

**200-201.exam-labs.premium.exam.98q**

Number: 200-201  
Passing Score: 800  
Time Limit: 120 min  
File Version: 1.0

**ExamLabs**

**200-201**

**Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)**

**Version 1.0**

## **Exam A**

### **QUESTION 1**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 2**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 3**

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 4**

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

**QUESTION 5**

Which utility blocks a host portscan?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 6**

Which event is user interaction?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 8

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

Refer to the exhibit. What information is depicted?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 9

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 10

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

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 11**

Which regular expression matches "color" and "colour"?

- A. colo?ur
- B. col[0-8]+our
- C. colou?r
- D. col[0-9]+our

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 12**

A user received a malicious attachment but did not run it.

Which category classifies the intrusion?

- A. weaponization
- B. reconnaissance
- C. installation
- D. delivery

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 13**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

An investigator is examining a copy of an ISO file that is stored in CDFS format.

What type of evidence is this file?

- A. data from a CD copied using Mac-based system
- B. data from a CD copied using Linux system
- C. data from a DVD copied using Windows system
- D. data from a CD copied using Windows

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 15**

Which piece of information is needed for attribution in an investigation?

- A. proxy logs showing the source RFC 1918 IP addresses
- B. RDP allowed from the Internet
- C. known threat actor behavior
- D. 802.1x RADIUS authentication pass and fail logs

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 16**

```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;  
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1  
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from  
127.0.0.1 port 38346 ssh2
```

Refer to the exhibit. In which Linux log file is this output found?

- A. /var/log/authorization.log
- B. /var/log/dmesg
- C. var/log/var.log
- D. /var/log/auth.log

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 17**

What is the difference between the ACK flag and the RST flag in the NetFlow log session?

- A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete
- B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
- C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
- D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 19**

Date	Flow Start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2020-01-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→	192.168.0.1:20521	1	82	1

Refer to the exhibit. Which type of log is displayed?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 21**

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

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

An analyst discovers that a legitimate security alert has been dismissed.

Which signature caused this impact on network traffic?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

DRAG DROP

Drag and drop the security concept on the left onto the example of that concept on the right.

**Select and Place:**



Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

**Correct Answer:**

Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 24**

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 25**

Which security principle requires more than one person is required to perform a critical task?

- A. least privilege
- B. need to know
- C. separation of duties
- D. due diligence

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 26**

What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)

- A. Untampered images are used in the security investigation process
- B. Tampered images are used in the security investigation process
- C. The image is tampered if the stored hash and the computed hash match
- D. Tampered images are used in the incident recovery process
- E. The image is untampered if the stored hash and the computed hash match

**Correct Answer: BE**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

What makes HTTPS traffic difficult to monitor?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 28**

DRAG DROP

```
> 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
```

**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 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

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 29**

```

File      Actions      Edit      View      Help

  48 41.270348133 185.199.111.153 → 192.168.88.164 TLSv1.2 123 Application Data
  49 41.270348165 185.199.111.153 → 192.168.88.164 TLSv1.2 104 Application Data
  50 41.270356290 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
  51 41.270369874 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
  52 41.270430171 192.168.88.164 → 185.199.111.153 TLSv1.2 104 Application Data
  53 41.271767772 185.199.111.153 → 192.168.88.164 TLSv1.2 2854 Application Data
  54 41.271767817 185.199.111.153 → 192.168.88.164 TLSv1.2 904 Application Data
  55 41.271788996 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849
  56 41.271973293 192.168.88.164 → 185.199.111.153 TLSv1.2 97 Encrypted Alert
  57 41.272411701 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [FIN, ACK]
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849
  58 41.283301751 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
  59 41.283301808 185.199.111.153 → 192.168.88.164 TLSv1.2 97 Encrypted Alert
  60 41.283321947 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
  61 41.283939151 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [FIN, ACK]
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
  62 41.283945760 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
  63 41.284635561 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759
  64 41.284642324 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=904 Win=0 Len=0

```

An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture the analyst cannot determine the technique and payload used for the communication.

Which obfuscation technique is the attacker using?

- A. Base64 encoding
- B. transport layer security encryption
- C. SHA-256 hashing
- D. ROT13 encryption

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 30

Which artifact is used to uniquely identify a detected file?

- A. file timestamp
- B. file extension
- C. file size
- D. file hash

**Correct Answer: D**

**Section: (none)**

### Explanation

### Explanation/Reference:

#### QUESTION 31

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

**Correct Answer:** B

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 32

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

Refer to the exhibit. Which event is occurring?

- A. A binary named "submit" is running on VM cuckoo1.
- B. A binary is being submitted to run on VM cuckoo1
- C. A binary on VM cuckoo1 is being submitted for evaluation
- D. A URL is being evaluated to see if it has a malicious binary

**Correct Answer:** C

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 33

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

**Correct Answer:** B

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 34

Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

- A. decision making
- B. rapid response
- C. data mining
- D. due diligence

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 35

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

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 36

An analyst is exploring the functionality of different operating systems.

What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

- A. queries Linux devices that have Microsoft Services for Linux installed
- B. deploys Windows Operating Systems in an automated fashion
- C. is an efficient tool for working with Active Directory
- D. has a Common Information Model, which describes installed hardware and software

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 37

One of the objectives of information security is to protect the CIA of information and systems.

What does CIA mean in this context?

- A. confidentiality, identity, and authorization
- B. confidentiality, integrity, and authorization
- C. confidentiality, identity, and availability
- D. confidentiality, integrity, and availability

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 38**

What is rule-based detection when compared to statistical detection?

- A. proof of a user's identity
- B. proof of a user's action
- C. likelihood of user's action
- D. falsification of a user's identity

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 39**

What is personally identifiable information that must be safeguarded from unauthorized access?

- A. date of birth
- B. driver's license number
- C. gender
- D. zip code

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 40**

How does an SSL certificate impact security between the client and the server?

- A. by enabling an authenticated channel between the client and the server
- B. by creating an integrated channel between the client and the server
- C. by enabling an authorized channel between the client and the server
- D. by creating an encrypted channel between the client and the server

**Correct Answer:** D

**Section:** (none)

**Explanation**



**Explanation/Reference:**

**QUESTION 41**

Which type of data consists of connection level, application-specific records generated from network traffic?

- A. transaction data
- B. location data
- C. statistical data
- D. alert data

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 42**

At which layer is deep packet inspection investigated on a firewall?

- A. internet
- B. transport
- C. application
- D. data link

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

- A. NetScout
- B. tcpdump
- C. SolarWinds
- D. netsh

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

DRAG DROP

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

**Select and Place:**

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

**Correct Answer:**

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 45

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.

What is the initial event called in the NIST SP800-61?

- A. online assault
- B. precursor
- C. trigger
- D. instigator

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 46

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

## Explanation/Reference:

### QUESTION 47

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 48

No.	Time	Source	Destination	Protocol	Length	Info
18	0.011910	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 bf	.....x.vv.:n..
0050	e6 b8 b8 b2 ba 08 d6 6d	0d 38 fb 91 45 de fc ee	.....m .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	pdy/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		.....

Refer to the exhibit. Which application protocol is in this PCAP file?

- A. SSH

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


**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 49

<ul style="list-style-type: none"><li>SPRT</li><li>SRVLOC</li><li>SSCOP</li><li>SSH</li><li>SSL</li><li>STANAG 5066</li><li>StarTeam</li><li>STP</li><li>SUA</li><li>SYNCHROPHASOR</li><li>T.38</li><li>TACACS+</li><li>TALI</li><li>TCAP</li><li><b>TCP</b></li><li>TCPENCAP</li><li>TDMoE</li></ul>	<p>Show TCP summary in protocol tree: <input checked="" type="checkbox"/></p> <p>Validate the TCP checksum if possible: <input type="checkbox"/></p> <p>Allow subdissector to reassemble TCP streams: <input checked="" type="checkbox"/> </p> <p>Analyze TCP sequence numbers: <input checked="" type="checkbox"/></p> <p>Relative sequence numbers: <input checked="" type="checkbox"/></p> <p>Scaling factor to use when not available from capture: <input type="text" value="Not known"/></p> <p>Track number of bytes in flight: <input checked="" type="checkbox"/></p> <p>Calculate conversation timestamps: <input type="checkbox"/></p> <p>Try heuristic sub-dissectors first: <input type="checkbox"/></p> <p>Ignore TCP Timestamps in summary: <input type="checkbox"/></p> <p>Do not call subdissectors for error packets: <input type="checkbox"/></p> <p>TCP Experimental Options with a Magic Number: <input checked="" type="checkbox"/></p>
---	--

Refer to the exhibit. What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?

- A. insert TCP subdissectors
- B. extract a file from a packet capture
- C. disable TCP streams
- D. unfragment TCP

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 50

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:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 51**

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 52**

Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

- A. CSIRT
- B. PSIRT
- C. public affairs
- D. management

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 53**

An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network.

What is the impact of this traffic?

- A. ransomware communicating after infection
- B. users downloading copyrighted content
- C. data exfiltration
- D. user circumvention of the firewall

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 54**

How is attacking a vulnerability categorized?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 55**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 56**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 57**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 58**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 59**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 60**

Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

- A. forgery attack
- B. plaintext-only attack
- C. ciphertext-only attack
- D. meet-in-the-middle attack

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 61**

What causes events on a Windows system to show Event Code 4625 in the log messages?

- A. The system detected an XSS attack
- B. Someone is trying a brute force attack on the network
- C. Another device is gaining root access to the system
- D. A privileged user successfully logged into the system

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 62**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 63**

```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

Refer to the exhibit. What does the message indicate?

- A. an access attempt was made from the Mosaic web browser
- B. a successful access attempt was made to retrieve the password file
- C. a successful access attempt was made to retrieve the root of the website
- D. a denied access attempt was made to retrieve the password file

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 64**

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



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

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 65

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp     Postfix smtpd
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd
Service Info: Host: 172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Refer to the exhibit. What does the output indicate about the server with the IP address 172.18.104.139?

- A. open ports of a web server
- B. open port of an FTP server
- C. open ports of an email server
- D. running processes of the server

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 66

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

Refer to the exhibit. 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

- A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator
- B. MAC is the strictest of all levels of control and DAC is object-based access
- C. DAC is controlled by the operating system and MAC is controlled by an administrator
- D. DAC is the strictest of all levels of control and MAC is object-based access

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

A malicious file has been identified in a sandbox analysis tool.

Which piece of information is needed to search for additional downloads of this file by other hosts?

- A. file type
- B. file size
- C. file name
- D. file hash value

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 70**

Which attack method intercepts traffic on a switched network?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 71**

Which two elements are used for profiling a network? (Choose two.)

- A. session duration
- B. total throughput
- C. running processes
- D. listening ports
- E. OS fingerprint

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 72**

What does an attacker use to determine which network ports are listening on a potential target device?

- A. man-in-the-middle
- B. port scanning
- C. SQL injection
- D. ping sweep

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 73**

What is a purpose of a vulnerability management framework?

- A. identifies, removes, and mitigates system vulnerabilities
- B. detects and removes vulnerabilities in source code
- C. conducts vulnerability scans on the network
- D. manages a list of reported vulnerabilities

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 74

<IMG SRC=j%41vascript:alert('attack')>

Refer to the exhibit. Which kind of attack method is depicted in this string?

- A. cross-site scripting
- B. man-in-the-middle
- C. SQL injection
- D. denial of service

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 75

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522->80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpametag.gif?js=1&ts=147629607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522->80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?

- A. 2317
- B. 1986
- C. 2318
- D. 2542

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 76

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 77**

How is NetFlow different than 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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 78**

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

- A. least privilege
- B. need to know
- C. integrity validation
- D. due diligence

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 79**

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 80**

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

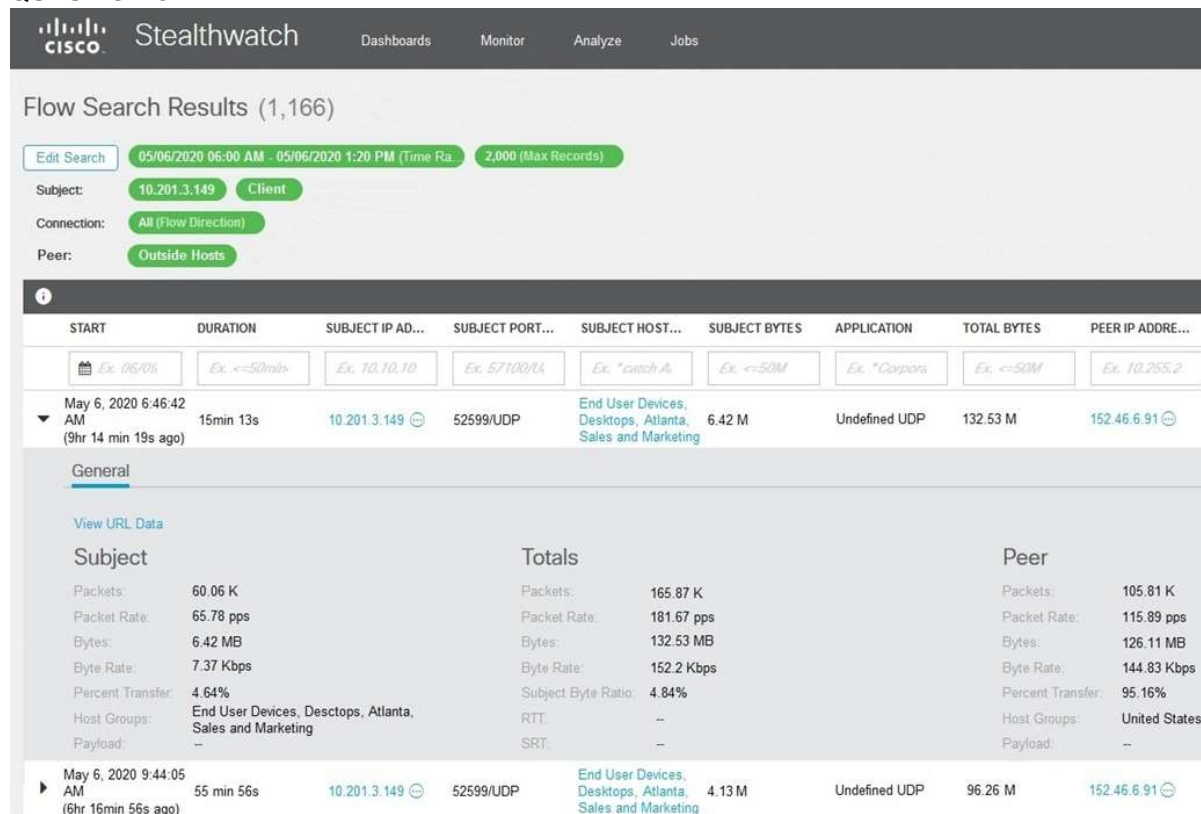
**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

## QUESTION 81



The screenshot shows the Cisco Stealthwatch interface. At the top, there's a navigation bar with 'Dashboards', 'Monitor', 'Analyze', and 'Jobs'. Below this, the 'Flow Search Results' section shows 1,166 results. The search filters are: Subject: 10.201.3.149 (Client), Connection: All (Flow Direction), and Peer: Outside Hosts. The search criteria are set to 05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Range) and 2,000 (Max Records).

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADRE...
May 6, 2020 6:46:42 AM (9hr 14min 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

Below the table, there's a 'General' tab with a 'View URL Data' link. The 'Subject' section shows statistics for 10.201.3.149: Packets: 60.06 K, Packet Rate: 65.78 pps, Bytes: 6.42 MB, Byte Rate: 7.37 Kbps, Percent Transfer: 4.64%, Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing, and Payload: --. The 'Totals' section shows: Packets: 165.87 K, Packet Rate: 181.67 pps, Bytes: 132.53 MB, Byte Rate: 152.2 Kbps, Subject Byte Ratio: 4.84%, RTT: --, and SRT: --. The 'Peer' section shows statistics for 152.46.6.91: Packets: 105.81 K, Packet Rate: 115.89 pps, Bytes: 126.11 MB, Byte Rate: 144.83 Kbps, Percent Transfer: 95.16%, Host Groups: United States, and Payload: --.

Refer to the exhibit. 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.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 82**

A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs.

Which technology should be used to accomplish this task?

- A. application whitelisting/blacklisting
- B. network NGFW
- C. host-based IDS
- D. antivirus/antispyware software

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 83**

What is the virtual address space for a Windows process?

- A. physical location of an object in memory
- B. set of pages that reside in the physical memory
- C. system-level memory protection feature built into the operating system
- D. set of virtual memory addresses that can be used

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 84**

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 86**

Which category relates to improper use or disclosure of PII data?

- A. legal
- B. compliance
- C. regulated
- D. contractual

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 87**

Which regex matches only on all lowercase letters?

- A. [a-z]+
- B. [^a-z]+
- C. a-z+
- D. a\*z+

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 88**

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

- A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
- B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 89**



An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise.

Which kind of evidence is this IP address?

- A. best evidence
- B. corroborative evidence
- C. indirect evidence
- D. forensic evidence

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 90

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 91

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	*

Refer to the exhibit. Which type of log is displayed?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 92

Overview

Analysis

Policies

Devices

Objects

Content Explorer

Connections > Security Intelligence Events

Intrusions

Files

Hosts

Users

Vulnerabilities

Correlation

Custom

Search

Health

System

Help

Security Intelligence Events

(switch workflow)

Bookmark This Page

Report Designer

Dashboard

View Bookmarks

Security Intelligence with Application Details > Table View of Security Intelligence Events

2018-03-02 07:20:20 - 2018-03-07 13:47:20

Search Constraints

Edit Search

Serve Search

Expanding

Disabled Columns

Jump to...

<div><div></div></div>	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ICMP Type
<div><div></div></div>	2018-03-07 13:42:01		Sinkhole DNS Block		10.0.10.75		JERI LABORDE (DCLOUD-SOC-LOAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
<div><div></div></div>	2018-03-07 13:42:01		Sinkhole DNS Block		10.0.0.100		AMPARO GIVENS (DCLOUD-SOC-LOAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
<div><div></div></div>	2018-03-07 13:42:01		Sinkhole DNS Block		10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC-LOAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

<<

Page 1

of 1 >>

Displaying rows 1-3 of 3 rows

View

Delete

View All

Delete All

Refer to the exhibit. Which two elements in the table are parts of the 5-tuple? (Choose two.)

- A. First Packet
- B. Initiator User
- C. Ingress Security Zone
- D. Source Port
- E. Initiator IP

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 93

Which security principle is violated by running all processes as root or administrator?

- A. principle of least privilege
- B. role-based access control
- C. separation of duties
- D. trusted computing base

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 94

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

What is the difference between deep packet inspection and stateful inspection?

- A. Deep packet inspection is more secure than stateful inspection on Layer 4
- B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
- C. Stateful inspection is more secure than deep packet inspection on Layer 7
- D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 96**

Which evasion technique is a function of ransomware?

- A. extended sleep calls
- B. encryption
- C. resource exhaustion
- D. encoding

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 97**

DRAG DROP

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

**Select and Place:**

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

**Correct Answer:**

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

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 98**

What does cyber attribution identity in an investigation?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**