

Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals



NEW QUESTION 1

During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

- A. examination
- B. investigation
- C. collection
- D. reporting

Answer: C

NEW QUESTION 2

Which two elements are assets in the role of attribution in an investigation? (Choose two.)

- A. context
- B. session
- C. laptop
- D. firewall logs
- E. threat actor

Answer: AE

NEW QUESTION 3

Refer to the exhibit.

Interface: 192.168.1.29 --- 0x11		
Internet Address	Physical Address	Type
192.168.1.10	d8-a7-56-d7-19-ea	dynamic
192.168.1.67	d8-a7-56-d7-19-ea	dynamic
192.168.1.1	01-00-5e-00-00-16	static

What is occurring in this network?

- A. ARP cache poisoning
- B. DNS cache poisoning
- C. MAC address table overflow
- D. MAC flooding attack

Answer: A

NEW QUESTION 4

An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)

- A. signatures
- B. host IP addresses
- C. file size
- D. dropped files
- E. domain names

Answer: BE

NEW QUESTION 5

What is a benefit of agent-based protection when compared to agentless protection?

- A. It lowers maintenance costs
- B. It provides a centralized platform
- C. It collects and detects all traffic locally
- D. It manages numerous devices simultaneously

Answer: B

NEW QUESTION 6

What is the difference between statistical detection and rule-based detection models?

- A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
- B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
- C. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
- D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis

Answer: B

NEW QUESTION 7

Which process is used when IPS events are removed to improve data integrity?

- A. data availability
- B. data normalization
- C. data signature
- D. data protection

Answer: B

NEW QUESTION 8

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

tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

NEW QUESTION 9

What is the function of a command and control server?

- A. It enumerates open ports on a network device
- B. It drops secondary payload into malware
- C. It is used to regain control of the network after a compromise
- D. It sends instruction to a compromised system

Answer: D

NEW QUESTION 10

Refer to the exhibit.

```
GET /item.php?id=34' or sleep(10)
```

This request was sent to a web application server driven by a database. Which type of web server attack is represented?

- A. parameter manipulation
- B. heap memory corruption
- C. command injection
- D. blind SQL injection

Answer: D

NEW QUESTION 10

Which attack method intercepts traffic on a switched network?

- A. denial of service
- B. ARP cache poisoning
- C. DHCP snooping
- D. command and control

Answer: C

NEW QUESTION 14

What specific type of analysis is assigning values to the scenario to see expected outcomes?

- A. deterministic
- B. exploratory
- C. probabilistic
- D. descriptive

Answer: A

NEW QUESTION 15

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 server

Answer: B

NEW QUESTION 19

What is the practice of giving an employee access to only the resources needed to accomplish their job?

- A. principle of least privilege
- B. organizational separation
- C. separation of duties
- D. need to know principle

Answer: A

NEW QUESTION 20

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
18	0.011918	10.0.2.15	192.124.249.9	TCP	78	50588→443 [SYN] Seq=1
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443→50588 [SYN, ACK]
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588→443 [ACK] Seq=1
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443→50586 [SYN, ACK]
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586→443 [ACK] Seq=1
23	0.023212	10.0.2.15	192.124.249.9	TCP	261	50588→443 [PSH, ACK]
24	0.023373	10.0.2.15	192.124.249.9	TCP	261	50586→443 [PSH, ACK]
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443→50588 [ACK] Seq=1
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443→50586 [ACK] Seq=1
27	0.037413	192.124.249.9	10.0.2.15	TCP	2792	443→50586 [PSH, ACK]
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586→443 [ACK] Seq=2

> Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)

> Linux cooked capture

> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)

> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A

> Data [205 bytes]

Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...

[Length: 205]

0000	00 04 00 01 00 06 08 00	27 7a 3c 93 00 00 08 00 *z<.....
0010	45 00 00 f5 48 7b 40 00	40 06 2b f3 0a 00 02 0f	E...H{@. @.+.....
0020	c0 7c f9 09 c5 9a 01 bb	0e 1f dc b4 00 b4 aa 02
0030	50 18 72 10 c6 7c 00 00	16 03 01 00 c8 01 00 00	P.r.. ..
0040	c4 03 03 0e 06 ea d0 78	d1 76 76 c1 3a b4 6e bfx.vv.:n..
0050	e6 b8 b8 b2 ba 08 d6 6d	0d 38 fb 91 45 de fc eem .8..E...
0060	8b 6e f8 00 00 1e c0 2b	c0 2f cc a9 cc a8 c0 2c	.n.....+ ./.....
0070	c0 30 c0 0a c0 09 c0 13	c0 14 00 33 00 39 00 2f	.0..... ...3.9./
0080	00 35 00 0a 01 00 00 7d	00 00 00 16 00 14 00 00	.5.....}
0090	11 77 77 77 2e 6c 69 6e	75 78 6d 69 6e 74 2e 63	.wwwlin uxmint.c
00a0	6f 6d 00 17 00 00 ff 01	00 01 00 00 0a 00 08 00	om.....
00b0	06 00 17 00 18 00 19 00	0b 00 02 01 00 00 23 00#.
00c0	00 33 74 00 00 00 10 00	17 00 15 02 68 32 08 73	.3t.....h2.s
00d0	70 64 79 2f 33 2e 31 08	68 74 74 70 2f 31 2e 31	pdv/3.1. http/1.1
00e0	00 05 00 05 01 00 00 00	00 00 0d 00 18 00 16 04
00f0	01 05 01 06 01 02 01 04	03 05 03 06 03 02 03 05
0100	02 04 02 02 02	

Which application protocol is in this PCAP file?

- A. SSH
- B. TCP
- C. TLS
- D. HTTP

Answer: B

NEW QUESTION 21

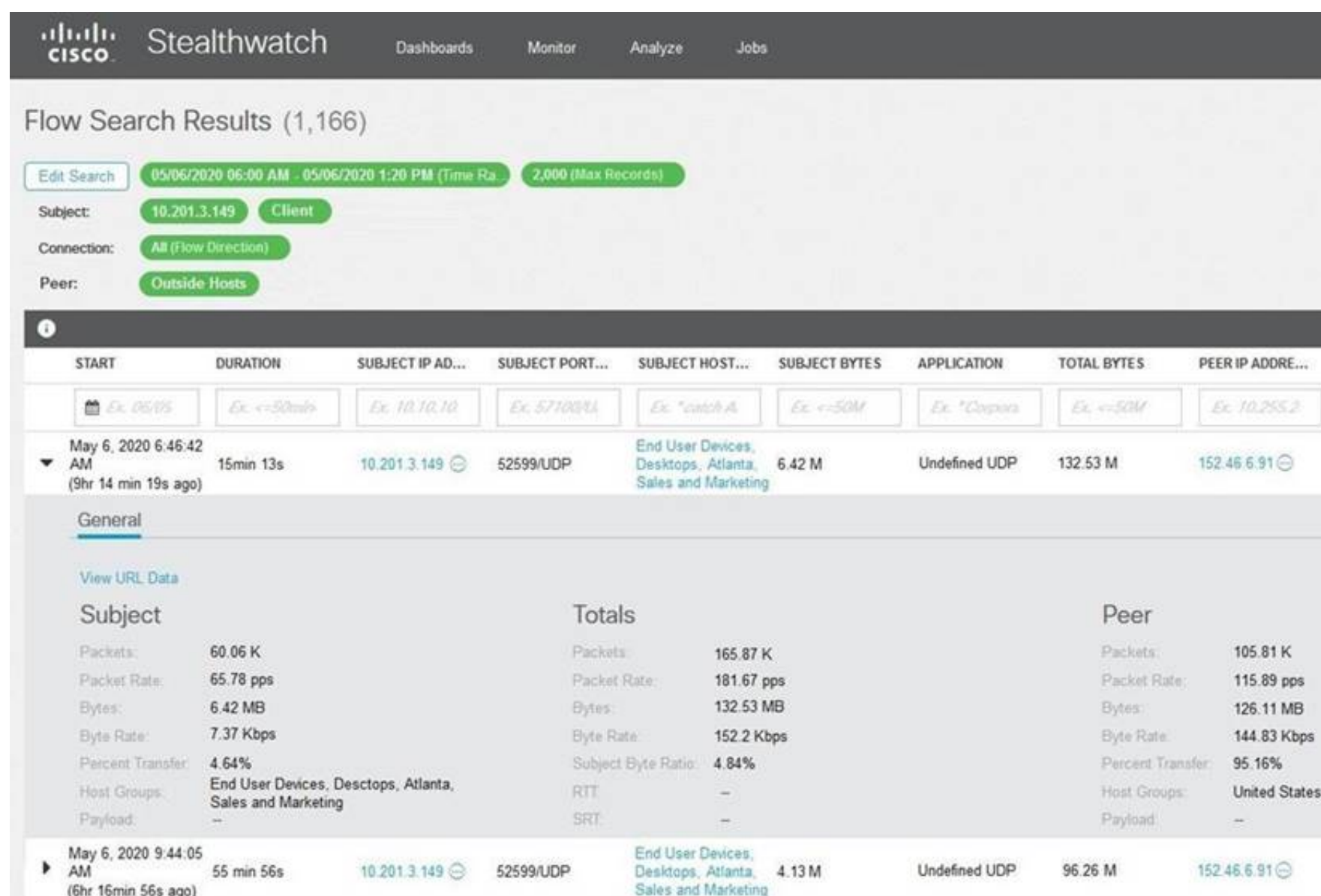
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

- A. Tapping interrogation replicates signals to a separate port for analyzing traffic
- B. Tapping interrogations detect and block malicious traffic
- C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
- D. Inline interrogation detects malicious traffic but does not block the traffic

Answer: A

NEW QUESTION 23

Refer to the exhibit.



Stealthwatch Dashboards Monitor Analyze Jobs

Flow Search Results (1,166)

Edit Search 05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Ra) 2,000 (Max Records)

Subject: 10.201.3.149 Client

Connection: All (Flow Direction)

Peer: Outside Hosts

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDRE...
May 6, 2020 6:46:42 AM (9hr 14 min 19s ago)	15min 13s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	6.42 M	Undefined UDP	132.53 M	152.46.6.91

General

View URL Data

Subject	Totals	Peer
Packets: 60.06 K	Packets: 165.87 K	Packets: 105.81 K
Packet Rate: 65.78 pps	Packet Rate: 181.67 pps	Packet Rate: 115.89 pps
Bytes: 6.42 MB	Bytes: 132.53 MB	Bytes: 126.11 MB
Byte Rate: 7.37 Kbps	Byte Rate: 152.2 Kbps	Byte Rate: 144.83 Kbps
Percent Transfer: 4.64%	Subject Byte Ratio: 4.84%	Percent Transfer: 95.16%
Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing	RTT: -	Host Groups: United States
Payload: -	SRT: -	Payload: -

May 6, 2020 9:44:05 AM (6hr 16min 56s ago)	55 min 56s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	4.13 M	Undefined UDP	96.26 M	152.46.6.91
---	------------	--------------	-----------	--	--------	---------------	---------	-------------

What is the potential threat identified in this Stealthwatch dashboard?

- A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
- B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
- C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
- D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

Answer: D

NEW QUESTION 26

What are the two characteristics of the full packet captures? (Choose two.)

- A. Identifying network loops and collision domains.
- B. Troubleshooting the cause of security and performance issues.
- C. Reassembling fragmented traffic from raw data.
- D. Detecting common hardware faults and identify faulty assets.
- E. Providing a historical record of a network transaction.

Answer: CE

NEW QUESTION 27

Which step in the incident response process researches an attacking host through logs in a SIEM?

- A. detection and analysis
- B. preparation
- C. eradication
- D. containment

Answer: A

NEW QUESTION 30

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 link 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

NEW QUESTION 35

Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

- A. resource exhaustion
- B. tunneling
- C. traffic fragmentation
- D. timing attack

Answer: A

NEW QUESTION 36

A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

- A. reconnaissance
- B. action on objectives
- C. installation
- D. exploitation

Answer: C

NEW QUESTION 37

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

- A. destination IP address
- B. TCP ACK
- C. HTTP status code
- D. URI

Answer: D

NEW QUESTION 41

What do the Security Intelligence Events within the FMC allow an administrator to do?

- A. See if a host is connecting to a known-bad domain.
- B. Check for host-to-server traffic within your network.
- C. View any malicious files that a host has downloaded.
- D. Verify host-to-host traffic within your network.

Answer: A

NEW QUESTION 46

What makes HTTPS traffic difficult to monitor?

- A. SSL interception
- B. packet header size
- C. signature detection time
- D. encryption

Answer: D

NEW QUESTION 50

Refer to the exhibit.

Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

Which type of log is displayed?

- A. IDS
- B. proxy
- C. NetFlow
- D. sys

Answer: D

NEW QUESTION 52

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot
- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

Answer: AD

NEW QUESTION 53

What is an attack surface as compared to a vulnerability?

- A. any potential danger to an asset
- B. the sum of all paths for data into and out of the application
- C. an exploitable weakness in a system or its design
- D. the individuals who perform an attack

Answer: B

NEW QUESTION 56

What does cyber attribution identify in an investigation?

- A. exploit of an attack
- B. threat actors of an attack
- C. vulnerabilities exploited
- D. cause of an attack

Answer: B

NEW QUESTION 58

What is the difference between an attack vector and attack surface?

- A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vector identifies vulnerabilities that are independent of user actions.
- B. An attack vector identifies components that can be exploited; and an attack surface identifies the potential path an attack can take to penetrate the network.
- C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.
- D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

Answer: C

NEW QUESTION 62

Which HTTP header field is used in forensics to identify the type of browser used?

- A. referrer
- B. host
- C. user-agent
- D. accept-language

Answer: C

NEW QUESTION 63

Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 66

Which security technology allows only a set of pre-approved applications to run on a system?

- A. application-level blacklisting
- B. host-based IPS
- C. application-level whitelisting
- D. antivirus

Answer: C

NEW QUESTION 70

A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?

- A. application identification number
- B. active process identification number
- C. runtime identification number
- D. process identification number

Answer: D

NEW QUESTION 74

A system administrator is ensuring that specific registry information is accurate.
Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

- A. file extension associations
- B. hardware, software, and security settings for the system
- C. currently logged in users, including folders and control panel settings
- D. all users on the system, including visual settings

Answer: B

NEW QUESTION 75

What is an example of social engineering attacks?

- A. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company
- B. receiving an email from human resources requesting a visit to their secure website to update contact information
- C. sending a verbal request to an administrator who knows how to change an account password
- D. receiving an invitation to the department's weekly WebEx meeting

Answer: B

NEW QUESTION 78

An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

- A. sequence numbers
- B. IP identifier
- C. 5-tuple
- D. timestamps

Answer: C

NEW QUESTION 82

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

- A. destination IP address
- B. URI
- C. HTTP status code
- D. TCP ACK

Answer: B

NEW QUESTION 83

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.011641	10.0.2.15	192.124.249.9	TCP	76	50586-443 [SYN] Seq=0 Win=
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588-443 [SYN] Seq=0 Win=
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK] Seq=0
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1 Ack=
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1 Ack=
23	0.023212	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1 Ack=
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1 Ack=
27	0.037413	192.124.249.9	10.0.2.15	TLSv1.2	2792	Server Hello
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=206 Ac

> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
 > Linux cooked capture
 > Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
 > Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
 > Secure Sockets Layer

0000	00 04 00 01 00 06 08 00	27 7a 3c 93 00 00 08 00 *z<.....
0010	45 00 00 f5 eb 3e 40 00	40 06 89 2f 0a 00 02 0f	E....>@. @../....
0020	c0 7c f9 09 c5 9c 01 bb	4d db 7f f7 00 b3 b0 02 M.....
0030	50 18 72 10 c6 7c 00 00	16 03 01 00 c8 01 00 00	P.r..
0040	c4 03 03 d1 08 45 78 b7	2c 90 04 ee 51 16 f1 82Ex.0...
0050	16 43 ec d4 89 60 34 4a	7b 80 a6 d1 72 d5 11 87	.C....4J {...r...
0060	10 57 cc 00 00 1e c0 2b	c0 2f cc a9 cc a8 c0 2c	.W.....+ ./.....
0070	c0 30 c0 0a c0 09 c0 13	c0 14 00 33 00 39 00 2f	.0..... ...3.9./
0080	00 35 00 0a 01 00 00 7d	00 00 00 16 00 14 00 00	.5.....}
0090	11 77 77 77 2e 6c 69 6e	75 78 6d 69 6e 74 2e 63	.wwwlin uxmint.c
00a0	6f 6d 00 17 00 00 ff 01	00 01 00 00 0a 00 08 00	om.....
00b0	06 00 17 00 18 00 19 00	0b 00 02 01 00 00 23 00
00c0	00 33 74 00 00 00 10 00	17 00 15 02 68 32 08 73	.3t.....h2.s
00d0	70 64 79 2f 33 2e 31 08	68 74 74 70 2f 31 2e 31	pdy/3.2. http/1.1
00e0	00 05 00 05 01 00 00 00	00 00 0d 00 18 00 16 04
00f0	01 05 01 06 01 02 01 04	03 05 03 06 03 02 03 05
0100	02 04 02 02 02	

Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 87

What does cyber attribution identify in an investigation?

- A. cause of an attack
- B. exploit of an attack
- C. vulnerabilities exploited
- D. threat actors of an attack

Answer: D

NEW QUESTION 92

What are two social engineering techniques? (Choose two.)

- A. privilege escalation
- B. DDoS attack
- C. phishing
- D. man-in-the-middle
- E. pharming

Answer: CE

NEW QUESTION 96

How does an attacker observe network traffic exchanged between two users?

- A. port scanning
- B. man-in-the-middle
- C. command injection
- D. denial of service

Answer: B

NEW QUESTION 101

Which two compliance frameworks require that data be encrypted when it is transmitted over a public network? (Choose two.)

- A. PCI
- B. GLBA
- C. HIPAA
- D. SOX
- E. COBIT

Answer: AC

NEW QUESTION 106

What is a difference between SOAR and SIEM?

- A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not
- B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not
- C. SOAR receives information from a single platform and delivers it to a SIEM
- D. SIEM receives information from a single platform and delivers it to a SOAR

Answer: A

NEW QUESTION 109

Which action prevents buffer overflow attacks?

- A. variable randomization
- B. using web based applications
- C. input sanitization
- D. using a Linux operating system

Answer: C

NEW QUESTION 113

Which IETF standard technology is useful to detect and analyze a potential security incident by recording session flows that occurs between hosts?

- A. SFlow
- B. NetFlow
- C. NFlow
- D. IPFIX

Answer: D

NEW QUESTION 114

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan
- C. internet exposed devices
- D. single factor authentication

Answer: D

NEW QUESTION 117

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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 First Try
- * 200-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 200-201 Practice Test Here](#)