

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.leads4pass.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

What is a difference between inline traffic interrogation and traffic mirroring?

- A. Inline inspection acts on the original traffic data flow
- B. Traffic mirroring passes live traffic to a tool for blocking
- C. Traffic mirroring inspects live traffic for analysis and mitigation
- D. Inline traffic copies packets for analysis and security

Correct Answer: A

Inline traffic interrogation analyzes traffic in real time and has the ability to prevent certain traffic from being forwarded Traffic mirroring doesn\\'t pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device

QUESTION 2

What describes the defense-m-depth principle?

- A. defining precise guidelines for new workstation installations
- B. categorizing critical assets within the organization
- C. isolating guest Wi-Fi from the focal network
- D. implementing alerts for unexpected asset malfunctions

Correct Answer: C

QUESTION 3

According to CVSS, what is attack complexity?

- A. existing exploits available in the wild exploiting the vulnerability
- B. existing circumstances beyond the attacker\\'s control to exploit the vulnerability
- C. number of actions an attacker should perform to exploit the vulnerability
- D. number of patches available for certain attack mitigation and how complex the workarounds are

Correct Answer: B

QUESTION 4



DRAG DROP

Refer to the exhibit.

No.			Tin	ne		Sour	rce			Desti	inatio	on		Prot	ocol	Leng	th Info					
		17	0.0	116	41	10.0	0.2.	15		192.	124	.249	9.9	TOP		7	6 505	36-4	143	[SYN]	Seq=0	Win
		18	0.0	119	18	10.0	0.2.	15		192.	124	.249	9.9	TCP		7	6 505	38-4	143	[SYN]	Seq=0	Win
		19	0.0	226	56	192	.124	.249	9.9	10.0	.2.	15		TCP		6	2 443-	-505	88	[SYN,	ACK]	Seq=
		20	0.0	227	02	10.0	0.2.	15		192.	124	.249	9.9	TCP	18	5	6 505	8-4	143	[ACK]	Seq=1	Ack
		21	0.0	229	88	192	.124	.249	9.9	10.0	.2.	15	3	TCP		6	2 443-	-505	686	[SYN,	ACK]	Seq=
						10.0								TCP			6 505	6-4	143	[ACK]	Seq=1	Ack:
		2.3	0.0)232	12	10.0	1.2	15		192.	124	.24	9.9	TLS	v1,2		1 011					
						10.0							9.9	TLS	v1.2		1 Cli					
								.249						TCP						120 PHONE STATE OF	Seq=1	
								.249						TCP							Seq=1	Ack
								.249							v1.2		2 Ser	100000000000000000000000000000000000000	0.000	3000		
21		2.8	0.0	374	2.6	10.0	1.2.	1.5	- 1	192.	124	.24	9.9	TCP		E	6 505	36-4	143	[ACK]	Sea=2	06 A
> Tran > Secu	ire S	Sock	ets	Lay	er	06			27	7a	3с	93	00	00	08	00 .			*z<			
> Secu	ire s	ock 04	ets 00	Lay	er 00		08	00									>					
> Secu	00 45	04 00 7c	00 00 f9	01 f5 09	00 eb c5	06 3e 9c	08 40 01	00 00 bb	40	06	89	2f	0a		02	Of E		@.	0	/ · · · ·		
> Secu 0000 0010	00 45	04 00 7c	00 00 f9	01 f5 09	00 eb c5	06 3e	08 40 01	00 00 bb	40 4d	06 db	89 7f	2f f7	0a 00	00 53	02	0f E	>	@. 	0 M	/ · · · ·		
0000 0010 0020	00 45 c0 50	04 00 7c 18	00 00 f9 72	01 f5 09	00 eb c5 c6	06 3e 9c	08 40 01 00	00 00 bb 00	40 4d 16	06 db 03	89 7f 01	2f f7 00	0a 00 c8	00 b3 01	02 b0	0f E 02 . 00 F	>	@ . 	@ M	/ · · · · · · · · · · · · · · · · · · ·		
0000 0010 0020 0030	00 45 c0 50 c4	04 00 7c 18 03	00 00 f9 72 03	01 f5 09 10 d1	00 eb c5 c6 08	06 3e 9c 7c	08 40 01 00 78	00 00 bb 00 b7	40 4d 16 2c	06 db 03 90	89 7f 01 04	2f f7 00 ee	0a 00 c8 51	00 b3 01 16	02 b0 00	0f E 02 . 00 F 82 .	> 	@. x.	@ M 	/ 		
0000 0010 0020 0030 0040 0050 0060	00 45 c0 50 c4	04 00 7c 18 03 43	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	40 4d 16 2c 7b	06 db 03 90 80	89 7f 01 04 a6	2f f7 00 ee d1	0a 00 c8 51 72	00 b3 01 16	02 b0 00 f1	0f E 02 . 00 F 82 . 87 .	> .r	@. x. 4J	@ M {	/ .0		
0000 0010 0020 0030 0040	00 45 c0 50 c4 16	04 00 7c 18 03 43	00 00 f9 72 03 ec cc	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 2b	40 4d 16 2c 7b c0	06 db 03 90 80	89 7f 01 04 a6 cc	2f f7 00 ee d1 a9	0a 00 c8 51 72 cc	00 b3 01 16 d5 a8	02 b0 00 f1	0f E 02 . 00 F 82 . 87 . 2c .	> E	@. x. 4J	@ M {	/ 		
0000 0010 0020 0030 0040 0050 0060	00 45 c0 50 c4 16 10	04 00 7c 18 03 43 57	00 00 f9 72 03 ec cc	01 f5 09 10 d1 d4 00	00 eb c5 c6 08 89 00 c0	06 3e 9c 7c 45 60 1e	08 40 01 00 78 34 c0 c0	00 00 bb 00 b7 4a 2b	40 4d 16 2c 7b c0	06 db 03 90 80 2f 14	89 7f 01 04 a6 cc 00	2f f7 00 ee d1 a9 33	0a 00 c8 51 72 cc 00	00 b3 01 16 d5 a8	02 b0 00 f1 11 c0	0f E 02 . 00 F 82 . 87 . 2c . 2f .	> E	@. x. 4J .+	@ M { ./.	/ .0 .r 3.9./		
0000 0010 0020 0030 0040 0050 0060 0070 0080	00 45 c0 50 c4 16 10	04 00 7c 18 03 43 57 30 35	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	40 4d 16 2c 7b c0 c0	06 db 03 90 80 2f 14 00	89 7f 01 04 a6 cc 00	2f f7 00 ee d1 a9 33 16	0a 00 c8 51 72 cc 00	00 b3 01 16 d5 a8 39	02 b0 00 f1 11 c0	0f E 02 . 00 F 82 . 87 . 2c . 2f .	> .r E	@. 4J .+ 	@ M { ./.	/ .0 .r 3.9./		
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090	00 45 c0 50 c4 16 10 c0 00 11 6f	04 00 7c 18 03 43 57 30 35 77 6d	00 00 f9 72 03 ec cc c0 00 77	01 f5 09 10 d1 d4 00 0a 0a 77 17	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 6e	40 4d 16 2c 7b c0 c0 00 75	06 db 03 90 80 2f 14 00 78	89 7f 01 04 a6 cc 00 00 6d	2f f7 00 ee d1 a9 33 16	0a 00 c8 51 72 cc 00 00 6e	00 b3 01 16 d5 a8 39 14 74	02 b0 00 f1 11 c0 00 2e 08	0f E 02 . 00 F 82 . 87 . 2c . 2f . 00 .	> E E	@. x. 4J .+ 	@ M { ./.	/ .0 .r 3.9./		
0000 0010 0020 0030 0040 0050 0060 0070	00 45 c0 50 c4 16 10 c0 00 11 6f	04 00 7c 18 03 43 57 30 35 77	00 00 f9 72 03 ec cc c0 00 77	01 f5 09 10 d1 d4 00 0a 0a 77 17	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 69 ff	00 00 bb 00 b7 4a 2b 13 7d 6e 01	40 4d 16 2c 7b c0 c0 00 75	06 db 03 90 80 2f 14 00 78	89 7f 01 04 a6 cc 00 6d 00	2f f7 00 ee d1 a9 33 16	0a 00 c8 51 72 cc 00 00 6e 0a 00	00 b3 01 16 d5 a8 39 14 74 00	02 b0 00 f1 11 c0 00 2e 08 23	0f E 02 . 00 F 82 . 87 . 2c . 2f . 00 . 63 .	> E E C W 0 5	@. x. 4J .+ }	@ M { ./. xmi		,	
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 00a0	00 45 c0 50 c4 16 10 c0 00 11 6f	04 00 7c 18 03 43 57 30 35 77 6d 00	00 00 f9 72 03 ec cc 00 77 00 17	01 f5 09 10 d1 d4 00 0a 77 17 00	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 69 ff	00 00 bb 00 b7 4a 2b 13 7d 6e 01	40 4d 16 2c 7b c0 c0 00 75 00 0b	06 db 03 90 80 2f 14 00 78 01 00	89 7f 01 04 a6 cc 00 6d 00	2f f7 00 ee d1 a9 33 16 69 00	0a 00 c8 51 72 cc 00 00 6e 0a 00 68	00 b3 01 16 d5 a8 39 14 74 00 00 32	02 b0 00 f1 11 c0 00 2e 08 23 08	0f E 02 . 00 F 82 . 87 . 2c . 2f . 00 . 63 . 00 .	> E C W 5 wwwli	@. 4J .+ .}	@ M { ./. .xmi	/ .0 .r 3.9./		
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 00a0 00b0	00 45 c0 50 c4 16 10 c0 00 11 6f	04 00 7c 18 03 43 57 30 35 77 6d 00 33	00 00 f9 72 03 ec cc 00 77 00 17	01 f5 09 10 d1 d4 00 0a 0a 77 17 00 00	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 69 ff 19	00 00 bb 00 b7 4a 2b 13 7d 6e 01 00	40 4d 16 2c 7b c0 c0 00 75 00	06 db 03 90 80 2f 14 00 78 01 00	89 7f 01 04 a6 cc 00 6d 00 02 15	2f f7 00 ee d1 a9 33 16 69 00	0a 00 c8 51 72 cc 00 00 6e 0a 00 68	00 b3 01 16 d5 a8 39 14 74 00 00 32	02 b0 00 f1 11 c0 00 2e 08 23	0f E 02 . 00 F 82 . 87 . 2c . 2f . 00 . 63 . 00 .	> E E CE W 0 5 wwwlim	@. 4J .+ }	@ M { ./. .xmi	/ .0 .r 3.9./	, , , , , , , , , , , , , , , , , , , ,	
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 00a0 00b0 00c0	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	00 00 f9 72 03 ec c0 00 77 00 17 74	01 f5 09 10 d1 d4 00 0a 0a 77 17 00 00 2f	00 eb c5 c6 08 89 00 c0 12 e 00 18 00 33	06 3e 9c 7c 45 60 1e 09 00 6c 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 00	40 4d 16 2c 7b c0 c0 00 75 00 0b 17 68	06 db 03 90 80 2f 14 00 78 01 00 00 74	89 7f 01 04 a6 cc 00 6d 00 2 15 74	2f f7 00 ee d1 a9 33 16 69 00 01 02 70	0a 00 c8 51 72 cc 00 00 6e 0a 00 68 2f	00 b3 01 16 d5 a8 39 14 74 00 00 32	02 b0 00 f1 11 c0 00 2e 08 23 08 2e	0f E 02 . 00 F 82 . 87 . 2c . 2f . 00 . 63 . 00 . 73 .	> E E CE CE CE CE CE	@. 4J .+ .} n u	@ M { ./. .xmi	/ .0 .r 3.9./	, , , , , , , , , , , , , , , , , , , ,	
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 00b0 00c0 00d0	00 45 c0 50 c4 16 10 c0 00 11 6ff 066 00 70 00	04 00 7c 18 03 43 57 30 35 77 6d 00 33 64 05	00 00 f9 72 03 ec cc 00 77 00 17 74 79	01 f5 09 10 d1 d4 00 0a 77 17 00 00 2f 05	00 eb c5 c6 08 89 00 c0 12 e 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	40 4d 16 2c 7b c0 00 75 00 0b 17 68 00	06 db 03 90 80 2f 14 00 78 01 00 00 74 00	89 7f 01 04 a6 cc 00 6d 00 02 15 74 0d	2f f7 00 ee d1 a9 33 16 69 00 01 02 70 00	0a 00 c8 51 72 cc 00 00 6e 0a 2f 18	00 b3 01 16 d5 a8 39 14 74 00 00 32 31 00	02 b0 00 f1 11 c0 00 2e 08 23 08 2e	0f E 02 . 00 F 82 . 87 . 2c . 2f . 00 . 63 . 00 . 73 . 31 p	> E E CE C	@. 4J .+ .} n u	@ M { ./. .xmi	/ .0 .r 3.9./	, , , , , , , , , , , , , , , , , , , ,	

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

What is a Heartbleed vulnerability?

A. denial of service

https://www.leads4pass.com/200-201.html Leads4Pass

2024 Latest leads4pass 200-201 PDF and VCE dumps Download

- B. information disclosure
- C. buffer overflow
- D. command injection

Correct Answer: B

QUESTION 6

Which of these describes volatile evidence?

- A. logs
- B. registers and cache
- C. disk and removable drives
- D. usernames

Correct Answer: B

Caches and Registers- Data in memory is the most volatile. This includes data in central processor unit (CPU) registers, caches, and system random access memory(RAM).- The data in cache and CPU registers is the most volatile,

mostlybecause the storage space is so small.

https://blogs.getcertifiedgetahead.com/cfr-and-order-ofvolatility/#:~:text=Caches%20and%20Registers,storage%20space%20is%20so%20small.

QUESTION 7

Refer to the exhibit.

```
Capturing on 'eth0'
    1 0.000000000 ca:4f:4d:4b:38:5a ? Broadcast
                                                  ARP 42 Who has 192.168.88.149?
Tell 192.168.88.12
   2 0.000055428 82:69:61:3e:fa:99 ? ca:4f:4d:4b:38:5a ARP 42 192.168.88.149 is at
82:69:61:3e:fa:99
    3 0.000080556 192.168.88.12 ? 192.168.88.149 TCP 74 49098 ? 80 [SYN] Seq=0
Win=64240 Len=0 MSS=1460 SACK PERM=1 TSval=65609529 TSecr=0 WS=128
```

What must be interpreted from this packet capture?

A. IP address 192.168.88 12 is communicating with 192 168 88 149 with a source port 74 to destination port 49098 using TCP protocol

- B. IP address 192.168.88.12 is communicating with 192 168 88 149 with a source port 49098 to destination port 80 using TCP protocol.
- C. IP address 192.168.88.149 is communicating with 192.168 88.12 with a source port 80 to destination port 49098

Leads4Pass

https://www.leads4pass.com/200-201.html

2024 Latest leads4pass 200-201 PDF and VCE dumps Download

using TCP protocol.

D. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.

Correct Answer: B

QUESTION 8

Which regular expression is needed to capture the IP address 192.168.20.232?

A. ^ (?:[0-9]{1,3}\.){3}[0-9]{1,3}

B. ^ (?:[0-9]f1,3}\.){1,4}

C. ^ (?:[0-9]{1,3}\.)\\'

D. ^ ([0-9]-{3})

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/cs-mars/4-3/user/guide/local_controller/appreexp.html

QUESTION 9

What is the role of NAT in data visibility?

- A. load balancing
- B. hiding IP addresses
- C. web filtering
- D. encrypting files

Correct Answer: B

QUESTION 10

An engineer needs to have visibility on TCP bandwidth usage, response time, and latency, combined with deep packet inspection to identify unknown software by its network traffic flow. Which two features of Cisco Application Visibility and Control should the engineer use to accomplish this goal? (Choose two.)

A. management and reporting

B. traffic filtering

- C. adaptive AVC
- D. metrics collection and exporting
- E. application recognition

Correct Answer: AE

QUESTION 11

Refer to the exhibit.

			Tin	ne	-	Sou	rce]	Dest	inati	on		Prot	ocol	Leng	th Info			
		10	U.1	7115	TO	10.1	1.4.	10		LJZ.	124	. 445	. >	IUP	ALUSAN - 1981		0 20200	OPP+([DIN]	seq-
		000000	A RESERVED	000000000000000000000000000000000000000	SCHOOL STATE	OCCUPATION OF	94550000000	1.249.	200	200002000	STATE OF THE PERSON NAMED IN	CONTRACT.	-200	TCP		(52 443→5	0588	[SYN,	ACK]
						10.0						.249	. 9	TCP		5	6 50588	3→443	[ACK]	Seq=
		21	0.0	0229	88	192	.124	1.249.	PERSONAL PROPERTY.	security pac	(COURSESSE)	0000		TCP		(52 443→5	0586	[SYN,	ACK]
						10.0			1	192.	124	.249	. 9	TCP		5	6 50586	→443	[ACK]	seq=
		23	0.0	0232	12	10.0	0.2.	15	1	192.	124	.249	.9	TCP		26	51 50588	3→443	[PSH,	ACK
			0.0	0233	373	10.0				192.	124		.9				1 5058			ACK
			10070000		100000000000000000000000000000000000000	Control of the last		.249.	7999 HE	1000000000	4000			TCP			2 443→5		[ACK]	seq=
			10000000				1979-1900-190	1.249.		000000000000000000000000000000000000000				TCP			52 443→5			Seq:
								1.249.						TCP			92 443→5			
4 (2.8	0.0	374	26	10.0).2.	.15		192.	124	.249	. 9	TCP			56 50586	-443	[ACK]	Sea
	_	16	030	1000	801	.000	0c4	03030	e06	ead	1078	d176	76	c13a	ab46	ebf				
0000	00	3337	0.53275		3000	06	34.76.76						10000	00	38.470.0					
0010	45	00	00	f5	48	7b	40	00	40	06	2b	f3	0a	00	02	Of E	H{@.			
0010 0020	45 c0	00 7c	00 f9	f5 09	48 c5	7b 9a	40 01	00 dd	40 0e	06 1f	2b dc	f3 b4	0a 00	00 b4	02 aa	0f E		@.+		
0010 0020 0030	45	00	00	f5 09 10	48 c5 c6	7b 9a 7c	40 01 00	00 dd 00 00	40 0e 16	06 1f 03	2b dc 01	f3 b4 00	0a 00 c8	00 b4 01	02 aa 00	0f E	Н{@.	0.+	 	
0010 0020 0030 0040	45 c0 50 c4	00 7c 18 03	00 f9 72 03	f5 09 10 0e	48 c5 c6 06	7b 9a 7c ea	40 01 00 d0	00 dd 00 00	40 0e 16	06 1f 03 76	2b dc 01 76	f3 b4 00 c1	0a 00 c8 3a	00 b4 01 b4	02 aa 00 6e	0f E 02 . 00 F	H{@.	@.+ · · · ·	 	
0010 0020 0030 0040 0050	45 c0 50 c4	00 7c 18 03	00 f9 72 03	f5 09 10 0e	48 c5 c6 06	7b 9a 7c	40 01 00 d0	00 6 bb 0 00 7	40 0e 16 dl	06 1f 03 76	2b dc 01 76	f3 b4 00	0a 00 c8 3a	00 b4 01 b4	02 aa 00 6e	0f E 02 . 00 F bf .	H{@.	@.+ 	 	
0010 0020 0030 0040 0050	45 c0 50 c4 e6	00 7c 18 03	00 f9 72 03 b8	f5 09 10 0e b2	48 c5 c6 06 ba	7b 9a 7c ea	40 01 00 d0 d6	00 6 bb 0 00 7 78 6 6d 0	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 E 02 . 00 F bf . ee .	:H{@.	@.+ 	n	
0010 0020 0030 0040 0050 0060	45 c0 50 c4 e6 8b	00 7c 18 03 b8	00 f9 72 03 b8	f5 09 10 0e b2 00	48 c5 c6 06 ba 00	7b 9a 7c ea 08	40 01 00 d0 d6 c0	00 6 bb (00 7 78 6 6d (2b (40 0e 16 d1 0d	06 1f 03 76 38 2f	2b dc 01 76 fb	f3 b4 00 c1 91 a9	0a 00 c8 3a 45	00 b4 01 b4 de	02 aa 00 6e fc	0f E 02 . 00 F bf . ee .	:H{@.	@.+ vv n .8 + ./	n	
0010 0020 0030 0040 0050 0060 0070	45 c0 50 c4 e6 8b c0	00 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	00 db 00 178 dd 02b dd 13 dd	40 0e 16 d1 0d	06 1f 03 76 38 2f	2b dc 01 76 fb cc	f3 b4 00 c1 91 a9 33	0a 00 c8 3a 45	00 b4 01 b4 de a8	02 aa 00 6e fc c0	0f E 02 . 00 F bf . ee . 2c . 2f .	H{@.	@.+ vv n .8 + ./	.:.n	
0010 0020 0030 0040 0050 0060 0070 0080	45 c0 50 c4 e6 8b c0	00 7c 18 03 b8 6e 30	00 f9 72 03 b8 f8	f5 09 10 0e b2 00 0a	48 c5 c6 06 ba 00 c0	7b 9a 7c ea 08 1e 09	40 01 00 d0 d6 c0 c0	00 db 00 78 6d 02b 07d 7d 0	40 0e 16 d1 0d c0 c0	06 1f 03 76 38 2f 14 00	2b dc 01 76 fb cc 00	f3 b4 00 c1 91 a9 33	0a 00 c8 3a 45 cc 00	00 b4 01 b4 de a8 39	02 aa 00 6e fc c0	0f E 02 . 00 F bf . ee . 2c . 2f . 00 .	H{@.	@.+ c.vv n 8 + ./	.:.nE	
0010 0020 0030 0040 0050 0060 0070 0080 0090	45 c0 50 c4 e6 8b c0 00	00 7c 18 03 b8 6e 30 35	00 f9 72 03 b8 f8 c0	f5 09 10 0e b2 00 0a 0a	48 c5 c6 06 ba 00 c0	7b 9a 7c ea 08 1e 09 00 6c	40 01 00 d0 d6 c0 c0	00 bb (00 78 6d (2b (2b 7d (6e)	40 0e 16 d1 0d c0 c0	06 1f 03 76 38 2f 14 00	2b dc 01 76 fb cc 00 00	f3 b4 00 c1 91 a9 33 16	0a 00 c8 3a 45 cc 00 6e	00 b4 01 b4 de a8 39	02 aa 00 6e fc c0 00	0f E 02 . 00 F bf . ee . 2c . 2f . 00 . 63 .	n	@.+ c .vv n .8 + ./ }	.:.nE	
0010 0020 0030 0040 0050 0060 0070 0080 0090 00a0	45 c0 50 c4 e6 8b c0 00	00 7c 18 03 b8 6e 30 35 77	00 f9 72 03 b8 f8 c0 00 77	f5 09 10 0e b2 00 0a 0a 77	48 c5 c6 06 ba 00 c0 01 2e	7b 9a 7c ea 08 1e 09 00 6c	40 01 00 d0 d6 c0 c0 00	00 6 bb 0 78 6 6d 0 2b 6 13 6 6e 6	40 0e 16 d1 0d c0 c0	06 1f 03 76 38 2f 14 00 78	2b dc 01 76 fb cc 00 6d	f3 b4 00 c1 91 a9 33 16 69	0a 00 c8 3a 45 cc 00 6e	00 b4 01 b4 de a8 39 14	02 aa 00 6e fc c0 00 00	0f E 02 . 00 F bf . ee . 2c . 2f . 00 . 63 .	H{@.	@.+ vv n .8 + ./ 	.:.nE	
0010 0020 0030 0040 0050 0060 0070 0080 0090 00a0 00b0	45 c0 50 c4 e6 8b c0 00 11 6f	00 7c 18 03 b8 6e 30 35 77 6d	00 f9 72 03 b8 f8 c0 00 77 00	f5 09 10 0e b2 00 0a 0a 77 17	48 c5 c6 06 ba 00 c0 01 2e 00	7b 9a 7c ea 08 1e 09 00 6c 00	40 01 00 d0 d6 c0 c0 69 ff	00 6 6 6 6 6 6 6 00 00 6	40 0e 16 d1 0d c0 00 75	06 1f 03 76 38 2f 14 00 78 01	2b dc 01 76 fb cc 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	02 aa 00 6e fc c0 00 2e 08	0f E 02 . 00 E bf . ee . 2c . 2f . 00 . 63 . 00 . 00	0H(@.	@.+ c.vv n .8 + ./ uxm.	.:.nE	
0010 0020 0030 0040 0050 0060 0070 0080 0090 00a0 00b0 00c0	45 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	48 c5 c6 06 ba 00 c0 01 2e 00 18	7b 9a 7c ea 08 1e 09 00 6c 00 00	40 01 00 d0 d6 c0 c0 69 ff 19	00 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	40 0e 16 d1 0d c0 c0 75 00 0b	06 1f 03 76 38 2f 14 00 78 01 00	2b dc 01 76 fb cc 00 6d 00 02 15	f3 b4 00 c1 91 a9 33 16 69 00 01	0a 00 c8 3a 45 cc 00 6e 0a 00 68	00 b4 01 b4 de a8 39 14 74 00 00 32	02 aa 00 6e fc c0 00 2e 08 23 08	0f E 02 . 00 E bf . ee . 2c . 2f . 00 . 63 . 00 . 73	%.r . %.r . %.r . 0 5 wwwlin	@.+ 	.:.n .E .3.9./	
0010 0020 0030 0040 0050 0060 0070 0080 0090 00b0 00c0 00d0	45 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	00 f9 72 03 b8 f8 c0 00 77 00 17 74 79	f5 09 10 0e b2 00 0a 0a 77 17 00 00 2f	48 c5 c6 06 ba 00 c0 01 2e 00 18 00 33	7b 9a 7c ea 08 1e 09 00 6c 00 00 2e	40 01 00 d0 d6 c0 00 69 ff 19 10 31	00 bb 00 78 6d 02b 66 7d 66 01 00 00 00 08	40 0e 16 d1 0d c0 c0 75 00 0b 17	06 1f 03 76 38 2f 14 00 78 01 00 74	2b dc 01 76 fb cc 00 6d 00 74	f3 b4 00 c1 91 a9 33 16 69 00 01 02 70	0a 00 c8 3a 45 cc 00 6e 0a 68 2f	00 b4 01 b4 de a8 39 14 74 00 00 32 31	02 aa 00 6e fc c0 00 2e 08 23 08 2e	0f E 02	0H(@.	@.+ 	.:.n .E .3.9./	
0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 00b0 00c0 00d0 00e0	45 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 0a 77 17 00 00 2f 05	48 c5 c6 06 ba 00 c0 01 2e 00 18 00 33 01	7b 9a 7c ea 08 1e 09 00 6c 00 00 2e 00	40 01 00 d0 d6 c0 c0 69 ff 19 10 31	00 bb 00 78 6d 02 b 66 01 00 00 00 00 00 00 00 00 00 00 00 00	40 0e 16 d1 0d c0 c0 75 00 0b 17 68	06 1f 03 76 38 2f 14 00 78 01 00 00 74 00	2b dc 01 76 fb cc 00 6d 00 2 15 74 0d	f3 b4 00 c1 91 a9 33 16 69 00 01 02 70	0a 00 08 3a 45 00 00 6e 0a 2f	00 b4 01 b4 de a8 39 14 74 00 00 32 31 00	02 aa 00 6e fc c0 00 2e 08 23 08 2e 16	0f E 02	%.r . %.r . %.r . 0 5 wwwlin	@.+ 	.:.n .E .3.9./	
0010 0020 0030 0040 0050 0060 0070 0080 0090 00b0 00c0 00d0	45 c0 50 c4 e6 8b c0 00 11 6f 06 70 00 01	00 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 0a 77 17 00 00 2f 05	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 2e	40 01 00 d0 d6 c0 c0 69 ff 19 10 31	00 bb 00 78 6d 02 b 66 01 00 00 00 00 00 00 00 00 00 00 00 00	40 0e 16 d1 0d c0 c0 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 2 15 74 0d	f3 b4 00 c1 91 a9 33 16 69 00 01 02 70	0a 00 08 3a 45 00 00 6e 0a 2f	00 b4 01 b4 de a8 39 14 74 00 00 32 31 00	02 aa 00 6e fc c0 00 2e 08 23 08 2e 16	0f E 02 . 00 E bf . ee . 2c . 2f . 00 . 63 . 00 . 63 . 31 F 04 . 05 .	%.r . %.r . %.r . 0 5 wwwlin	@.+ 	.:.n .E .3.9./	

Which application protocol is in this PCAP file?

A. SSH

B. TCP



C.	TI	LS

D. HTTP

Correct Answer: C

QUESTION 12

Refer to the exhibit.

File Details

File name	lfile_saw.exe
File size	95084 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	3D2C6A23
MD5	d215cb65b405ab31b1b516a781c6b1ed
SHA1	1a855455a912c721b42f2665a9a0365b97d68a42
SHA256	e24669e5a2f74ab567c72d5030abedc4ed9f90ba23436b8db43b8fe63adecdd2
SHA512	56dbf450d5908bf958cd11928d7clbf847ee82613e006fc692888872281f69ca370aae3d93c2b803febc3372845bb5ef36b
Ssdeep	1536:WfX+sEYF75idaQwndckc9esY3iSa4Hlp2uLEKBa0e3IyWTWc80MzY75:qXBEYF7KmQwnRc9esYSSG9fnxdW4vS
PEID	None matched
Yara	• zeus_1 (Zeus Trojan)

A SOC engineer is analyzing the provided Cuckoo Sandbox report for a file that has been downloaded from an URL, received via email. What is the state of this file?

- A. The file was identified as PE32 executable for MS Windows and the Yara filed lists it as Trojan.
- B. The file was detected as executable and was matched by PEiD threat signatures for further analysis.
- C. The file was detected as executable, but no suspicious features are identified.
- D. The calculated SHA256 hash of the file was matched and identified as malicious.

Correct Answer: A

QUESTION 13

What is session data used for in network security?

A. It contains the set of parameters used for fetching logs.



https://www.leads4pass.com/200-201.html

2024 Latest leads4pass 200-201 PDF and VCE dumps Download

- B. It tracks cookies within each session initiated from user.
- C. It is the transaction log between monitoring software.
- D. It is the summary of the transmission between two network devices.

Correct Answer: D

Session data is a record of a conversation between two network endpoints, which are often a client and a server.

QUESTION 14

Which example represents the defense-in-depth principle?

- A. implementing a CMDB
- B. creating a separate VLAN to isolate networks
- C. creating a privileged group in AD
- D. implementing new security policy within the organization

Correct Answer: B

QUESTION 15

How does statistical detection differ from rule-based detection?

- A. Statistical detection involves the evaluation of events, and rule-based detection requires an evaluated set of events to function.
- B. Statistical detection defines legitimate data over time, and rule-based detection works on a predefined set of rules
- C. Rule-based detection involves the evaluation of events, and statistical detection requires an evaluated set of events to function Rule-based detection defines
- D. legitimate data over a period of time, and statistical detection works on a predefined set of rules

Correct Answer: B

Latest 200-201 Dumps

200-201 Practice Test

200-201 Braindumps