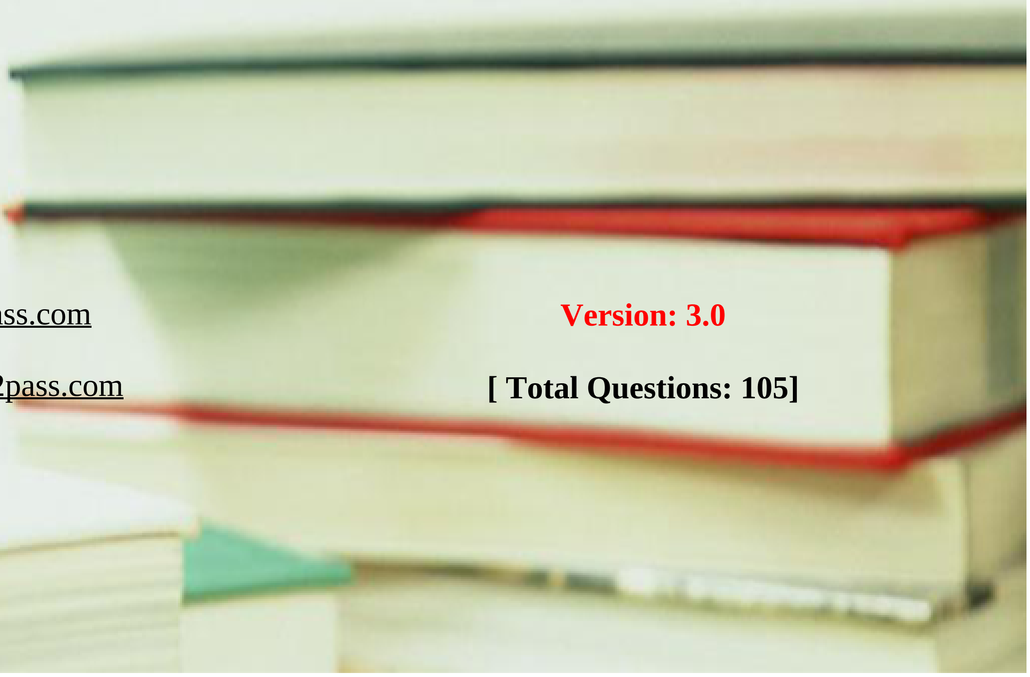
Solution 2Pass

Cisco

200-201

Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS)



Web: www.solution2pass.com

Email: support@solution2pass.com

Version: 3.0

[Total Questions: 105]

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@solution2pass.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@solution2pass.com and our technical experts will provide support within 24 hours.

Copyright

Question #:1

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: B E

Question #:2

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

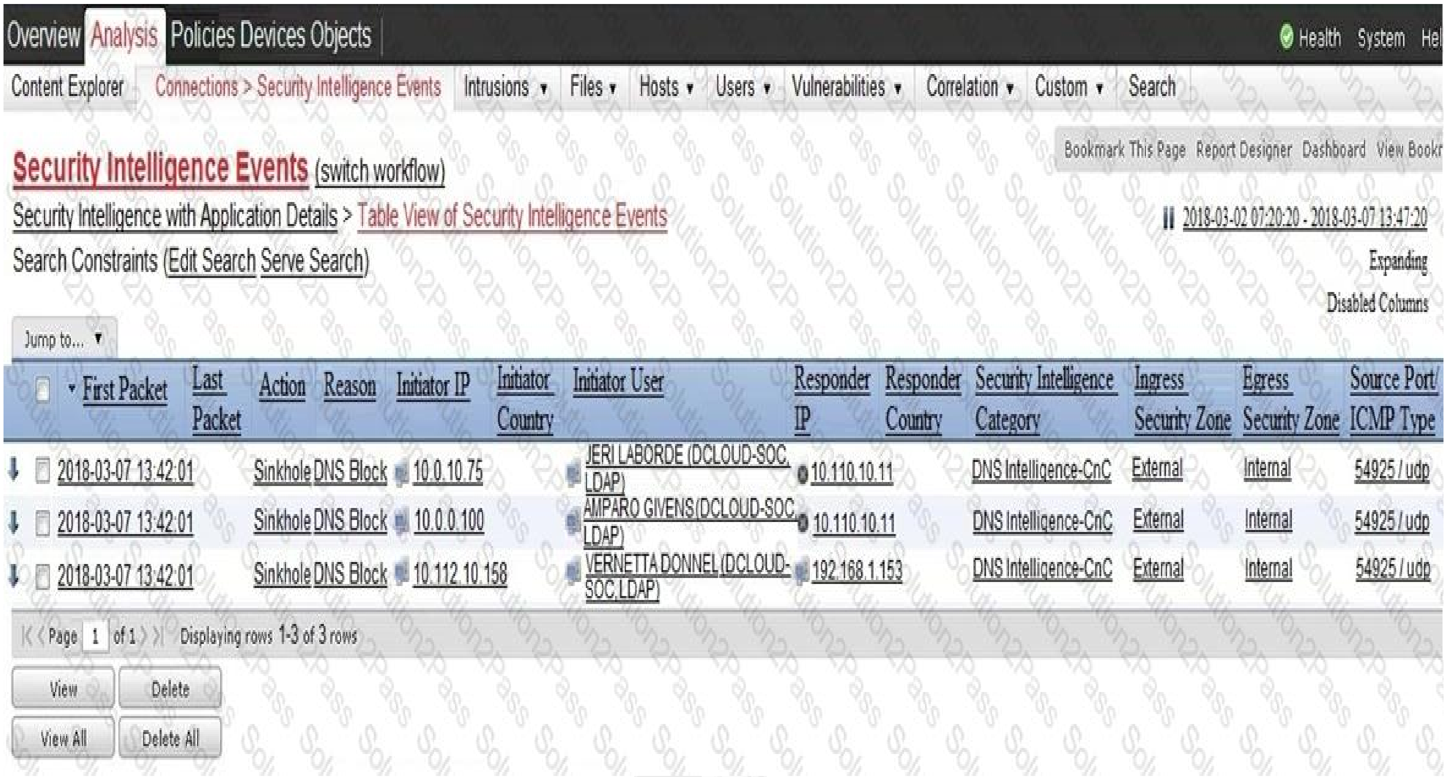
C. Traffic mirroring inspects live traffic for analysis and mitigation

D. Inline traffic copies packets for analysis and security

Answer: B

Question #:3

Refer to the exhibit.



Security Intelligence Events (switch workflow)

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

Search Constraints (Edit Search Serve Search)

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

	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
⬇ □	2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.10.75		JERI LABORDE (DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇ □	2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.0.100		AMPARO GIVENS(DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇ □	2018-03-07 13:42:01		Sinkhole	DNS Block	10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC,LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

|< < Page 1 of 1 > >| Displaying rows 1-3 of 3 rows

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

Answer: D E

Question #:4

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

Which technology makes this behavior possible?

A. encapsulation

B. TOR

C. tunneling

D. NAT

Answer: D

Question #:5

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

Answer: A

Question #:6

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

A. legal

B. compliance

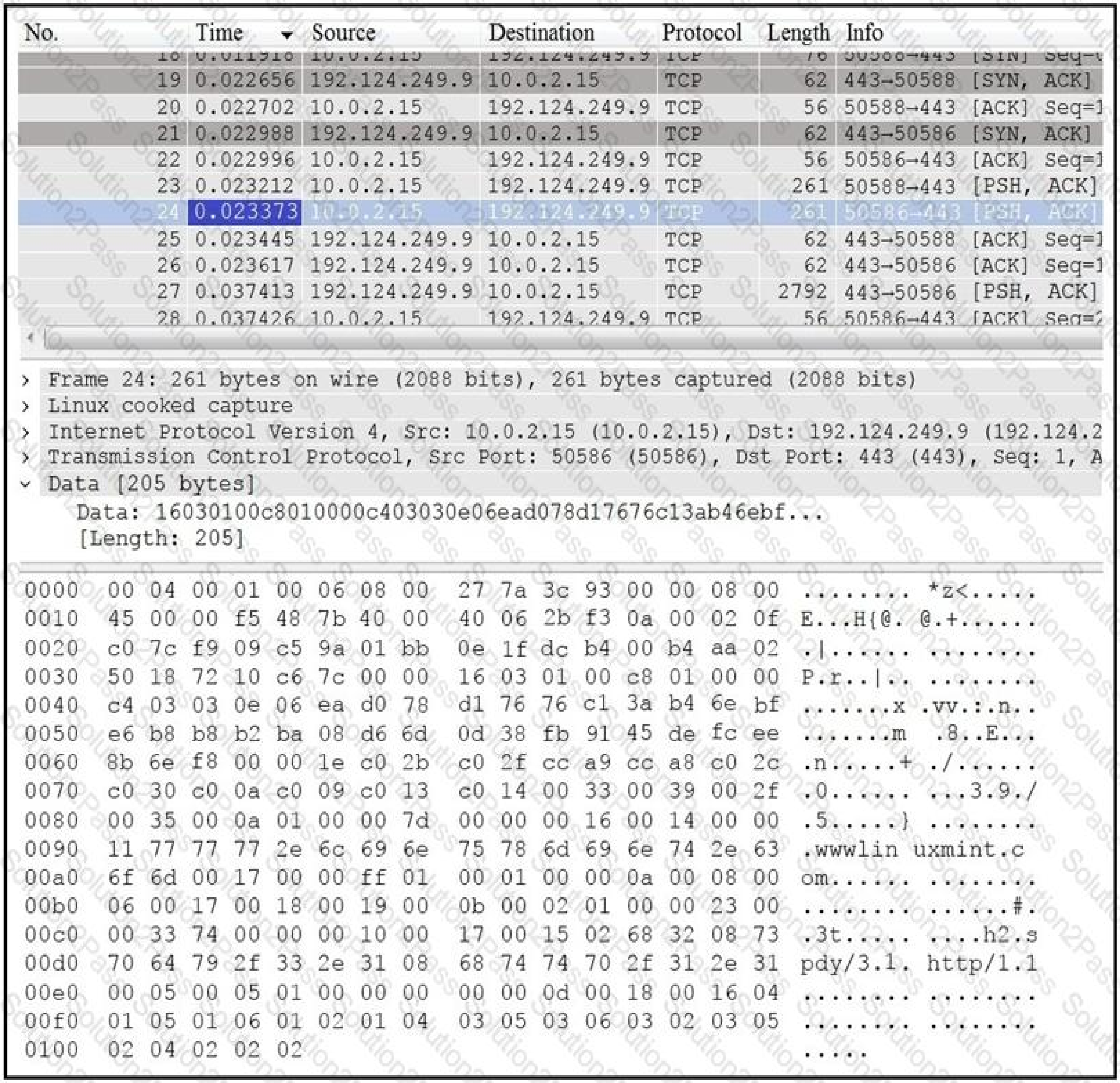
C. regulated

D. contractual

Answer: C

Question #:7

Refer to the exhibit.



```
No.      Time        Source          Destination     Protocol Length Info
      18 0.011918    10.0.2.15       192.124.249.9   TCP          76 50588→443 [SYN] Seq=0
      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 (192.124.2
> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A
v 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                                     .....
```

Which application protocol is in this PCAP file?

A. SSH

B. TCP

C. TLS

D. HTTP

Answer: B

Question #:8

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

Question #:9

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

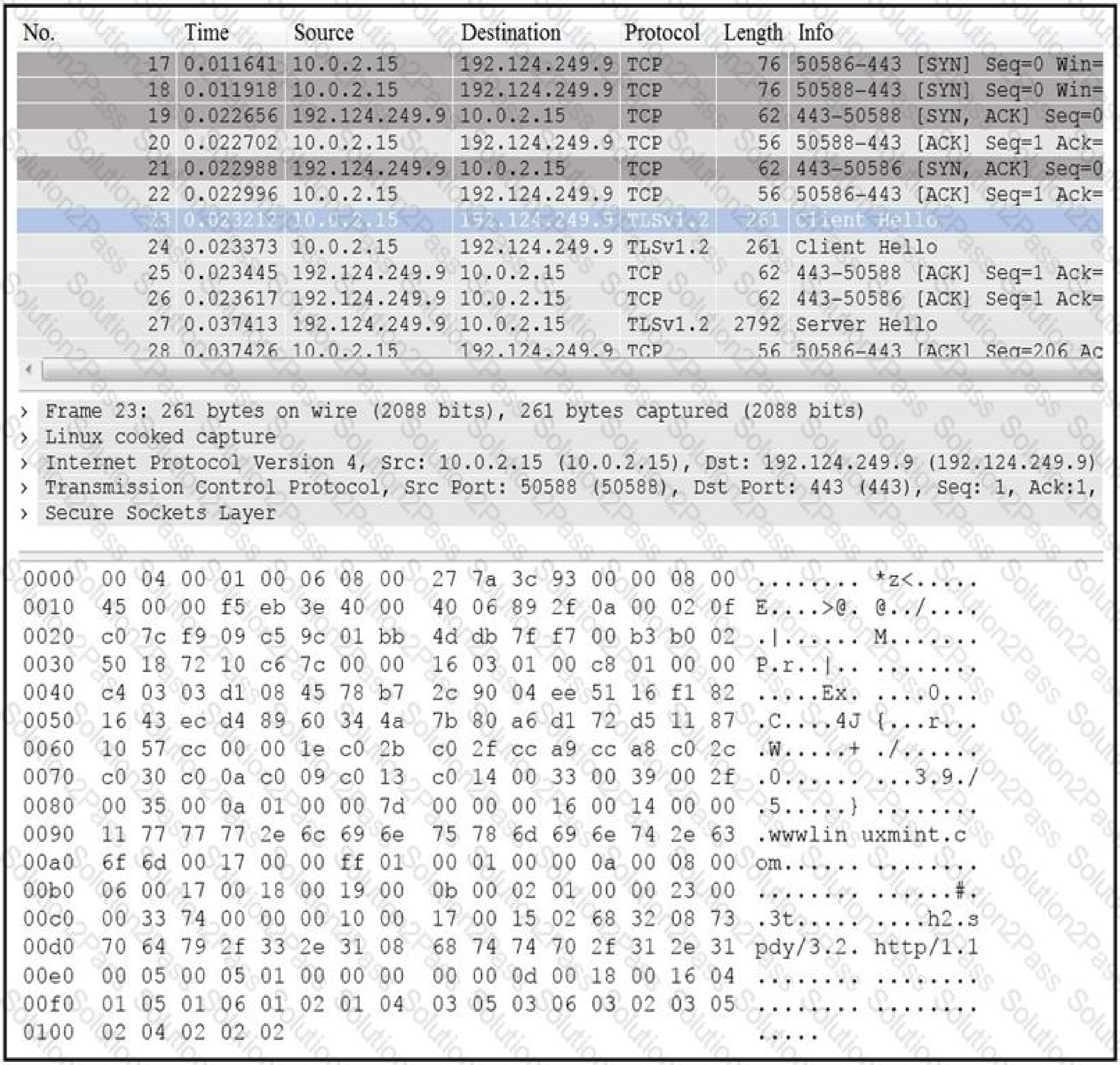
C. Stateful inspection is more secure than deep packet inspection on Layer 7

D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

Answer: D

Question #:10

Refer to the exhibit.

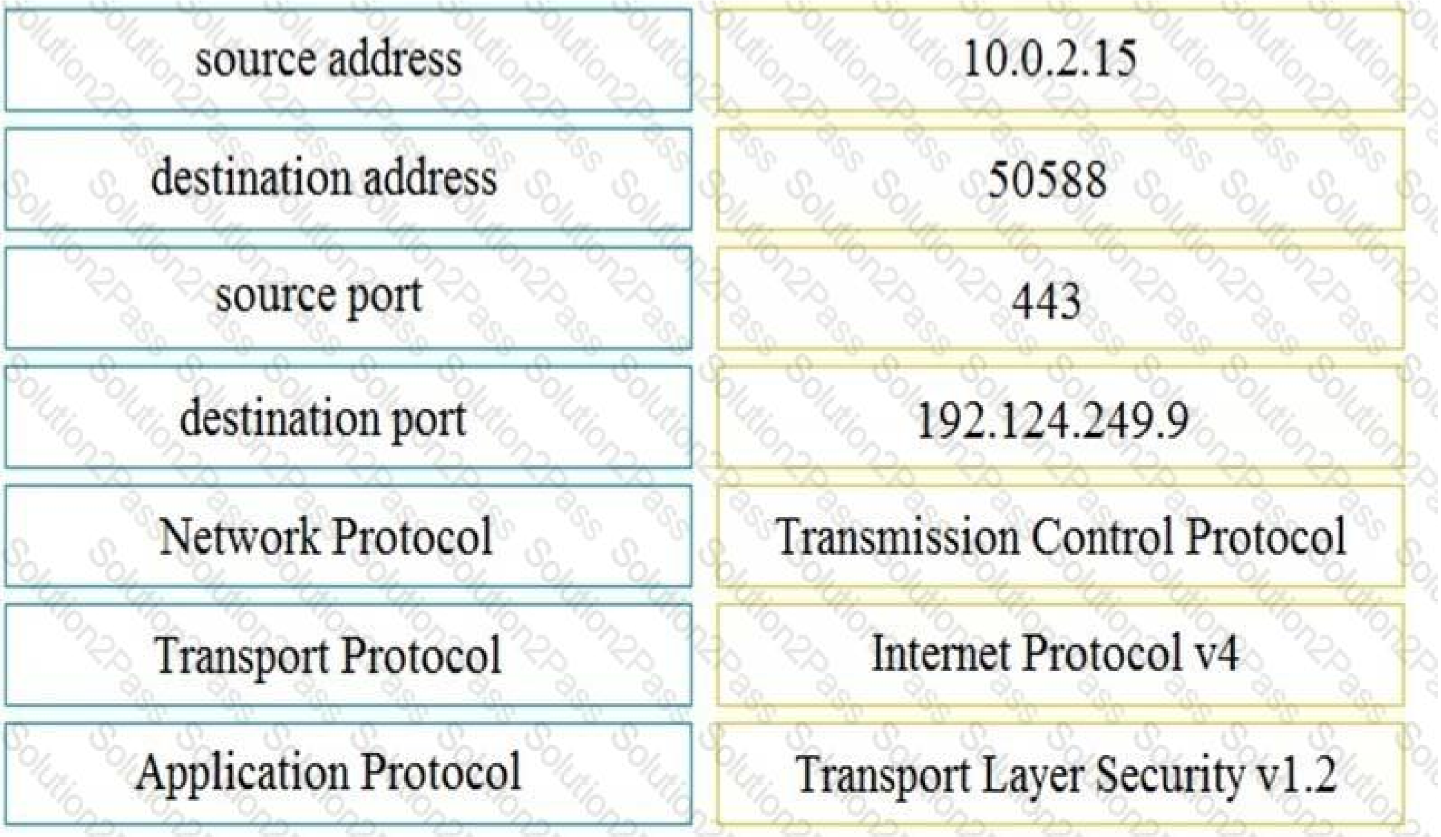


```
No.   Time      Source          Destination     Protocol Length Info
   17 0.011641  10.0.2.15       192.124.249.9   TCP          76 50586-443 [SYN] Seq=0 Win=
   18 0.011918  10.0.2.15       192.124.249.9   TCP          76 50588-443 [SYN] Seq=0 Win=
   19 0.022656  192.124.249.9   10.0.2.15       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
```

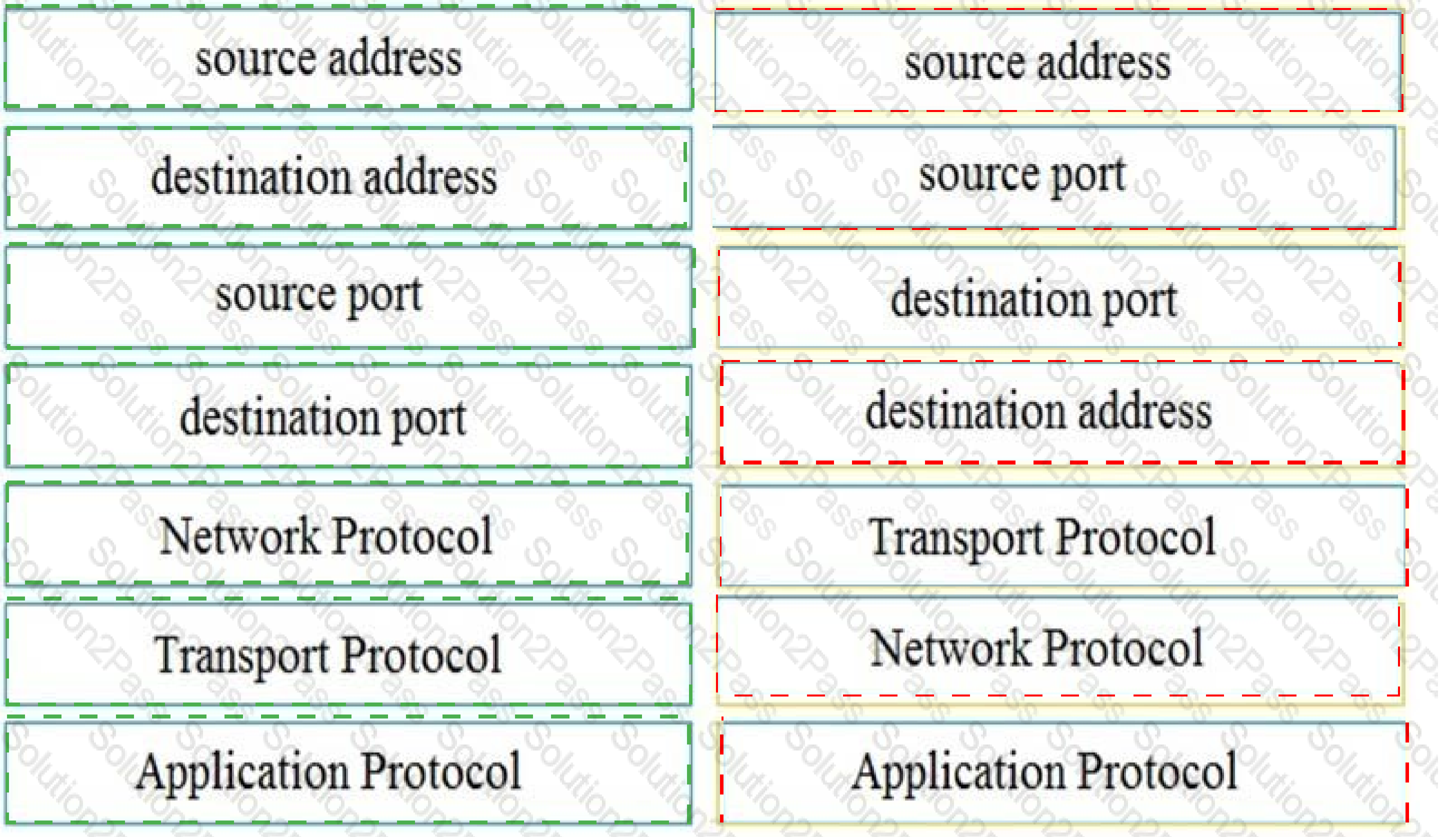
```
0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00  ........ *z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f  E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02  .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00  P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82  .....Ex. ....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.

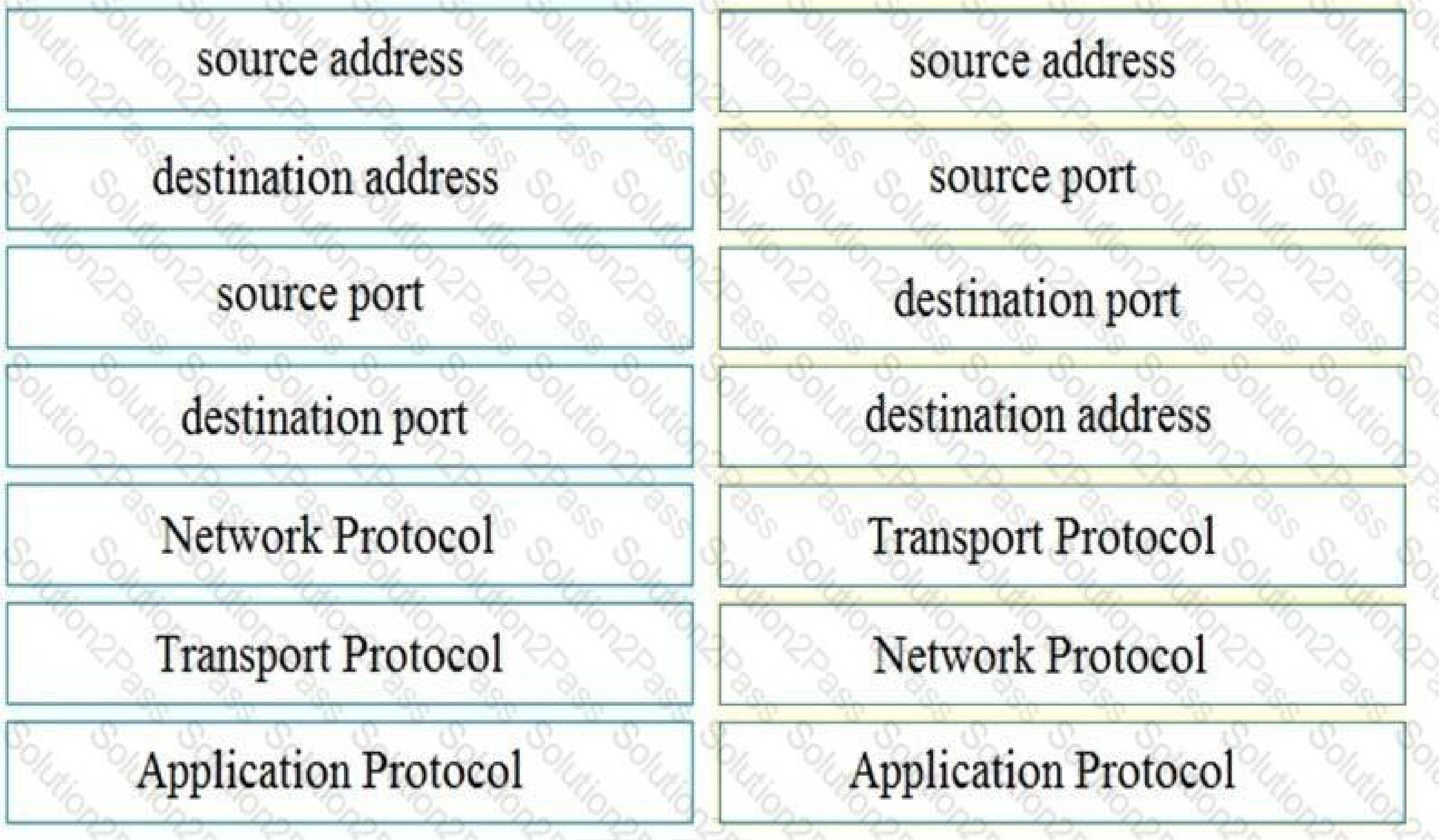


source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

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



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

Question #:11

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

Question #:12

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

Question #:13

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

Question #:14

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

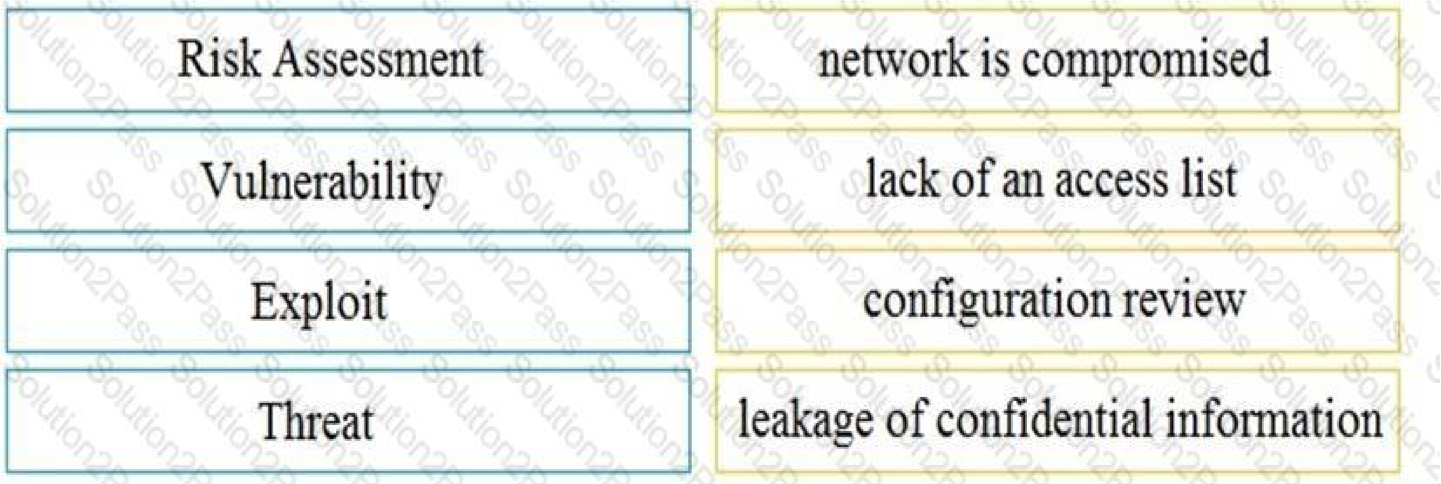
C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods

D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

Answer: C

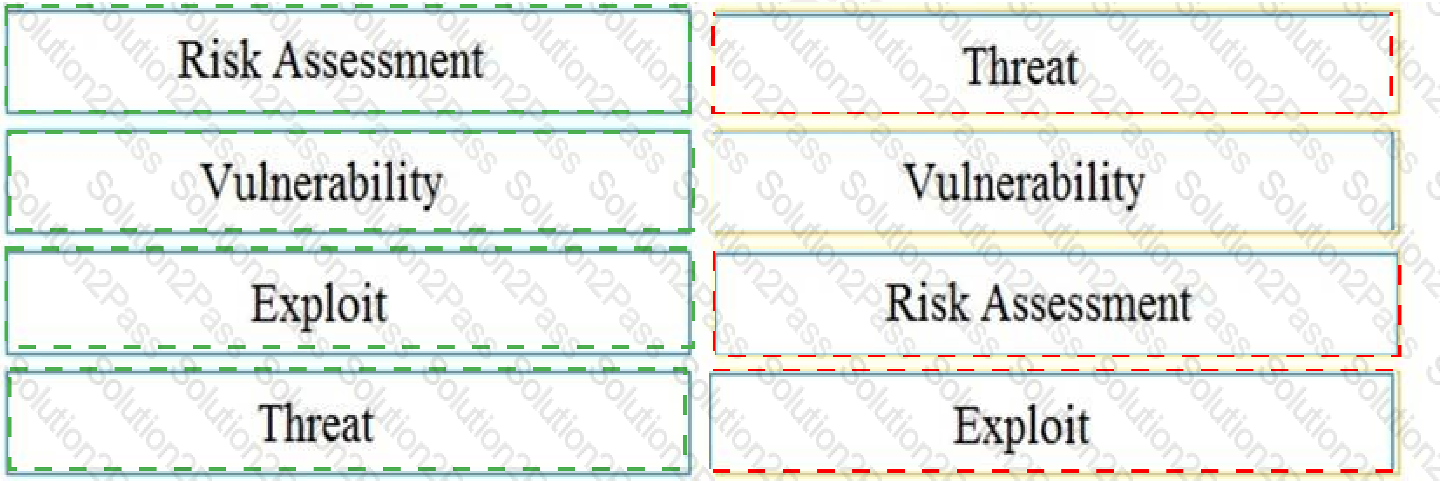
Question #:15

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

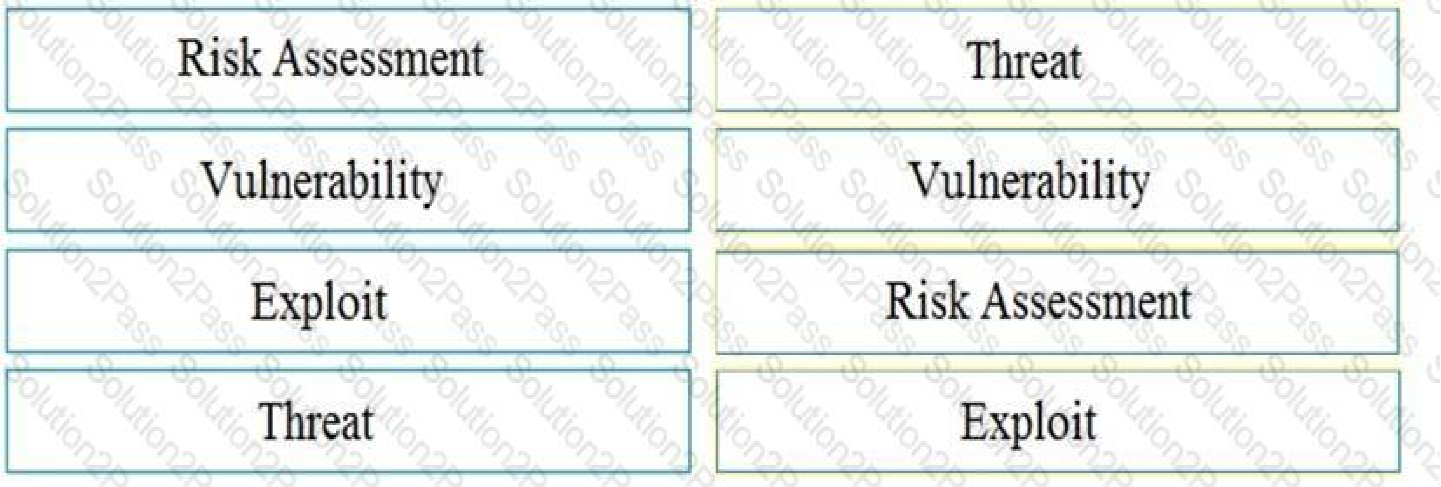


Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

Answer:



Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit



Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit

Question #:16

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

Answer: B

Question #:17

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

Answer: D

Question #:18

What is a purpose of a vulnerability management framework?

A. identifies, removes, and mitigates system vulnerabilities

B. detects and removes vulnerabilities in source code

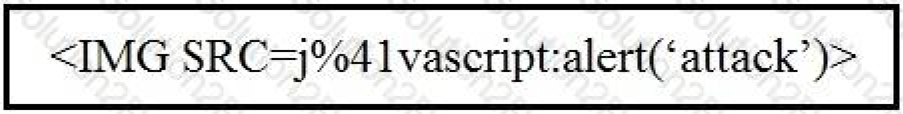
C. conducts vulnerability scans on the network

D. manages a list of reported vulnerabilities

Answer: A

Question #:19

Refer to the exhibit.



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

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

Answer: A

Question #:20

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

Question #:21

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

Question #:22

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

Which testing method did the intruder use?

A. social engineering

B. eavesdropping

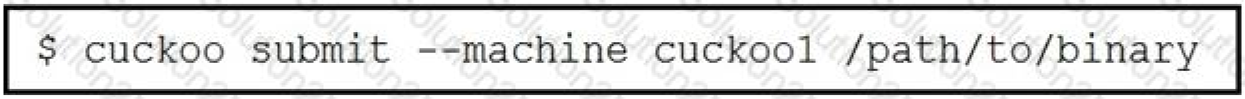
C. piggybacking

D. tailgating

Answer: A

Question #:23

Refer to the exhibit.



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

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

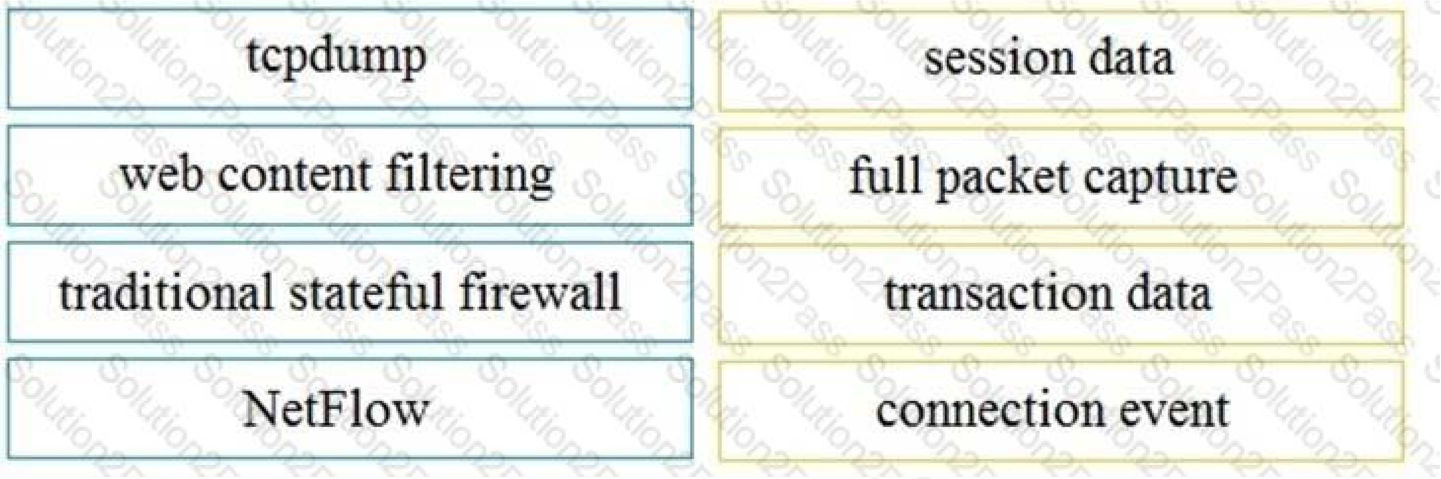
C. A binary on VM cuckoo1 is being submitted for evaluation

D. A URL is being evaluated to see if it has a malicious binary

Answer: C

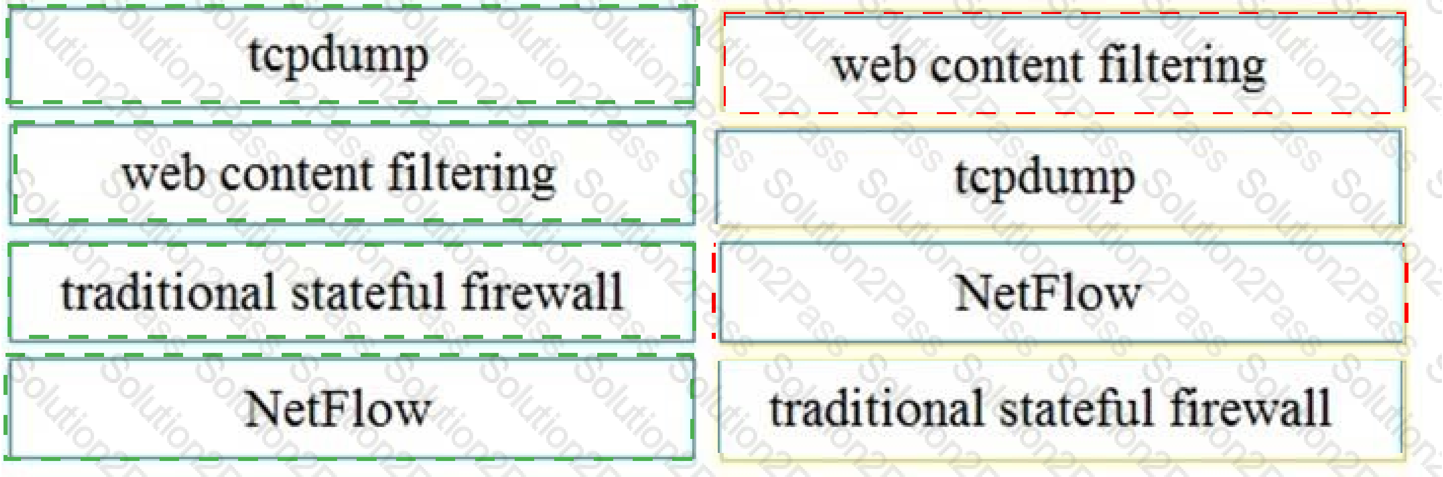
Question #:24

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

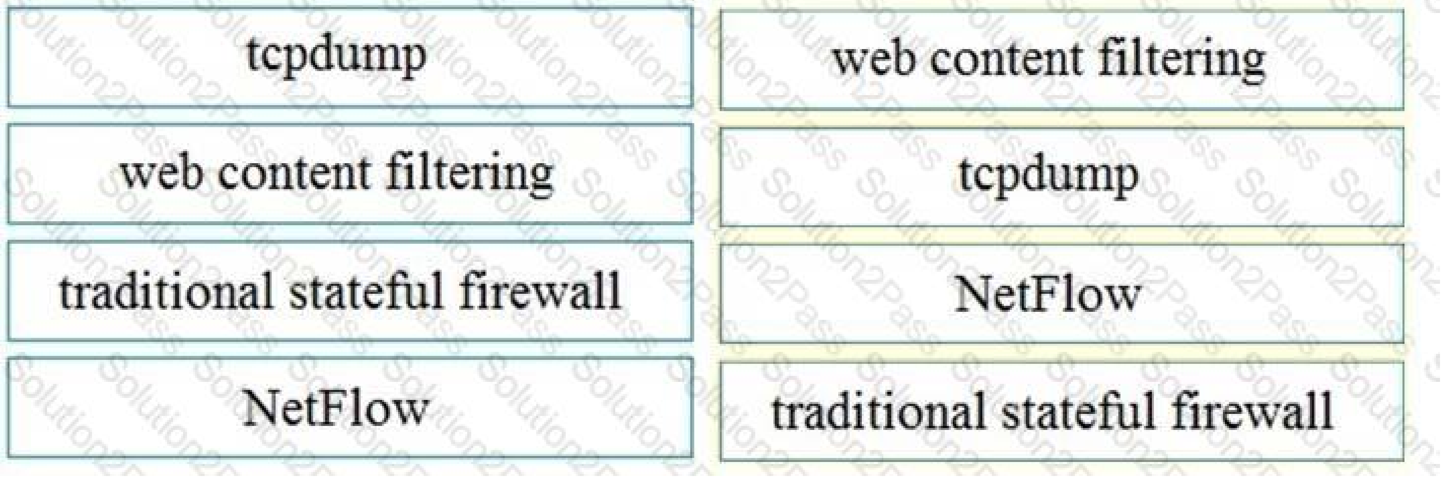


tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

Answer:



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



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

Question #:25

What makes HTTPS traffic difficult to monitor?

A. SSL interception

B. packet header size

C. signature detection time

D. encryption

Answer: D

Question #:26

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

Answer: C

Question #:27

Which artifact is used to uniquely identify a detected file?

A. file timestamp

B. file extension

C. file size

D. file hash

Answer: D

Question #:28

Which regex matches only on all lowercase letters?

A. [az]+

B. [^az]+

C. az+

D. a*z+

Answer: A

Question #:29

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

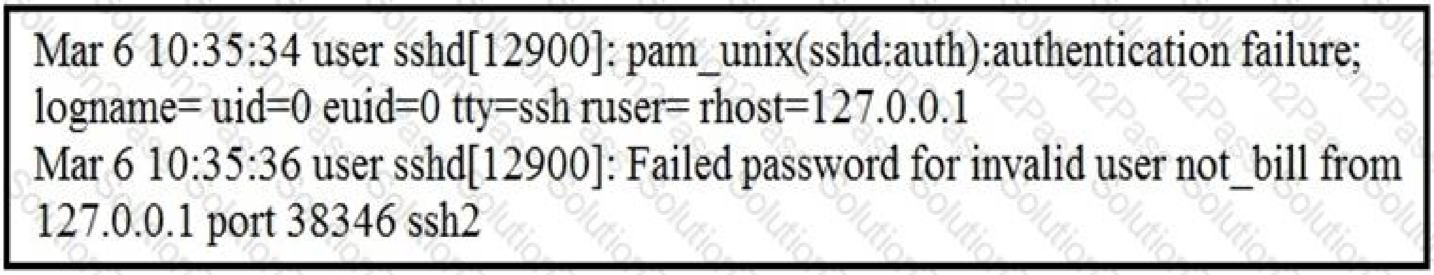
C. DAC is controlled by the operating system and MAC is controlled by an administrator

D. DAC is the strictest of all levels of control and MAC is object-based access

Answer: B

Question #:30

Refer to the exhibit.



```
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
```

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

Answer: D

Question #:31

Which access control model does SELinux use?

A. RBAC

B. DAC

C. MAC

D. ABAC

Answer: C

Question #:32

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

Answer: B

Question #:33

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

Answer: C D

Question #:34

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

Answer: D

Question #:35

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

Answer: B

Question #:36

The target web application server is running as the root user and is vulnerable to command injection. Which result of a successful attack is true?

A. cross-site scripting

B. cross-site scripting request forgery

C. privilege escalation

D. buffer overflow

Answer: B

Question #:37

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: A E

Question #:38

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

Question #:39

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

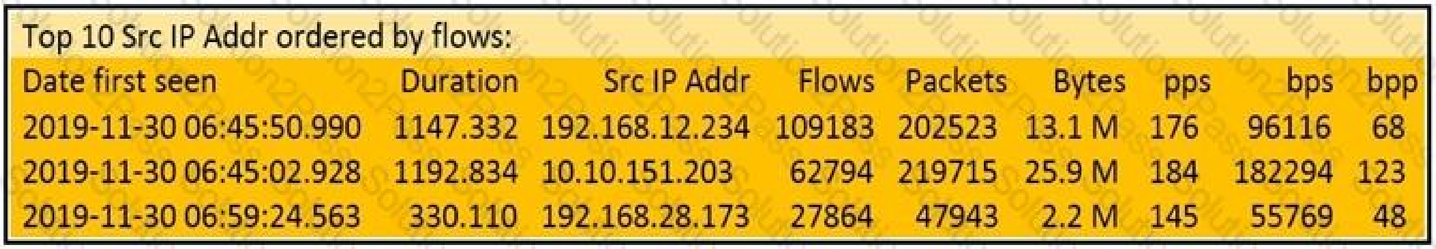
C. It authenticates domain identity when requesting SSL certificate

D. It validates client identity when communicating with the server

Answer: B

Question #:40

Refer to the exhibit.



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

What information is depicted?

A. IIS data

B. NetFlow data

C. network discovery event

D. IPS event data

Answer: B

Question #:41

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

Answer: B E

Question #:42

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

Answer: B

Question #:43

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

Which category classifies the intrusion?

A. weaponization

B. reconnaissance

C. installation

D. delivery

Answer: D

Question #:44

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

Question #:45

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

A. total throughout

B. session duration

C. running processes

D. OS fingerprint

E. listening ports

Answer: D E

Question #:46

Which evasion technique is a function of ransomware?

A. extended sleep calls

B. encryption

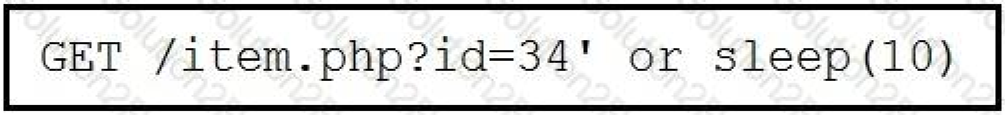
C. resource exhaustion

D. encoding

Answer: B

Question #:47

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

Question #:48

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.

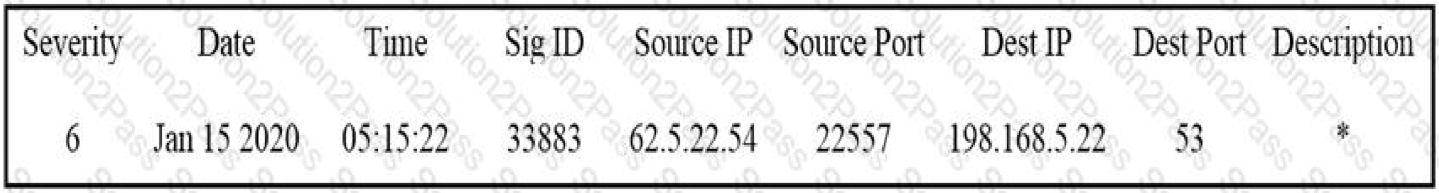
C. View any malicious files that a host has downloaded.

D. Verify host-to-host traffic within your network.

Answer: A

Question #:49

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

Question #:50

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

Question #:51

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

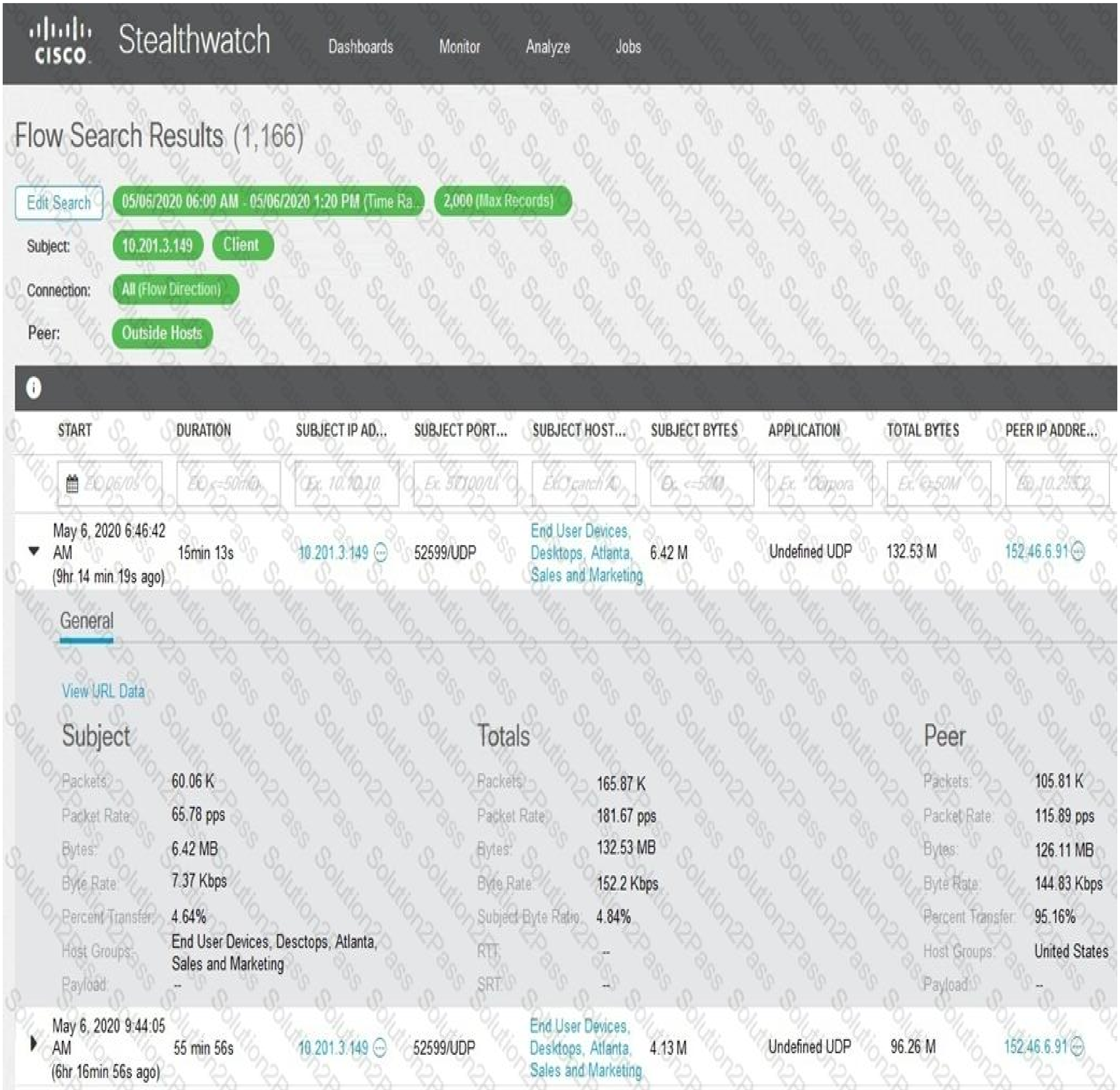
C. data mining

D. due diligence

Answer: A

Question #:52

Refer to the exhibit.



Flow Search Results (1,166)

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
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

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, Desctops, Atlanta, Sales and Marketing	RTT:	--	Host Groups:	United States
Payload:	--	SRT:	--	Payload:	--

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

Question #:53

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

A. NetScout

B. tcpdump

C. SolarWinds

D. netsh

Answer: B

Question #:54

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

Answer: A

Question #:55

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 arid fail logs

Answer: C

Question #:56

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

Question #:57

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: A D

Question #:58

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

Question #:59

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

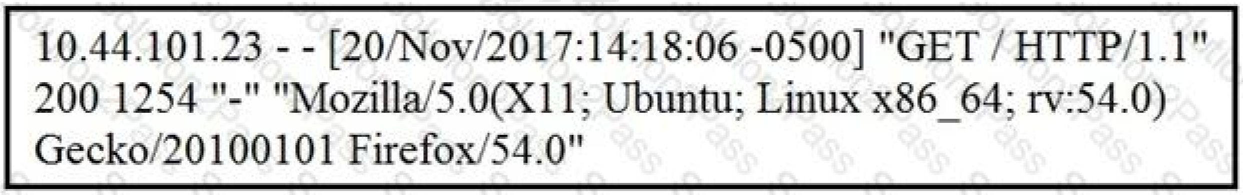
C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection

D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Answer: D

Question #:60

Refer to the exhibit.



```
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"
```

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

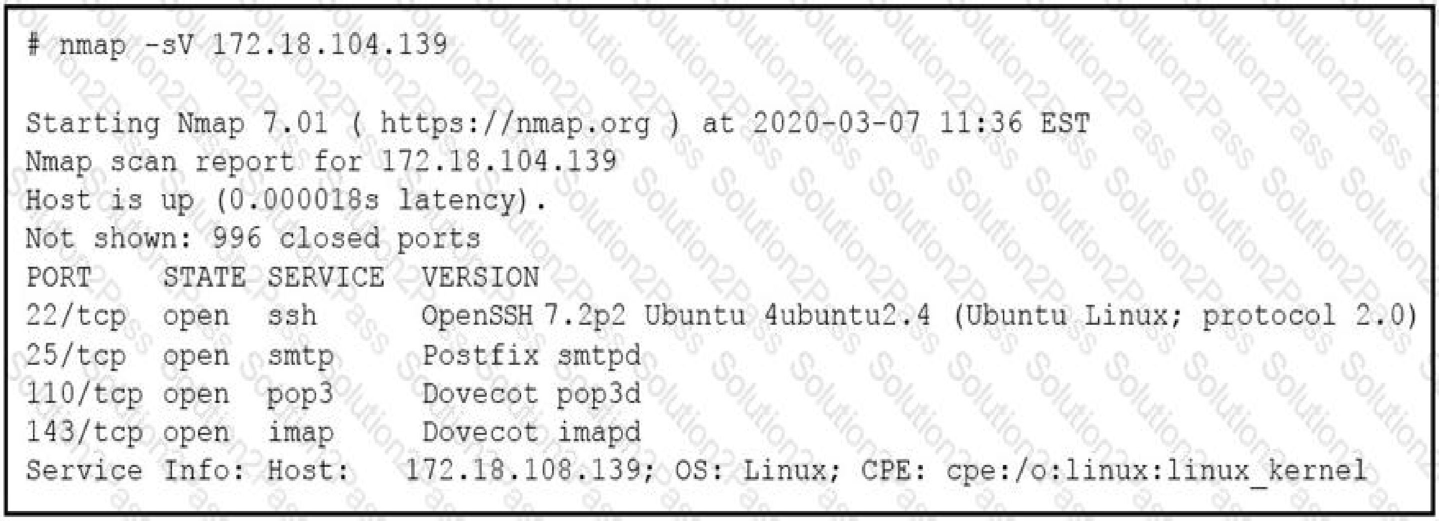
C. a successful access attempt was made to retrieve the root of the website

D. a denied access attempt was made to retrieve the password file

Answer: C

Question #:61

Refer to the exhibit.



```
# 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
```

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

Answer: C

Question #:62

Which event is user interaction?

A. gaining root access

B. executing remote code

C. reading and writing file permission

D. opening a malicious file

Answer: D

Question #:63

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

Answer: D

Question #:64

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

A. privilege escalation

B. DDoS attack

C. phishing

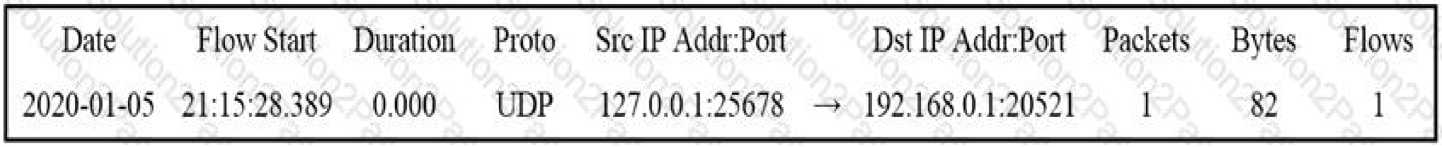
D. man-in-the-middle

E. pharming

Answer: C E

Question #:65

Refer to the exhibit.



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

Which type of log is displayed?

A. proxy

B. NetFlow

C. IDS

D. sys

Answer: B

Question #:66

Which utility blocks a host portscan?

A. HIDS

B. sandboxing

C. host-based firewall

D. antimalware

Answer: C

Question #:67

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

Answer: A

Question #:68

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

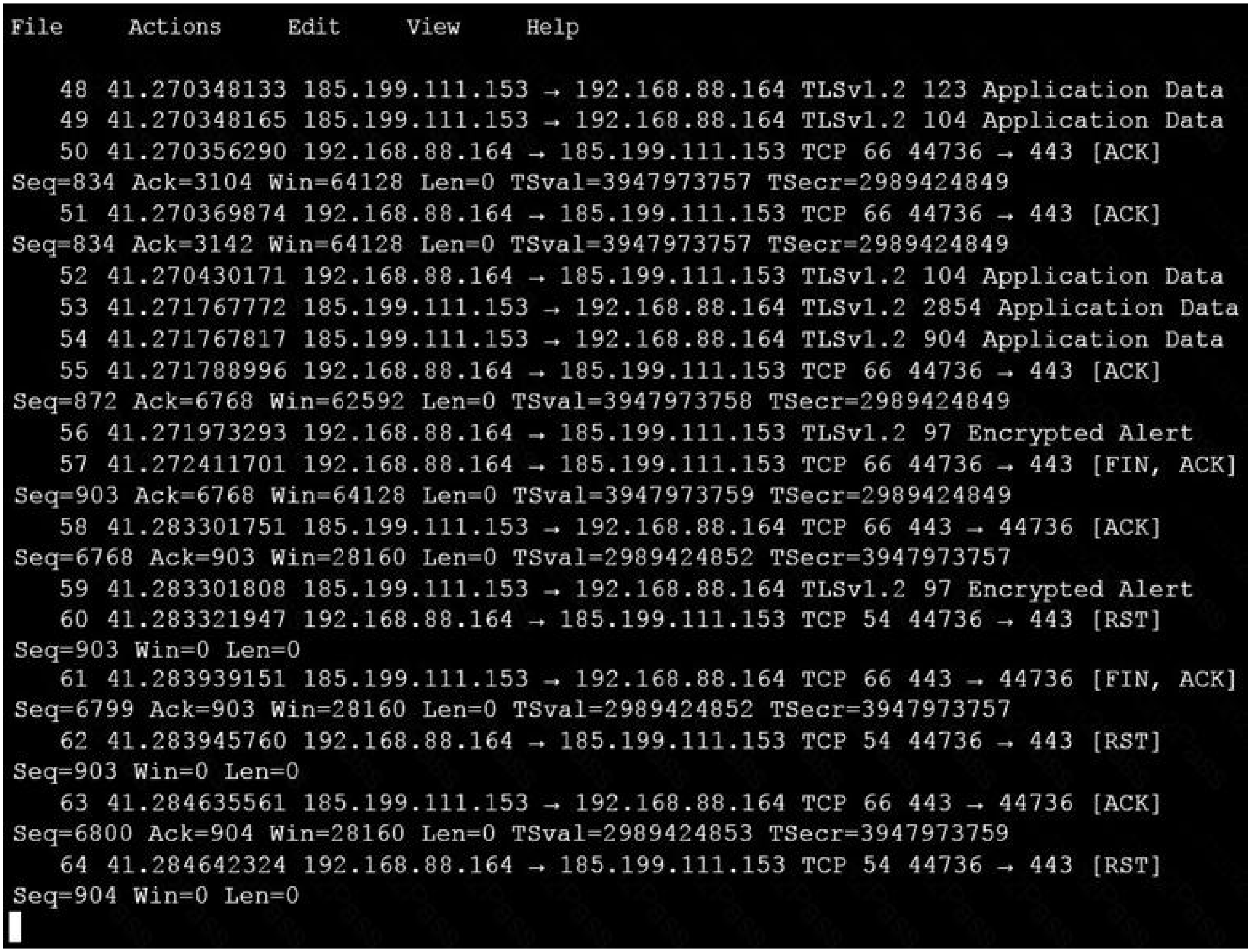
C. SOAR receives information from a single platform and delivers it to a SIEM

D. SIEM receives information from a single platform and delivers it to a SOAR

Answer: A

Question #:69

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.



```
   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
```

Which obfuscation technique is the attacker using?

A. Base64 encoding

B. transport layer security encryption

C. SHA-256 hashing

D. ROT13 encryption

Answer: B

Question #:70

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

Question #:71

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

A. detection and analysis

B. post-incident activity

C. vulnerability management

D. risk assessment

E. vulnerability scoring

Answer: A B

Question #:72

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

A. probabilistic

B. indirect

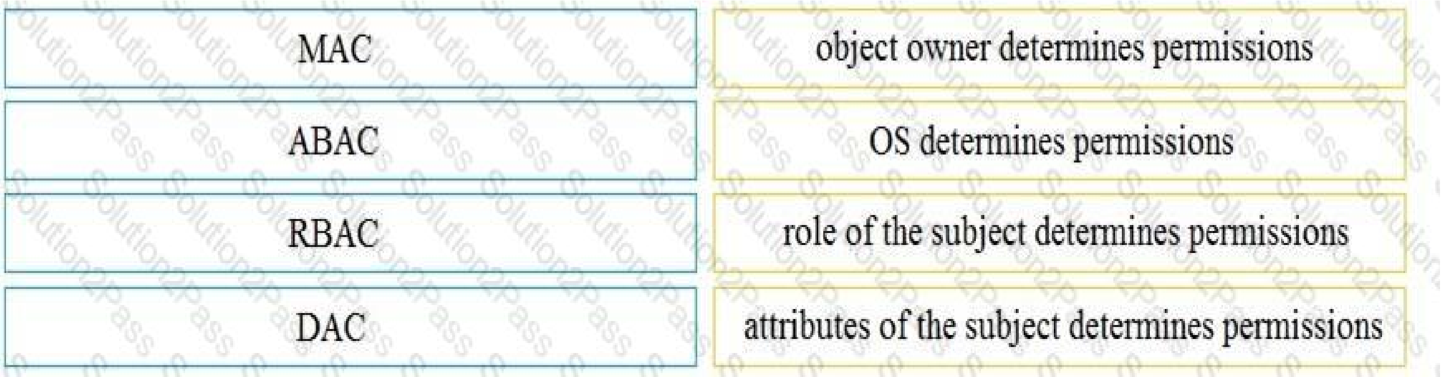
C. best

D. corroborative

Answer: D

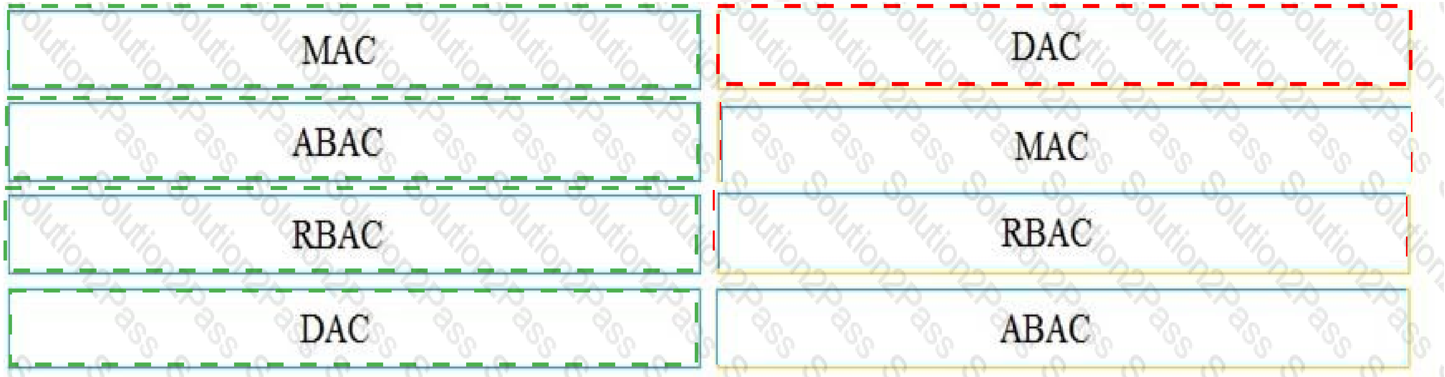
Question #:73

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

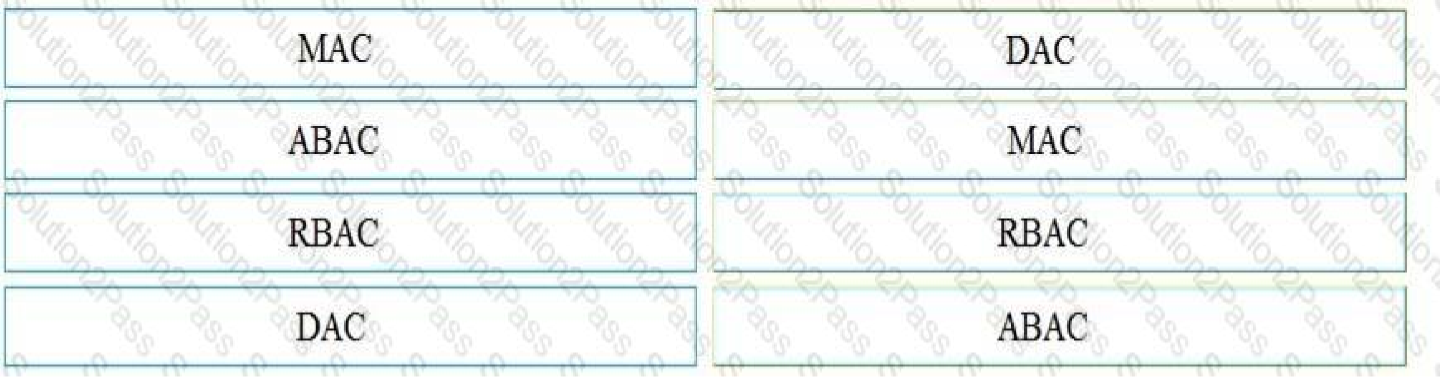


MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

Answer:



MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC



MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

Question #:74

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

Answer: B

Question #:75

Which attack method intercepts traffic on a switched network?

A. denial of service

B. ARP cache poisoning

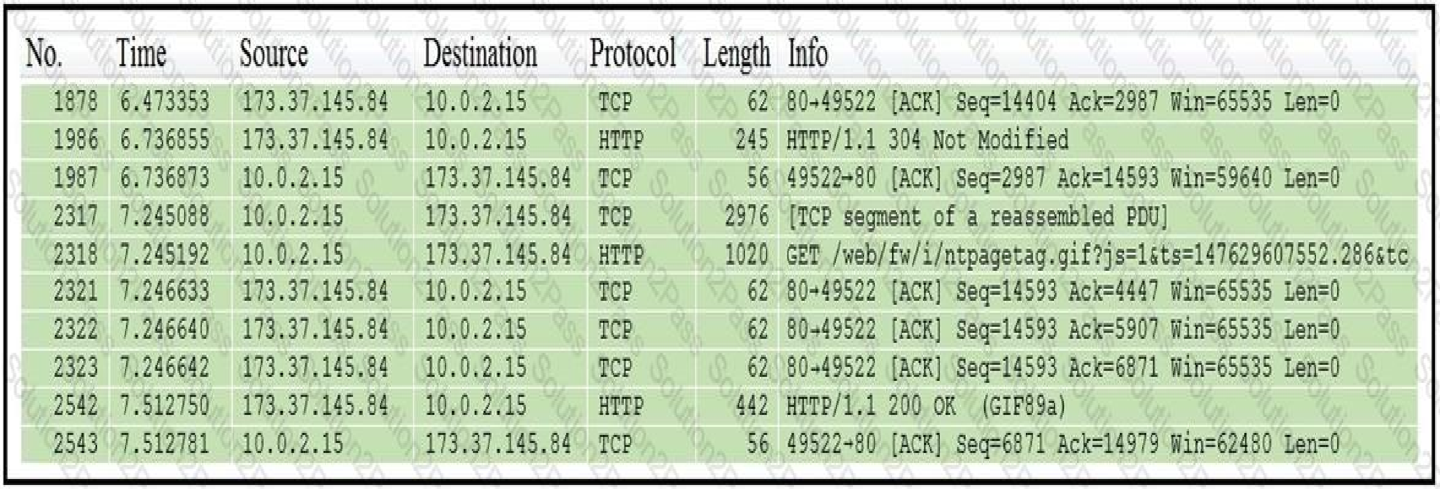
C. DHCP snooping

D. command and control

Answer: C

Question #:76

Refer to the exhibit.



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/ntpagetag.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

Which packet contains a file that is extractable within Wireshark?

A. 2317

B. 1986

C. 2318

D. 2542

Answer: D

Question #:77

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

Answer: D

Explanation

Section: (none)

Explanation

Question #:78

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

Question #:79

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

Answer: A

Question #:80

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

Which information is available on the server certificate?

A. server name, trusted subordinate CA, and private key

B. trusted subordinate CA, public key, and cipher suites

C. trusted CA name, cipher suites, and private key

D. server name, trusted CA, and public key

Answer: D

Question #:81

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

Question #:82

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

Answer: D

Question #:83

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

A. internet

B. transport

C. application

D. data link

Answer: C

Question #:84

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

Question #:85

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

Answer: B

Question #:86

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

Answer: B

Question #:87

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

Answer: C

Question #:88

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

Answer: B

Question #:89

You have identified a malicious file in a sandbox analysis tool. Which piece of file information from the analysis

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

A. file name

B. file hash value

C. file type

D. file size

Answer: B

Question #:90

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

Question #:91

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: C

Question #:92

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

Answer: D

Question #:93

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

Question #:94

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

Question #:95

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

Which type of evidence is this?

A. best evidence

B. prima facie evidence

C. indirect evidence

D. physical evidence

Answer: C

Question #:96

How is attacking a vulnerability categorized?

A. action on objectives

B. delivery

C. exploitation

D. installation

Answer: C

Question #:97

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

Answer: A

Question #:98

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

Answer: D

Question #:99

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

Question #:100

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

A. session duration

B. total throughput

C. running processes

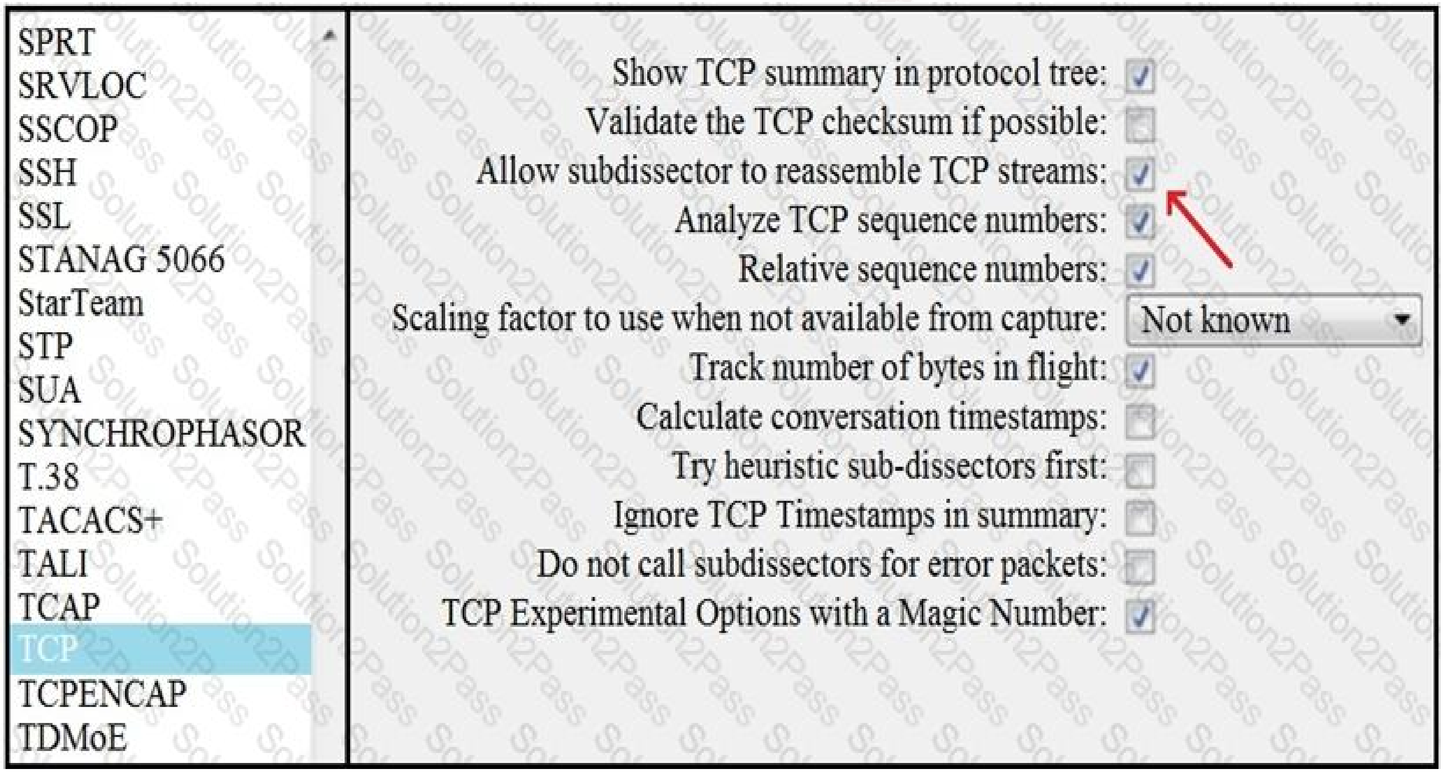
D. listening ports

E. OS fingerprint

Answer: D E

Question #:101

Refer to the exhibit.



Show TCP summary in protocol tree: ☑

Validate the TCP checksum if possible: □

Allow subdissector to reassemble TCP streams: ☑

Analyze TCP sequence numbers: ☑

Relative sequence numbers: ☑

Scaling factor to use when not available from capture: Not known

Track number of bytes in flight: ☑

Calculate conversation timestamps: □

Try heuristic sub-dissectors first: □

Ignore TCP Timestamps in summary: □

Do not call subdissectors for error packets: □

TCP Experimental Options with a Magic Number: ☑

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

Answer: D

Question #:102

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

A. colo?ur

B. col[08]+our

C. colou?r

D. col[09]+our

Answer: C

Question #:103

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: A C

Question #:104

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

Answer: D

Question #:105

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

Answer: D

About solution2pass.com

solution2pass.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@solution2pass.com
- Feedback: feedback@solution2pass.com
- Support: support@solution2pass.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.