d 00 02 15 74	93 2f f7 00 ee d1 a9 33 16 69 00 01 02 70	00 0a 00 c8 51 72 cc 00 00 6e 0a 00 68 2f	00 00 b3 01 16 d5 a8 39 14 74 00 00 32 31	08 02 b0 00 f1 11 c0 00 00 2e 08 23 08	00 .00 .00 .00 .00 .00 .00 .00 .00 .00	C W 0 5 www m 3t.	 .>@. .I .Ex. 4J + }	*z< @ M {   htt		, , , , , , , , , , , , , , , , , , , ,	CK.1,
> Trai > Section 0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0000 0000 0000	00 45 c0 50 c4 16 10 c0 00 11 6f 06 00 70	04 00 7c 18 03 43 57 30 35 77 6d 00 33 64 05	00 00 f9 72 03 ec cc c0 00 77 74 79 00	01 f5 09 10 d1 d4 00 0a 77 17 00 00 2f 05	00 eb c5 c6 08 89 00 c0 12 2e 00 18 00 33 01	06 3e 9c 7c 45 60 1e 09 00 6c 00 00 2e	08 40 01 00 78 34 c0 00 69 ff 19 10 31 00	00 00 bb 00 b7 4a 2b 13 7d 6e 01 00 00 00 8	27 40 4d 16 2c 7b c0 c0 00 75 00 0b 17 68 00	7a 06 db 03 90 80 2f 14 00 78 01 00 74 00	3c 89 7f 01 04 a6 cc 00 00 6d 00 22 15 74 0d	93 2f f7 00 ee d1 a9 33 16 69 00 01 02 70	00 0a 00 c8 51 72 cc 00 6e 0a 00 68 2f 18	00 00 b3 01 16 d5 a8 39 14 74 00 00 32 31 00	08 02 b0 00 f1 11 c0 00 00 2e 08 23 08 2e	00 .00 .00 .00 .00 .00 .00 .00 .00 .00	C W 0 5 www m 3t.		*z< @ M {   htt		, , , , , , , , , , , , , , , , , , , ,	



## **Braindump2go Guarantee All Exams 100% Pass**

**One Time!** 

	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					
Answer:		source address					
		source port					
		destination port					
		destination address					
		Transport Protocol					
		Network Protocol					
		Application Protocol					

#### **QUESTION 17**

Drag and Drop Question

Drag and drop the access control models from the left onto the correct descriptions on the right.

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

Answer:



# Braindump2go Guarantee All Exams 100% Pass One Time!

DAC

MAC

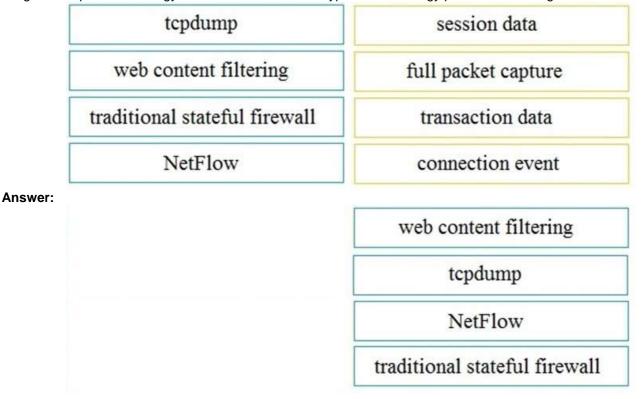
RBAC

ABAC

#### **QUESTION 18**

**Drag and Drop Question** 

Drag and drop the technology on the left onto the data type the technology provides on the right.



#### **QUESTION 19**

Which tool is commonly used by threat actors on a webpage to take advantage of the softwarevulnerabilities of a system to spread malware?

- A. exploit kit
- B. root kit
- C. vulnerability kit
- D. script kiddie kit

Answer: A

#### **QUESTION 20**

Which two methods might be used by an analyst to detect SSL/TLS encrypted command-and-control communication? (Choose two.)

- A. perform decryption and inspection of SSL/TLS traffic
- B. perform firewall HTTP application inspection to detect for the command and control traffic
- C. perform IPS HTTP deep packets inspection to detect for the command and control traffic

200-201 Exam Dumps 200-201 Exam Questions 200-201 PDF Dumps 200-201 VCE Dumps



### **Braindump2go Guarantee All Exams 100% Pass**

**One Time!** 

D. perform analysis of the NetFlow data to detect anomalous TLS/SSL flows

Answer: AD

#### **QUESTION 21**

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header.

Which technology makes this behavior possible?

- A. encapsulation
- B. TOR
- C. tunneling
- D. NAT

Answer: D

#### **QUESTION 22**

When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.

Which information is available on the server certificate?

- A. server name, trusted subordinate CA, and private key
- B. trusted subordinate CA, public key, and cipher suites
- C. trusted CA name, cipher suites, and private key
- D. server name, trusted CA, and public key

Answer: D

#### **QUESTION 23**

A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.

Which type of evidence is this?

- A. best evidence
- B. prima facie evidence
- C. indirect evidence
- D. physical evidence

Answer: C

#### **QUESTION 24**

Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

- A. detection and analysis
- B. post-incident activity
- C. vulnerability management
- D. risk assessment
- E. vulnerability scoring

Answer: AB

#### **QUESTION 25**

Which utility blocks a host portscan?

A. HIDS

200-201 Exam Dumps 200-201 Exam Questions 200-201 PDF Dumps 200-201 VCE Dumps

https://www.braindump2go.com/200-201.html



## Braindump2go Guarantee All Exams 100% Pass

**One Time!** 

B. sandboxing

C. host-based firewall

D. antimalware

Answer: C

#### **QUESTION 26**

Which event is user interaction?

- A. gaining root access
- B. executing remote code
- C. reading and writing file permission
- D. opening a malicious file

Answer: D

#### **QUESTION 27**

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the fink launched, it infected machines and the intruder was able to access the corporate network. Which testing method did the intruder use?

- A. social engineering
- B. eavesdropping
- C. piggybacking
- D. tailgating

Answer: A

#### **QUESTION 28**

Refer to the exhibit. What information is depicted?

Top 10 Src IP Addr ordered by flows:										
Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp		
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68		
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123		
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48		

- A. IIS data
- B. NetFlow data
- C. network discovery event
- D. IPS event data

Answer: B

#### **QUESTION 29**

Which type of evidence supports a theory or an assumption that results from initial evidence?

- A. probabilistic
- B. indirect
- C. best
- D. corroborative

Answer: D

200-201 Exam Dumps 200-201 Exam Questions 200-201 PDF Dumps 200-201 VCE Dumps