

# Cisco

# Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals





#### **NEW QUESTION 1**

An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

- A. Recovery
- B. Detection
- C. Eradication
- D. Analysis

Answer: B

# **NEW QUESTION 2**

Which signature impacts network traffic by causing legitimate traffic to be blocked?

- A. false negative
- B. true positive
- C. true negative
- D. false positive

Answer: D

# **NEW QUESTION 3**

A company encountered a breach on its web servers using IIS 7 5 Dunng the investigation, an engineer discovered that an attacker read and altered the data on a secure communication using TLS 1 2 and intercepted sensitive information by downgrading a connection to export-grade cryptography. The engineer must mitigate similar incidents in the future and ensure that clients and servers always negotiate with the most secure protocol versions and cryptographic parameters. Which action does the engineer recommend?

- A. Upgrade to TLS v1 3.
- B. Install the latest IIS version.
- C. Downgrade to TLS 1.1.
- D. Deploy an intrusion detection system

Answer: B

# **NEW QUESTION 4**

Which event is user interaction?

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

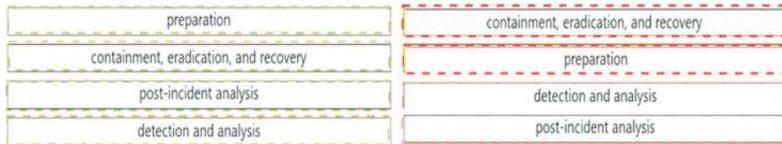
Answer: D

# **NEW QUESTION 5**

Drag and drop the elements from the left into the correct order for incident handling on the right.

preparation	create communication guidelines for effective incident handling	
containment, eradication, and recovery	gather indicators of compromise and restore the system	
post-incident analysis	document information to mitigate similar occurrences	
detection and analysis	collect data from systems for further investigation	





#### Does this meet the goal?

A. Yes B. No

Answer: A

#### **NEW QUESTION 6**



Which event artifact is used to identify HTTP GET requests for a specific file?

A. destination IP addressB. TCP ACKC. HTTP status codeD. URI

Answer: D

**NEW QUESTION 7** Refer to the exhibit.

Companying on Lab

```
Capturing on 'eth0'

1 0.00000000 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 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 49098 using TCP protocol.

Answer: B

#### **NEW QUESTION 8**

Which system monitors local system operation and local network access for violations of a security policy?

A. host-based intrusion detection

- B. systems-based sandboxing
- C. host-based firewall
- D. antivirus

#### Answer: A

#### Explanation:

HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

#### **NEW QUESTION 9**

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

A. detection and analysis

- B. post-incident activity
- C. vulnerability scoring
- D. vulnerability management

E. risk assessment

Answer: AB

#### **NEW QUESTION 10**

What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.

B. Tampered images are used as evidence.

C. Untampered images are used for forensic investigations.

D. Untampered images are deliberately altered to preserve as evidence

Answer: D

#### **NEW QUESTION 11**

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.

Answer: C



https://www.surepassexam.com/200-201-exam-dumps.html (263 New Questions)

#### **NEW QUESTION 12**

What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?

- A. TAPS interrogation is more complex because traffic mirroring applies additional tags to data and SPAN does not alter integrity and provides full duplex network.
- B. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.
- C. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools
- D. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.

#### Answer: D

#### **NEW QUESTION 13**

What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

A. central key management server

- B. web of trust
- C. trusted certificate authorities
- D. registration authority data

Answer: C

#### **NEW QUESTION 14**

What is the difference between a threat and a risk?

- A. Threat represents a potential danger that could take advantage of a weakness in a system
- B. Risk represents the known and identified loss or danger in the system
- C. Risk represents the nonintentional interaction with uncertainty in the system
- D. Threat represents a state of being exposed to an attack or a compromise, either physically or logically.

#### Answer: A

#### Explanation:

A threat is any potential danger to an asset. If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known—the threat is latent and not yet realized.

#### **NEW QUESTION 15**

Which utility blocks a host portscan?

A. HIDS

- B. sandboxing
- C. host-based firewall
- D. antimalware

Answer: C

# NEW QUESTION 16

Refer	to	the	exhibit.
1,0101	ιU		OMIDIC.

. Time	Source	Destination	Protocol	ength Info 4 1341 - 66 (SYN) Segm0 Win	CLAN IN COLUMN	
1 0.000000	10.128.0.2	10.0.0.2	TCP		0 Ack=1 Win=29288 Len=0 NSS	-1469
2 0.003987		10.0.0.2	TCP			
3 0.005514	10.128.0.2	10.128.0.2	TCP		0 Ack=1 Win=29200 Len=0 NSS	1400
4 0.008429	10.0.0.2		TCP	4 3342 - 80 [SYN] Seq=0 Win	AN A REPORT OF A	
5 0.010233	10.128.0.2	10.0.0.2			0 Ack=1 Win=2988 Len=0 NSS=1	
6 0.014072	10.128.0.2	10.0.0.2	TCP		0 Ack=1 Win=2900 Len=0 NSS=)	1460
7 0.016830	10.0.0.2	10.128.0.2	TCP	4 3343 - 88 [SYN] Seq=0 Win		100-22
8 0.022220	10.128.0.2	10.0.0.2	TCP		0 Ack=1 Win=29200 Len=0 MSS	
9 0.023496	10.128.0.2		TCP		0 Ack=1 Win=29200 Len=0 MSS	=1460
10 0.025243	10.0.0.2	10.128.0.2	TCP	4 3344 - 88 [SYN] Seq=0 Win		
11 0.026672	10.128.0.2		TCP		0 Ack=1 Win=29200 Len=0 MSS	
	10.128.0.2	10.0.0.2	TCP		Q Ack=1 Win=29200 Len=0 MSS:	
13 0.030523	10.128.0.2	10.0.0.2	TCP	8 88 - 3344 [SYN, ACK] Seq=	0 Ack=1 Win=29200 Len=0 MSS:	=1460
thernet II, Sro nternet Protoco ransmission Con Source Port: 3	2: 42:01:0a:f ol Version 4, ntrol Protoco 341	Src: 18.0.0.	2, Dst: 10	7), Dat: 42:01:0a:f0:00:01 28.0.2 rt: 80, Seq: 0, Len: 0	(42:01:0a:f0:00:01)	
Internet Protoco Fransmission Con Source Port: 3 Destination Po [Stream index: [TCP Segment L	:: 42:01:0a:f ol Version 4, atrol Protoco 341 rt: 80 0] en: 0]	0:00:17 (42:0 Src: 18.0.0. ), Src Port:	1:0a:f0:00 2, Dst: 10 3341, Dst	7), Dat: 42:01:0a:f0:00:01 28.0.2	(42:01:0a:£0:00:01)	
Athernet II, Sro Internet Protoco Fransmission Con Source Port: 3 Destination Po [Stream index:	<pre>: 42:01:0a:f 1 Version 4, trol Protoco 341 rt: 80 0] en: 0] r: 0 (relativ</pre>	ve sequence nu	(1:0a:f0:00 2, Dst: 10 3341, Dst	7), Dat: 42:01:0a:f0:00:01 28.0.2 rt: 80, Seq: 0, Len: 0	(42:01:0a:£0:00:01)	
thernet II, Sro Chternet Protoco Fransmission Con Source Port: 3 Destination Po [Stream index: [TCP Segment L. Sequence numbe [Next sequence Acknowledgemen	<pre>:: 42:01:0a:f of Version 4, atrol Protoco 341 rt: 80 0] en: 0] r: 0 (relativ number: 0 (r t number: 10)</pre>	ve sequence nu relative seque	(1:0a:f0:00 2, Dst: 10 3341, Dst	7), Dat: 42:01:0a:f0:00:01 28.0.2 rt: 80, Seq: 0, Len: 0	(42:01:0a:f0:00:01)	
thernet II, Sro Internet Protoco Source Port: 3 Destination Poo [Stream index: [TCP Segment L Sequence numbe [Next sequence Acknowledgemen 0101 = Head Flags: 0x002 ( Windows Size V	:: 42:01:0a:f ) Version 4, http://protocol 341 rt: 80 0] en: 0] r: 0 (relativ number: 0 (: t number: 10 er Length: 20 SYN) alue: 512	0:00:17 (42:0 Src: 18.0.0. bl, Src Port: ve sequence nu relative seque 23350884 0 bytes (5)	(1:0a:f0:00 2, Dst: 10 3341, Dst	7), Dat: 42:01:0a:f0:00:01 28.0.2 rt: 80, Seq: 0, Len: 0	(42:01:0a:f0:00:01)	
thernet II, Sro Internet Protoco Source Port: 3 Destination Poo [Stream index: [TCP Segment L- Sequence numbe [Next sequence 0101 = Head Flags: 0x002 ( Windows Size V [Calculated wi Checksum: 0x8d	:: 42:01:0a:f ) Version 4, htrol Protoco 341 rt: 80 0] en: 0] r: 0 (relativ number: 00 rt number: 10 er Length: 20 SYN) alue: 512 ndow size: 5: 5a [unverified]	0:00:17 (42:0 Src: 18.0.0. ), Src Port: ve sequence nu relative seque 23350884 0 bytes (5) 12] ed]	(1:0a:f0:00 2, Dst: 10 3341, Dst	7), Dat: 42:01:0a:f0:00:01 28.0.2 rt: 80, Seq: 0, Len: 0	(42:01:0a:f0:00:01)	
thernet II, Sro Chternet Protocor Source Port: 3 Destination Po [Stream index: [TCP Segment L- Sequence numbe [Next sequence Acknowledgemen 0101 = Head Plags: 0x002 Windows Size V [Calculated wi Checksum: 0x8d [Checksum Stat	:: 42:01:0a:f ) Version 4, htrol Protoco 341 rt: 80 0] en: 0] r: 0 (relativ number: 0 (: t number: 10 er Length: 2 SYN) alue: 512 ndow size: 5: 5a [unverificus: Unverificus:	0:00:17 (42:0 Src: 18.0.0. ), Src Port: ve sequence nu relative seque 23350884 0 bytes (5) 12] ed]	(1:0a:f0:00 2, Dst: 10 3341, Dst	7), Dat: 42:01:0a:f0:00:01 28.0.2 rt: 80, Seq: 0, Len: 0	(42:01:0a:f0:00:01)	
thernet II, Sro Internet Protoco Source Port: 3 Destination Poo [Stream index: [TCP Segment L- Sequence numbe [Next sequence 0101 = Head Flags: 0x002 ( Windows Size V [Calculated wi Checksum: 0x8d	:: 42:01:0a:f ) Version 4, htrol Protoco 341 rt: 80 0] en: 0] r: 0 (relativ number: 0 (: t number: 10 er Length: 2 SYN) alue: 512 ndow size: 5: 5a [unverificus: Unverificus:	0:00:17 (42:0 Src: 18.0.0. ), Src Port: ve sequence nu relative seque 23350884 0 bytes (5) 12] ed]	(1:0a:f0:00 2, Dst: 10 3341, Dst	7), Dat: 42:01:0a:f0:00:01 28.0.2 rt: 80, Seq: 0, Len: 0	(42:01:0a:£0:00:01)	

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.

## Answer: D



#### **NEW QUESTION 17**

How is NetFlow different from traffic mirroring?

- A. NetFlow collects metadata and traffic mirroring clones data.
- B. Traffic mirroring impacts switch performance and NetFlow does not.
- C. Traffic mirroring costs less to operate than NetFlow.
- D. NetFlow generates more data than traffic mirroring.

Answer: A

# **NEW QUESTION 18**

#### Refer to the exhibit.

5585 43,600368	192.168.56.183	197.168.00.8	10*	NE KK - AMERIC INCREMENTATING ACCOMPT MINI JELIS LENCE TSVAL SEPTIALISE TSecr-1715
5586 43.684379	192.168.50.101	192.168.56.2	S5Hv2	146 Server: Encrypted packet (len:00)
5587 43.604462	192 168.50.1	192.168.56.101	55Hv2	162 Client: Encrypted packet (lanis6)
5568 43 684497	192.168.56.201	192.168.56.1	TCF	66 22 - 39924 [ACK] Seg12122 Ack1743 Wint30336 Leni0 15val13697142357 15ecr11715
1589 43.011441	192.168.56.101	192.168.56.1	15Hv2	130 Server: Encrypted packet (len:64)
5550 43.011542	192.168.56.1	192.148.56.101	55Mv2	145 Client, Encrypted packet (len)86)
5591 43 411856	192.148.56.101	197.168.55.1	55842	538 Server: Diffie Hellman Key Eschange Reply, New Keys, Encrypted packet (lenit)
5597 48.812193	192.168 56 1	192.168.56.181	\$34rv2	82 Client: New Keys
5593 43.612287	197.168.50.101	192.168.56.1	TCP	66 22 - 39854 [ACK] Seg(1594 Ack:759 W10)30336 Len(0 TSval)3007142364 TSec(1)715
5594 43 012668	102.168.56.1	192.168.54.101	SSMV2	130 Client: Encrypted packet (leo:64)
5595 43.012097	192.168.56 101	192.168.56 t	TCP	66.22 - 39884 [ACK] Seg11594 Ack1823 Wim130336 Lemi0 TSval13697142365 TSecrit115
5596 43.615355	197,168 56 101	192 168.50.1	SSHv2	187 Server: Protocol (15H-2.0 Open55H 7 9p1 Debian 10+deb10u1)
5597 43,015375	192 168 56 1	192.168.56.101	TCP	66 39956 - 22 [ACK] Seg122 Ack142 Win129312 Len18 TSval11715548358 TSecr13697142
5598 43 615717	192.108.56.1	192.168.56 101	55842	738 Client: Key Exchange Init
5599 43.619998	192.168.56.101	192.168.58.1	55MV2	130 Server: Encrypted packet (len:04)
5600 43 619184	192.168.56 1	192.168.56.181	SSHv2	146 Client: Encrypted packet (len:80)
5601 43,624638	192,168.56.181	192.168.56.1	109	66 22 - 40018 [457, ACK] Septi Ack123 kin129050 (en10 15va[1369/142377 15ecr1371
5602 43.824751	192.168.56.101	192-148.56.1	TOP	66 22 - 40020 [RST, ACK] Segri Ack+23 Win+29056 Len+8 T5va1+5607142377 TSecr=171
5603 43.624867	192.108.58.101	192.168.56.1	TOP	66 22 - 40022 [RST, ACK] Sept1 Acks28 Wins29058 Lens8 T5vals3687142377 TSecre171
5604 43 625010	152.168.56.181	192.168.55.1		66 22 - 40024 [RST, ACK] Seg-1 Ack+23 Win+29056 Lenve TSval+3007142377 TSecr=171
5605 43.625111	192.168.58.101	192.168.56.1	TOP	66 22 - 40926 [RST, ACK] Sept1 Ack#23 Wint29050 Lent0 TSval#3007143377 TSecr#171
5006 43 825723	192.168.56.101	192.108.50.1	TCP.	65 22 - 40030 [RST, ACK] Segi1 Ack+23 Win+29056 Len+0 T5va1+3007142378 TSecr=171
5607 43.625835	192.168.56.101	192.168.56.1	TOP	66 22 - 40932 [RST, ACK] Segi1 Ack=23 Win=29050 Leni0 T5val=3097142378 TSecr=171
5668 43, 625985	192.168.56.101	192.168.56.1	TEP	66 22 - 40034 [RST, ACK] Septi Ackn23 Wint29056 Lent@ TSvalt3607142378 TSecret71
5603 43.626034	192.168.58.101	192.168.56.1	TOP	66 22 - 40038 [RST, ACK] Sept1 Ack+23 Win+29056 Len+8 Tova1+3687142378 TSecr+171
5618 43.626193	192-168.56-181	197.168.50.1	TOP	46 22 - 40040 [851, ACK] Sept1 Ack+23 Win+29056 Len+0 T5val+3007342578 T5ecr+171
5611 43 426283	192.568.58.101	192.168.56.1	TOP	66 22 - 40042 [RST, ACK] Segi1 Ack=23 Win=29056 Len=8 TSval=3097142378 TSecr=171
5632 43.626718	192.108.50.101	192.168.56.1	558v2	538 Server: Diffie-Wellman Key Exchange Roply, New Keys, Encrypted packet (lenvin
5613 43.627975	192.168.56.1	192.108.56.101	\$5Hv2	82 Client: New Keys
5614 43 827621	192.168.58.101	192.168.56.1	TCP	60 22 - 39878 [ACK] Seq:1594 Ack:759 Win=30356 Leni0 TSval=3097142308 TSecr:1715
40-8	COLUMN THE REAL PROPERTY OF	1	1.0 m 1	the second se

An engineer is analyzing a PCAP file after a recent breach An engineer identified that the attacker used an aggressive ARP scan to scan the hosts and found web and SSH servers. Further analysis showed several SSH Server Banner and Key Exchange Initiations. The engineer cannot see the exact data being transmitted over an encrypted channel and cannot identify how the attacker gained access How did the attacker gain access?

A. by using the buffer overflow in the URL catcher feature for SSH

- B. by using an SSH Tectia Server vulnerability to enable host-based authentication
- C. by using an SSH vulnerability to silently redirect connections to the local host

D. by using brute force on the SSH service to gain access

Answer: C

#### **NEW QUESTION 19**

Which security monitoring data type requires the largest storage space?

A. transaction data

- B. statistical data
- C. session data
- D. full packet capture

Answer: D

#### **NEW QUESTION 20**

A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows

B. CD data copy prepared in Mac-based system

C. CD data copy prepared in Linux system

D. CD data copy prepared in Android-based system

#### **NEW QUESTION 21**

What is a description of a social engineering attack?

A. fake offer for free music download to trick the user into providing sensitive dataB. package deliberately sent to the wrong receiver to advertise a new productC. mistakenly received valuable order destined for another person and hidden on purposeD. email offering last-minute deals on various vacations around the world with a due date and a counter

Answer: D

## **NEW QUESTION 22**

Which type of data collection requires the largest amount of storage space?

#### A. alert data



- B. transaction data C. session data
- D. full packet capture

## Answer: D

# **NEW QUESTION 23**

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

## **Explanation:**

Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

#### **NEW QUESTION 24**

A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

A. event name, log source, time, source IP, and host name

- B. protocol, source IP, source port, destination IP, and destination port
- C. event name, log source, time, source IP, and username
- D. protocol, log source, source IP, destination IP, and host name

#### Answer: B

#### **NEW QUESTION 25**

#### Refer to the exhibit.

9 16:40:35.696788 195.144.107.198 192.168.31.44 FTP 96 Response: 150 Opening BINARY mode data connection. 10 16:40:35.698384 195.144.107.198 192.168.31.44 TCP 66 1026 + 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 9 11 16:40:35.698521 192.168.31.44 195.144.107.198 TCP 54 1084 + 1026 [ACK] Seq=1 Ack=1 Win=132352 Len=0	7 16:40:35.637786		192.168.31.44	100 million (100 million)	
8 16:40:35.638091 192.168.31.44       195.144.107.198       TCP       66 1084 + 1026 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=         9 16:40:35.696788 195.144.107.198       192.168.31.44       FTP       96 Response: 150 Opening BINARY mode data connection.         10 16:40:35.698384 195.144.107.198       192.168.31.44       TCP       66 1026 + 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 S         11 16:40:35.698382 192.168.31.44       195.144.107.198       TCP       54 1084 + 1026 [ACK] Seq=1 Ack=1 Win=3132352 Len=0         12 16:40:35.698802 192.168.31.44       195.144.107.198       TCP       54 1084 + 1026 [ACK] Seq=4 Ack=1 Win=513 Len=0         13 16:40:35.759825 195.144.107.198       192.168.31.44       FTP_       2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)         15 16:40:35.759825 195.144.107.198       192.168.31.44       FTP_       2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)         15 16:40:35.759825 195.144.107.198       192.168.31.44       FTP_       5878 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)         17 16:40:35.832263 192.168.31.44       195.144.107.198       TCP       54 1084 + 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0         18 16:40:35.883496 195.144.107.198       192.168.31.44       FTP_       1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)         19 16:40:35.883596 195.144.107.198       192.168.31.44       FTP_ <td< td=""><td></td><td>103 100 34 44</td><td></td><td>FTP</td><td>104 Response: 227 Entering Passive Mode (195,144,107,198,4,2).</td></td<>		103 100 34 44		FTP	104 Response: 227 Entering Passive Mode (195,144,107,198,4,2).
9 16:40:35.696788 195.144.107.198       192.168.31.44       FTP       96 Response: 150 Opening BIMARY mode data connection.         10 16:40:35.698384 195.144.107.198       192.168.31.44       TCP       66 1026 + 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 9         11 16:40:35.698302 192.168.31.44       195.144.107.198       TCP       54 1084 + 1026 [ACK] Seq=1 Ack=1 Win=3132352 Len=0         12 16:40:35.698802 192.168.31.44       195.144.107.198       TCP       54 [TCP Window Update] 1084 + 1026 [ACK] Seq=1 Ack=1 Win=513 Len=0         13 16:40:35.739249 192.168.31.44       195.144.107.198       TCP       54 1081 + 21 [ACK] Seq=4 Ack=113 Win=513 Len=0         14 16:40:35.759825 195.144.107.198       192.168.31.44       FTP.       2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)         15 16:40:35.822152 195.144.107.198       192.168.31.44       FTP.       5878 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)         17 16:40:35.822263 192.168.31.44       195.144.107.198       TCP       54 1084 + 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0         18 16:40:35.883496 195.144.107.198       192.168.31.44       FTP.       1510 FTP Data: 1356 bytes (PASV) (RETR ResumableTransfer.png)         19 16:40:35.883496 195.144.107.198       192.168.31.44       FTP.       1510 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         19 16:40:35.883559 192.168.31.44       195.144.107.198       TCP       54	and an other states of the second	192.168.31.44	195.144.107.198	FTP	82 Request: RETR ResumableTransfer.png
1016:40:35.698384195.144.107.198192.168.31.44TCP661026 + 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 S1116:40:35.698521192.168.31.44195.144.107.198TCP541084 + 1026 [ACK] Seq=1 Ack=1 Win=32352 Len=01216:40:35.739249192.168.31.44195.144.107.198TCP541031 + 21 [ACK] Seq=4 Ack=1 Win=513 Len=01316:40:35.75925195.144.107.198192.168.31.44195.144.107.198TCP541084 + 1026 [ACK] Seq=1 Ack=2013 Win=513 Len=01416:40:35.75925192.168.31.44195.144.107.198TCP541084 + 1026 [ACK] Seq=1 Ack=2013 Win=4194304 Len=01516:40:35.75925192.168.31.44195.144.107.198TCP541084 + 1026 [ACK] Seq=1 Ack=2013 Win=4194304 Len=01616:40:35.822152195.144.107.198192.168.31.44FTP.5878 FTP Data:5824 bytes (PASV) (RETR ResumableTransfer.png)1716:40:35.822263192.168.31.44195.144.107.198TCP541084 + 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=01816:40:35.883496195.144.107.198192.168.31.44FTP.1510 FTP Data:1354 bytes (PASV) (RETR ResumableTransfer.png)1916:40:35.883496195.144.107.198192.168.31.44FTP.1408 FTP Data:1354 bytes (PASV) (RETR ResumableTransfer.png)1916:40:35.883599192.168.31.44FTP.1408 FTP Data:1354 bytes (PASV) (RETR ResumableTransfer.png)2016:40:35.883599192.168.31.44FTP.1408 FTP Data:1354 bytes (P	8 16:40:35.638091	192.168.31.44	195.144.107.198	TCP	66 1084 + 1026 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1016:40:35.698384195.144.107.198192.168.31.44TCP661026 + 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 S1116:40:35.698521192.168.31.44195.144.107.198TCP541084 + 1026 [ACK] Seq=1 Ack=1 Win=32352 Len=01216:40:35.739249192.168.31.44195.144.107.198TCP54[1031 + 21 [ACK] Seq=43 Ack=113 Win=513 Len=01416:40:35.75925195.144.107.198192.168.31.44FTP.2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)1516:40:35.75925192.168.31.44195.144.107.198TCP541084 + 1026 [ACK] Seq=1 Ack=2913 Win=4194304 Len=01616:40:35.822152195.144.107.198192.168.31.44FTP.2966 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)1716:40:35.822263192.168.31.44195.144.107.198TCP541084 + 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=01816:40:35.8383496195.144.107.198192.168.31.44FTP.1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)1916:40:35.8383496195.144.107.198192.168.31.44FTP.1510 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)1916:40:35.8383496195.144.107.198192.168.31.44FTP.1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)1916:40:35.8383496195.144.107.198192.168.31.44FTP.1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)2016:40:35.8383496195.144.107.198192.168.31.44FTP.1408 FTP Data: 1354 bytes (P	9 16:40:35.696788	195.144.107.198	192.168.31.44	FTP	96 Response: 150 Opening BINARY mode data connection.
12 16:40:35.698802 192.168.31.44195.144.107.198TCP54 [TCP Window Update] 1084 + 1026 [ACK] Seq=1 Ack=1 Win=4194304 Len=013 16:40:35.739249 192.168.31.44195.144.107.198TCP54 1031 + 21 [ACK] Seq=43 Ack=113 Win=513 Len=014 16:40:35.759825 195.144.107.198192.168.31.44FTP_2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)15 16:40:35.822152 195.144.107.198192.168.31.44FTP_5878 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)17 16:40:35.822263 192.168.31.44195.144.107.198TCP54 1084 + 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=018 16:40:35.883496 195.144.107.198192.168.31.44FTP_1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)19 16:40:35.883496 195.144.107.198192.168.31.44FTP_1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)19 16:40:35.883599 192.168.31.44195.144.107.198TCP54 1084 + 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=018 16:40:35.883599 192.168.31.44195.144.107.198TCP54 1084 + 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=021 16:40:35.944841 195.144.107.198192.168.31.44FTP1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)20 16:40:35.944841 195.144.107.198192.168.31.44FTP7B Response: 226 Transfer complete.22 16:40:35.944841 195.144.107.198192.168.31.44FTP7B Response: 226 Transfer complete.23 16:40:35.944841 195.144.107.198192.168.31.44FTP54 1026 + 1084 [F1N, ACK] Seq=1 Ack=11547 Ack=1 Win=66816 Len=023 16:40:35.944841 195.144.107.198195.144.107.198TCP	10 16:40:35.698384	195.144.107.198	192.168.31.44	TCP	66 1026 + 1084 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1456 WS=256 SAC
13 16:40:35.739249 192.168.31.44195.144.107.198TCP54 1031 + 21 [ACK] Seq=43 Ack=113 Win=513 Len=014 16:40:35.759825 195.144.107.198192.168.31.44FTP.2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)15 16:40:35.759925 192.168.31.44195.144.107.198TCP54 1084 + 1026 [ACK] Seq=1 Ack=2913 Win=4194304 Len=016 16:40:35.822152 195.144.107.198192.168.31.44FTP.5878 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)17 16:40:35.82263 192.168.31.44195.144.107.198TCP54 1084 + 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=018 16:40:35.883496 195.144.107.198192.168.31.44FTP.1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)19 16:40:35.883496 195.144.107.198192.168.31.44FTP.1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)19 16:40:35.88359 192.168.31.44195.144.107.198TCP54 1084 + 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=021 16:40:35.984841 195.144.107.198192.168.31.44FTP78 Response: 226 Transfer complete.22 16:40:35.944841 195.144.107.198192.168.31.44FTP78 Response: 226 Transfer complete.22 16:40:35.944841 195.144.107.198192.168.31.44FTP54 1026 + 1084 [FTN, ACK] Seq=11547 Ack=1 Win=66816 Len=023 16:40:35.944841 195.144.107.198192.168.31.44FCP54 1026 + 1084 [FTN, ACK] Seq=1 Ack=11547 Win=4194304 Len=023 16:40:35.944978 192.168.31.44195.144.107.198TCP54 1026 + 1084 [FTN, ACK] Seq=1 Ack=11548 Win=4194304 Len=023 16:40:35.944978 192.168.31.44195.144.107.198TCP54 1026 + 1084 [FTN,	11 16:40:35.698521	192.168.31.44	195.144.107.198	TCP	54 1084 + 1026 [ACK] Seq=1 Ack=1 Win=132352 Len=0
13 16:40:35.739249 192.168.31.44       195.144.107.198       TCP       54 1031 + 21 [ACK] Seq=43 Ack=113 Win=513 Len=0         14 16:40:35.759825 195.144.107.198       192.168.31.44       FTP       2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)         15 16:40:35.759925 192.168.31.44       195.144.107.198       TCP       54 1084 + 1026 [ACK] Seq=1 Ack=2913 Win=4194304 Len=0         16 16:40:35.822152 195.144.107.198       192.168.31.44       FTP       5878 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)         17 16:40:35.82263 192.168.31.44       195.144.107.198       TCP       54 1084 + 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0         18 16:40:35.883496 195.144.107.198       192.168.31.44       FTP       1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)         19 16:40:35.883496 195.144.107.198       192.168.31.44       FTP       1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)         19 16:40:35.883496 195.144.107.198       192.168.31.44       FTP       1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         20 16:40:35.883599 192.168.31.44       195.144.107.198       TCP       54 1084 + 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0         21 16:40:35.944841 195.144.107.198       192.168.31.44       FTP       1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         22 16:40:35.944841 195.144.107.198       192.168.31.44       FTP	12 16:40:35.698802	192.168.31.44	195.144.107.198	TCP	54 [TCP Window Update] 1084 + 1026 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
15       16:40:35.759925       192.168.31.44       195.144.107.198       TCP       54       1026       [ACK]       Seq=1       Ack=2913       Win=4194304       Len=0         16       16:40:35.822152       195.144.107.198       192.168.31.44       FTP       5878       FTP Data:       5824       bytes       (PASV)       (RETR ResumableTransfer.png)         17       16:40:35.822263       192.168.31.44       195.144.107.198       TCP       54       1084 → 1026       [ACK]       Seq=1       Ack=8737       Win=4194304       Len=0         18       16:40:35.883496       195.144.107.198       192.168.31.44       FTP       1510       FTP Data:       1456       bytes       (PASV)       (RETR ResumableTransfer.png)         19       16:40:35.883496       195.144.107.198       192.168.31.44       FTP       1408       FTP Data:       1354       bytes       (PASV)       (RETR ResumableTransfer.png)         20       16:40:35.883559       192.168.31.44       FTP       1408       FTP Data:       1354       bytes       (PASV)       (RETR ResumableTransfer.png)         20       16:40:35.944841       195.144.107.198       ICP       54       1084 → 1026       [ACK]       Seq=1       Ack=11547       Win=4194304	13 16:40:35.739249	192.168.31.44	195.144.107.198	TCP	54 1031 + 21 [ACK] Seg=43 Ack=113 Win=513 Len=0
16       16:40:35.822152       195.144.107.198       192.168.31.44       FTP       5878 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)         17       16:40:35.822263       192.168.31.44       195.144.107.198       TCP       54 1084 → 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0         18       16:40:35.883496       195.144.107.198       192.168.31.44       FTP       1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)         19       16:40:35.883496       195.144.107.198       192.168.31.44       FTP       1510 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         19       16:40:35.883559       192.168.31.44       FTP       1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         20       16:40:35.883559       192.168.31.44       FTP       1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         21       16:40:35.944841       195.144.107.198       192.168.31.44       FTP.       1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         21       16:40:35.944841       195.144.107.198       192.168.31.44       FTP.       78 Response: 226 Transfer complete.         22       16:40:35.944841       195.144.107.198       192.168.31.44       TCP       54 1026 + 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0         23       16:40:35.944978       192.168.31.44       TCP	14 16:40:35.759825	195.144.107.198	192.168.31.44	FTP_	2966 FTP Data: 2912 bytes (PASV) (RETR ResumableTransfer.png)
17 16:40:35.822263 192.168.31.44       195.144.107.198       TCP       54 1084 → 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0         18 16:40:35.883496 195.144.107.198       192.168.31.44       FTP       1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)         19 16:40:35.883496 195.144.107.198       192.168.31.44       FTP       1510 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         20 16:40:35.883559 192.168.31.44       195.144.107.198       TCP       54 1084 → 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0         21 16:40:35.944841 195.144.107.198       192.168.31.44       FTP       78 Response: 226 Transfer complete.         22 16:40:35.944841 195.144.107.198       192.168.31.44       TCP       54 1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0         23 16:40:35.944978 192.168.31.44       195.144.107.198       TCP       54 1026 → 1084 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0	15 16:40:35.759925	192.168.31.44	195.144.107.198	TCP	54 1084 -> 1026 [ACK] Seg=1 Ack=2913 Win=4194304 Len=0
17 16:40:35.822263 192.168.31.44       195.144.107.198       TCP       54 1084 → 1026 [ACK] Seq=1 Ack=8737 Win=4194304 Len=0         18 16:40:35.883496 195.144.107.198       192.168.31.44       FTP.       1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)         19 16:40:35.883496 195.144.107.198       192.168.31.44       FTP.       1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         20 16:40:35.883559 192.168.31.44       195.144.107.198       192.168.31.44       FTP.       1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         21 16:40:35.944841 195.144.107.198       192.168.31.44       FTP       78 Response: 226 Transfer complete.         22 16:40:35.944841 195.144.107.198       192.168.31.44       TCP       54 1026 + 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0         23 16:40:35.944978 192.168.31.44       195.144.107.198       TCP       54 1026 + 1084 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0	16 16:40:35.822152	195.144.107.198	192.168.31.44	FTP_	5878 FTP Data: 5824 bytes (PASV) (RETR ResumableTransfer.png)
19 16:40:35.883496 195.144,107.198       192.168.31.44       FTP       1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)         20 16:40:35.883559 192.168.31.44       195.144.107.198       TCP       54 1084 → 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0         21 16:40:35.944841 195.144.107.198       192.168.31.44       FTP       78 Response: 226 Transfer complete.         22 16:40:35.944841 195.144.107.198       192.168.31.44       TCP       54 1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0         23 16:40:35.944978 192.168.31.44       195.144.107.198       TCP       54 1026 → 1084 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0	17 16:40:35.822263	192.168.31.44	195.144.107.198	TCP	54 1084 + 1026 [ACK] Seg=1 Ack=8737 Win=4194304 Len=0
20 16:40:35.883559 192.168.31.44       195.144.107.198       TCP       54 1084 → 1026 [ACK] Seq=1 Ack=11547 Win=4194304 Len=0         21 16:40:35.944841 195.144.107.198       192.168.31.44       FTP       78 Response: 226 Transfer complete.         22 16:40:35.944841 195.144.107.198       192.168.31.44       TCP       54 1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0         23 16:40:35.944978 192.168.31.44       195.144.107.198       TCP       54 1026 → 1084 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0	18 16:40:35.883496	195.144.107.198	192.168.31.44	FTP.	1510 FTP Data: 1456 bytes (PASV) (RETR ResumableTransfer.png)
21 16:40:35.944841 195.144.107.198       192.168.31.44       FTP       78 Response: 226 Transfer complete.         22 16:40:35.944841 195.144.107.198       192.168.31.44       TCP       54 1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0         23 16:40:35.944978 192.168.31.44       195.144.107.198       TCP       54 1026 → 1084 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0	19 16:40:35.883496	195.144.107.198	192.168.31.44	FTP_	1408 FTP Data: 1354 bytes (PASV) (RETR ResumableTransfer.png)
22 16:40:35.944841 195.144.107.198 192.168.31.44 TCP 54 1026 → 1084 [FIN, ACK] Seq=11547 Ack=1 Win=66816 Len=0 23 16:40:35.944978 192.168.31.44 195.144.107.198 TCP 54 1084 → 1026 [ACK] Seq=1 Ack=11548 Win=4194304 Len=0	20 16:40:35.883559	192.168.31.44	195.144.107.198	TCP	54 1084 -> 1026 [ACK] Seg=1 Ack=11547 Win=4194304 Len=0
23 16:40:35.944978 192.168.31.44 195.144.107.198 TCP 54 1084 → 1026 [ACK] Seg=1 Ack=11548 Win=4194304 Len=0	21 16:40:35.944841	195.144.107.198	192.168.31.44	ETP	78 Response: 226 Transfer complete.
	22 16:40:35.944841	195.144.107.198	192.168.31.44	TCP	54 1026 + 1084 [FIN, ACK] Seg=11547 Ack=1 Win=66816 Len=0
24 16:48:35.945371 192.168.31.44 195.144.107.198 TCP 54 1084 jm 1026 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0	23 16:40:35.944978	192.168.31.44	195.144.107.198	TCP	54 1084 - 1026 [ACK] Seg=1 Ack=11548 Win=4194304 Len=0
0	24 16:40:35.945371	192.168.31.44	195.144.107.198	TCP	54 1084 [m 1026 [FIN, ACK] Seq=1 Ack=11548 Win=4194304 Len=0

Which frame numbers contain a file that is extractable via TCP stream within Wireshark?

A. 7,14, and 21 B. 7 and 21 C. 14,16,18, and 19 D. 7 to 21

Answer: B

#### **NEW QUESTION 26**

Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web application?

A. Hypertext Transfer Protocol **B. SSL Certificate** C. Tunneling D. VPN



Answer: B

# **NEW QUESTION 27**

.....



# **Thank You for Trying Our Product**

# We offer two products:

- 1st We have Practice Tests Software with Actual Exam Questions
- 2nd Questons and Answers in PDF Format

# 200-201 Practice Exam Features:

- \* 200-201 Questions and Answers Updated Frequently
- \* 200-201 Practice Questions Verified by Expert Senior Certified Staff
- \* 200-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 200-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click Order The 200-201 Practice Test Here