Cisco

Exam Questions 200-201

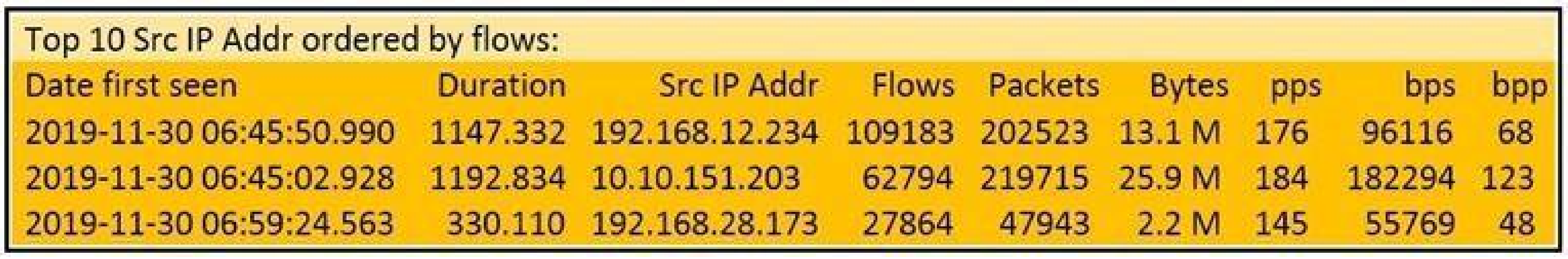
Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

A. syslog messages
B. full packet capture
C. NetFlow
D. firewall event logs

Answer: C

NEW QUESTION 2
Refer to the exhibit.



Top 10 Src IP Addr ordered by flows:

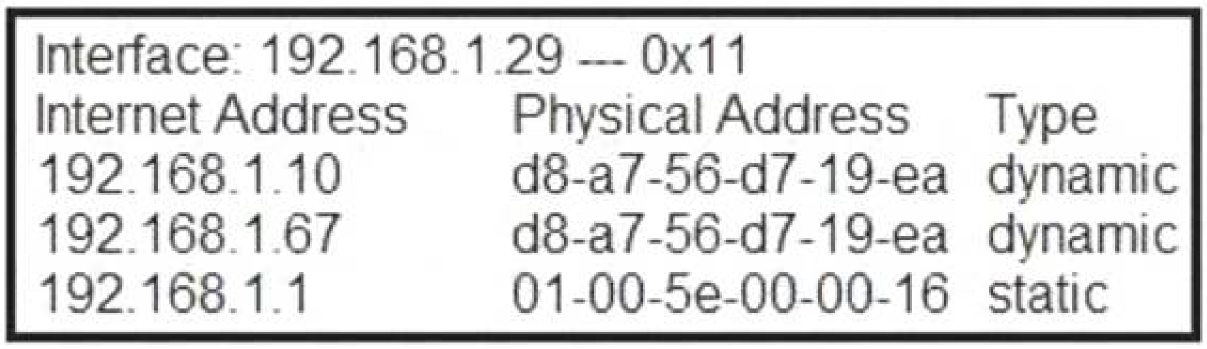
Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

What information is depicted?

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

Answer: B

NEW QUESTION 3
Refer to the exhibit.



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

What is occurring in this network?

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

Answer: A

NEW QUESTION 4
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

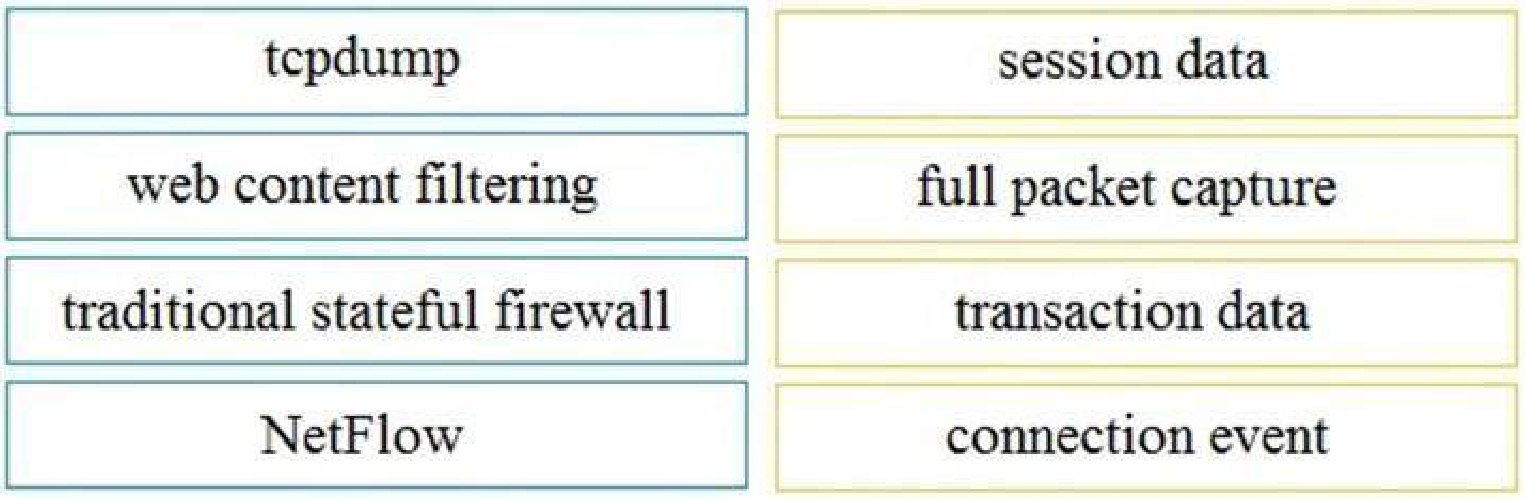
Answer: B

NEW QUESTION 5
Which process is used when IPS events are removed to improve data integrity?

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

Answer: B

NEW QUESTION 6
Drag and drop the technology on the left onto the data type the technology provides on the right.

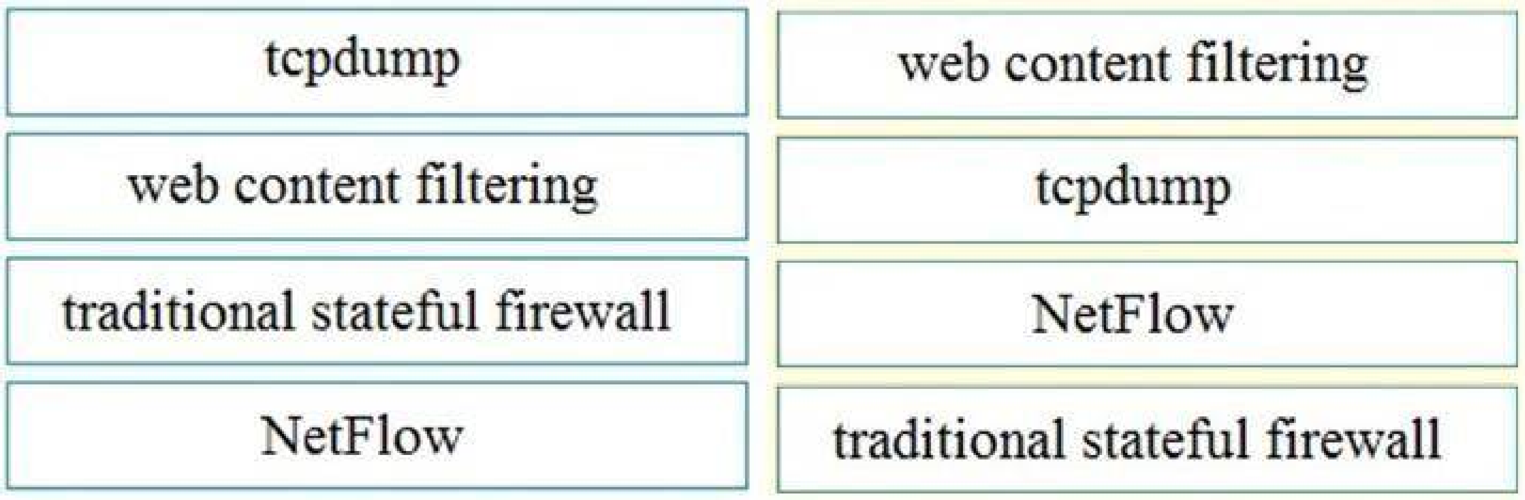


tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

A. Mastered
B. Not Mastered

Answer: A

Explanation:



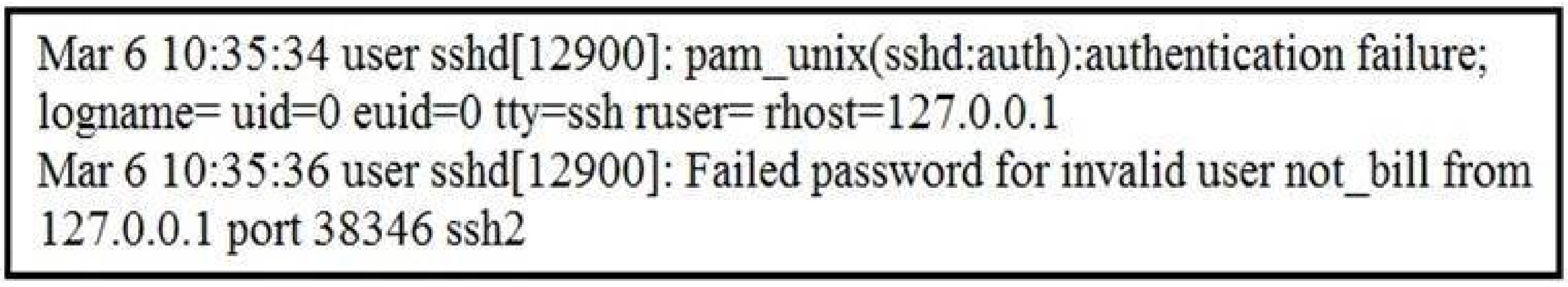
tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

NEW QUESTION 7
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: AB

NEW QUESTION 8
Refer to the exhibit.



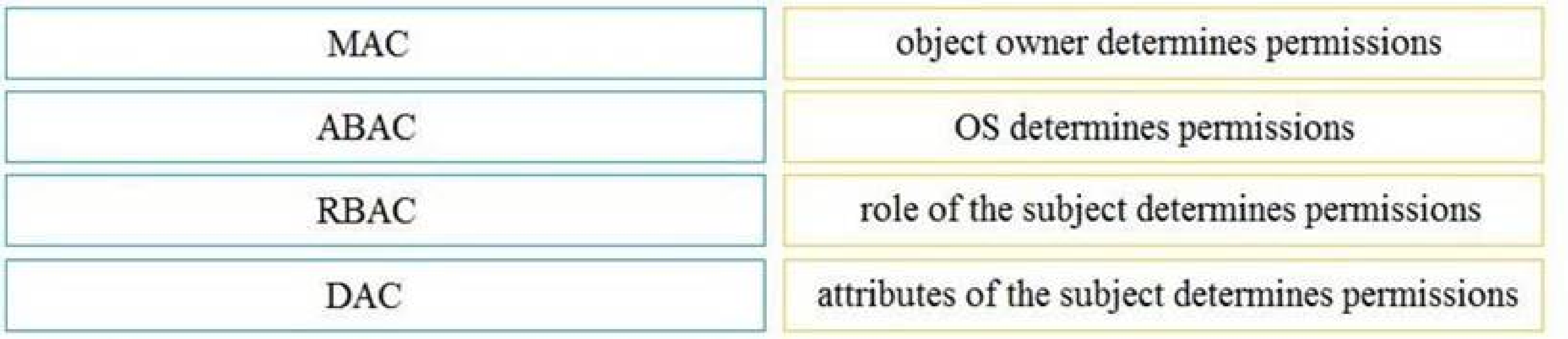
```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

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

NEW QUESTION 9
Drag and drop the access control models from the left onto the correct descriptions on the right.

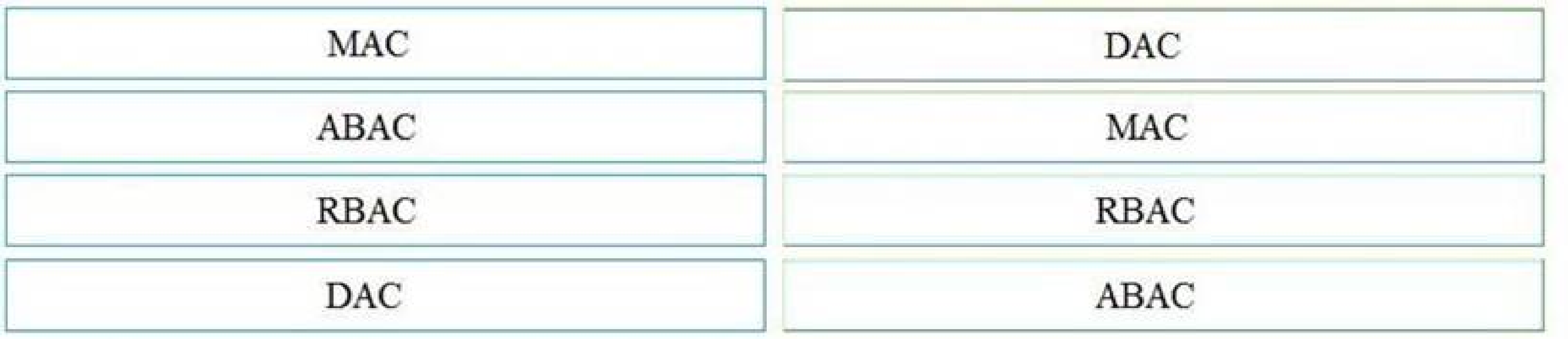


MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

A. Mastered
B. Not Mastered

Answer: A

Explanation:



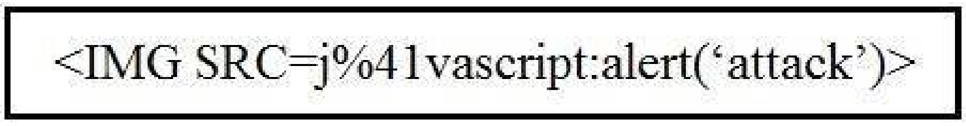
MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION 10
Which category relates to improper use or disclosure of PII data?

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

Answer: C

NEW QUESTION 10
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

NEW QUESTION 15
Which incidence response step includes identifying all hosts affected by an attack'?

A. post-incident activity
B. detection and analysis
C. containment eradication and recovery
D. preparation

Answer: A

NEW QUESTION 16
Which attack method intercepts traffic on a switched network?

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

Answer: C

NEW QUESTION 19

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

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

Answer: A

NEW QUESTION 23
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

NEW QUESTION 25
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

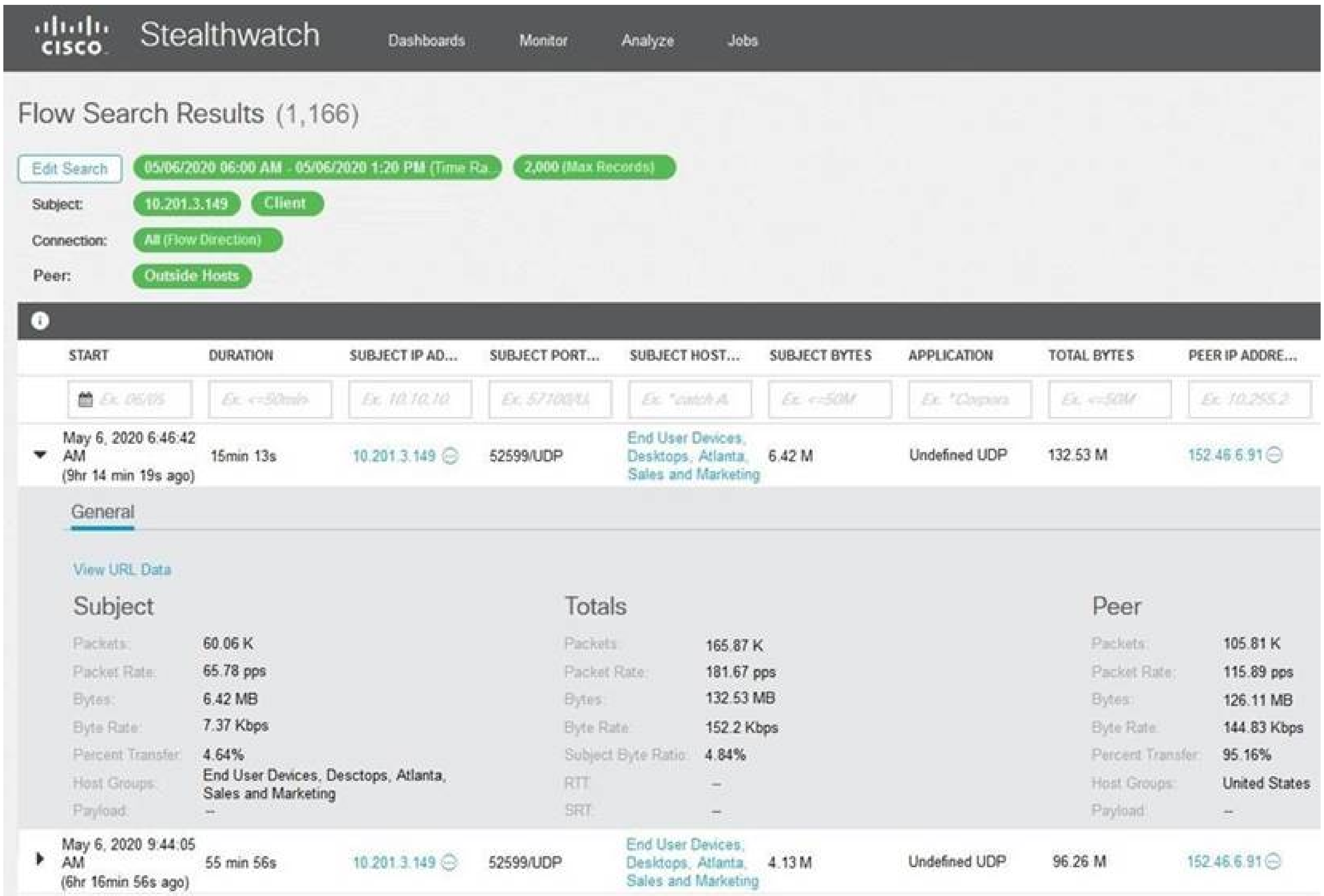
Answer: B

NEW QUESTION 27
Which metric is used to capture the level of access needed to launch a successful attack?

A. privileges required
B. user interaction
C. attack complexity
D. attack vector

Answer: A

NEW QUESTION 28
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...
Ex. 06/05	Ex. <=50min	Ex. 10.10.10	Ex. 57100/U	Ex. *catch A	Ex. <=50M	Ex. *Corpora	Ex. <=50M	Ex. 10.255.2
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

Subject

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, Desctops, Atlanta, Sales and Marketing
Payload:	--

Totals

Packets:	165.87 K
Packet Rate:	181.67 pps
Bytes:	132.53 MB
Byte Rate:	152.2 Kbps
Subject Byte Ratio:	4.84%
RTT:	--
SRT:	--

Peer

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
Payload:	--

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDRE...
May 6, 2020 9:44:05 AM (6hr 16min 56s ago)	55 min 56s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	4.13 M	Undefined UDP	96.26 M	152.46.6.91

What is the potential threat identified in this Stealthwatch dashboard?

A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.

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

Answer: D

NEW QUESTION 30
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

NEW QUESTION 34
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. integrity
B. confidentiality
C. availability
D. scope

Answer: A

NEW QUESTION 36
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

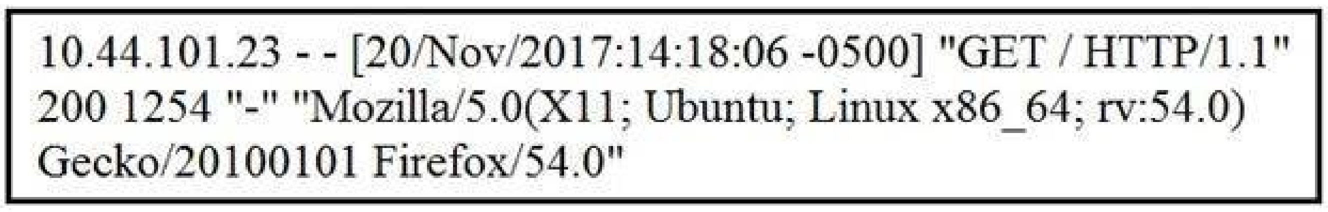
Answer: D

NEW QUESTION 39
A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

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

Answer: C

NEW QUESTION 42
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

NEW QUESTION 46
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

NEW QUESTION 49

What makes HTTPS traffic difficult to monitor?

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

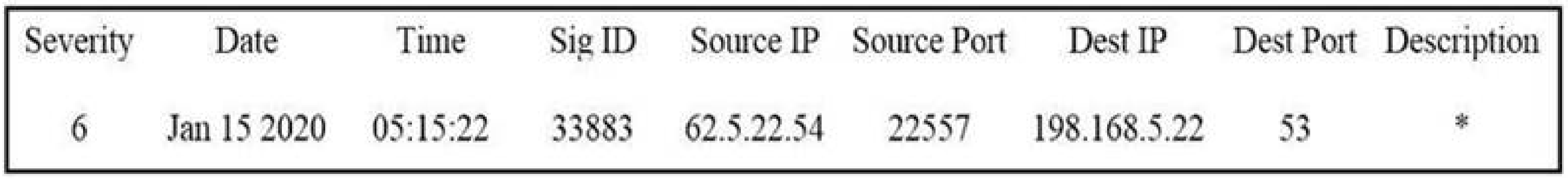
Answer: D

NEW QUESTION 54
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

NEW QUESTION 59
Refer to the exhibit.



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

Which type of log is displayed?

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

Answer: D

NEW QUESTION 64
What is an attack surface as compared to a vulnerability?

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

Answer: B

NEW QUESTION 66
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: CD

NEW QUESTION 68
What does cyber attribution identify in an investigation?

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

Answer: B

NEW QUESTION 69
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

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

Answer: B

NEW QUESTION 74
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: DE

NEW QUESTION 79
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

NEW QUESTION 82
Which security technology allows only a set of pre-approved applications to run on a system?

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

Answer: C

NEW QUESTION 84
A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?

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

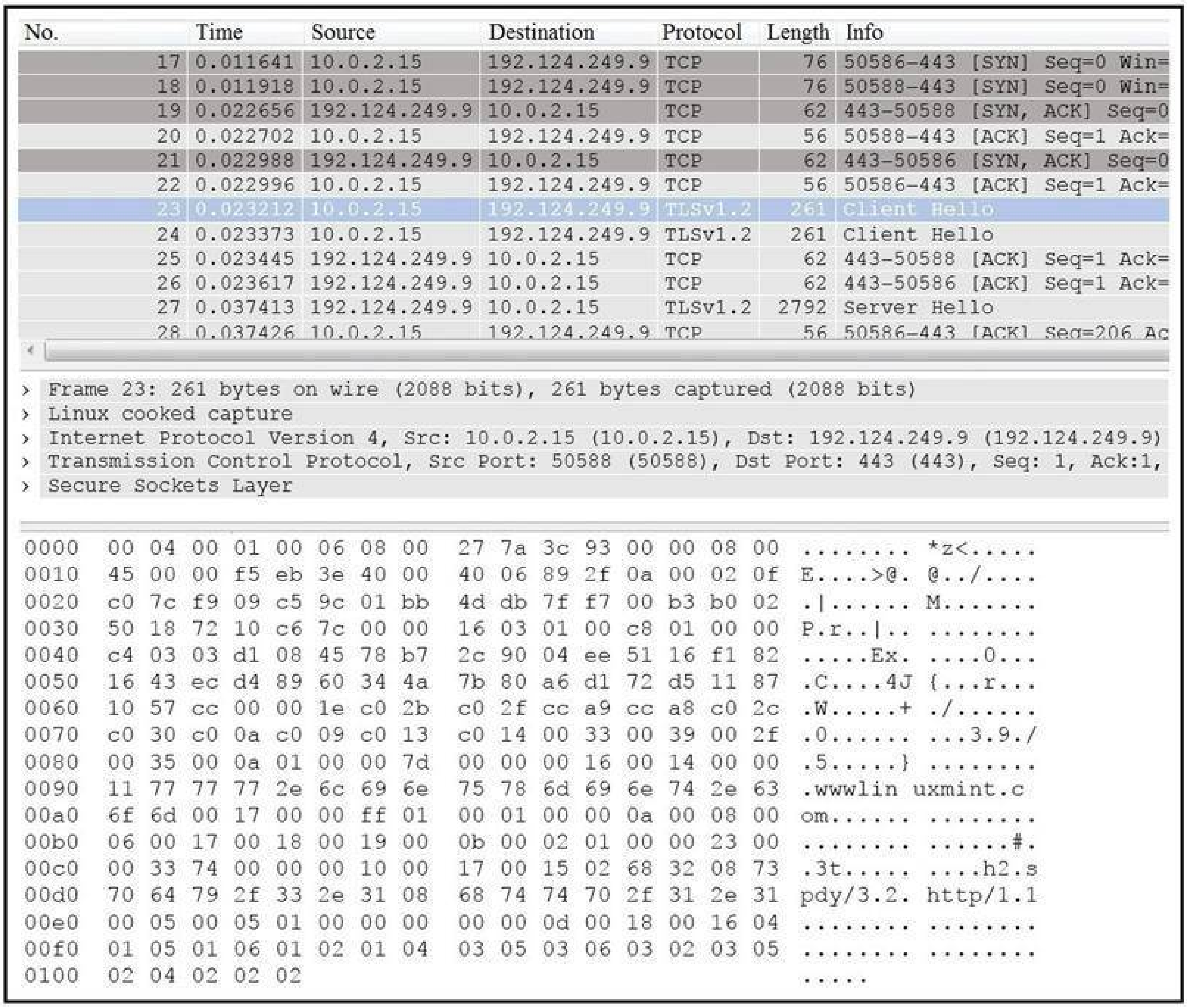
Answer: D

NEW QUESTION 87
An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

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

Answer: C

NEW QUESTION 92
Refer to the exhibit.

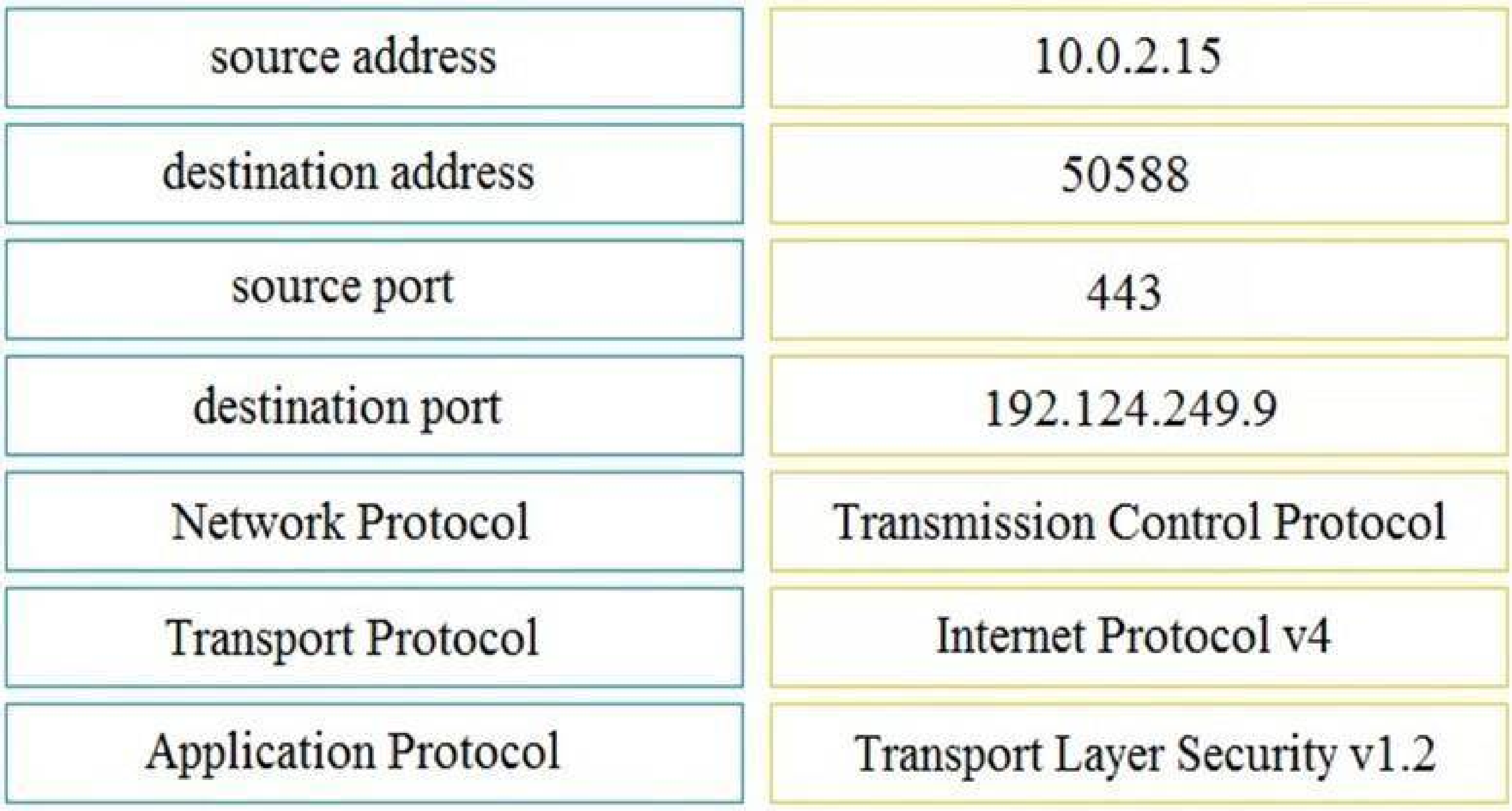


```
No.     Time      Source          Destination     Protocol Length Info
     17 0.011641  10.0.2.15       192.124.249.9   TCP         76 50586-443 [SYN] Seq=0 Win=
     18 0.011918  10.0.2.15       192.124.249.9   TCP         76 50588-443 [SYN] Seq=0 Win=
     19 0.022656  192.124.249.9   10.0.2.15       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. ....Q...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87   .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c   .W.....+ ./......
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f   .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00   .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63   .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00   om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00   ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73   .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31   pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04   ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05   ........ ........
0100  02 04 02 02 02                                     .....
```

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

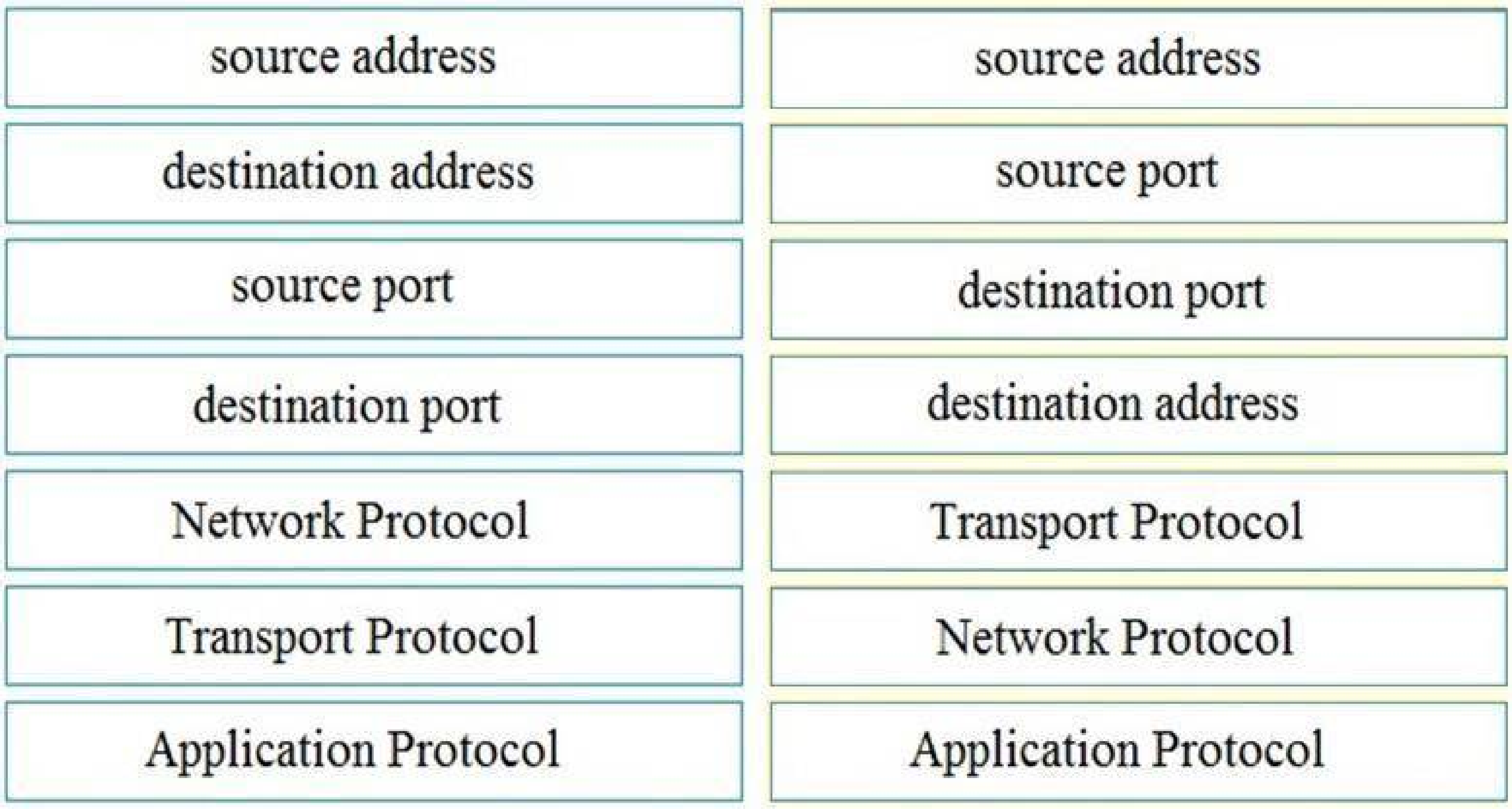


source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

NEW QUESTION 94
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

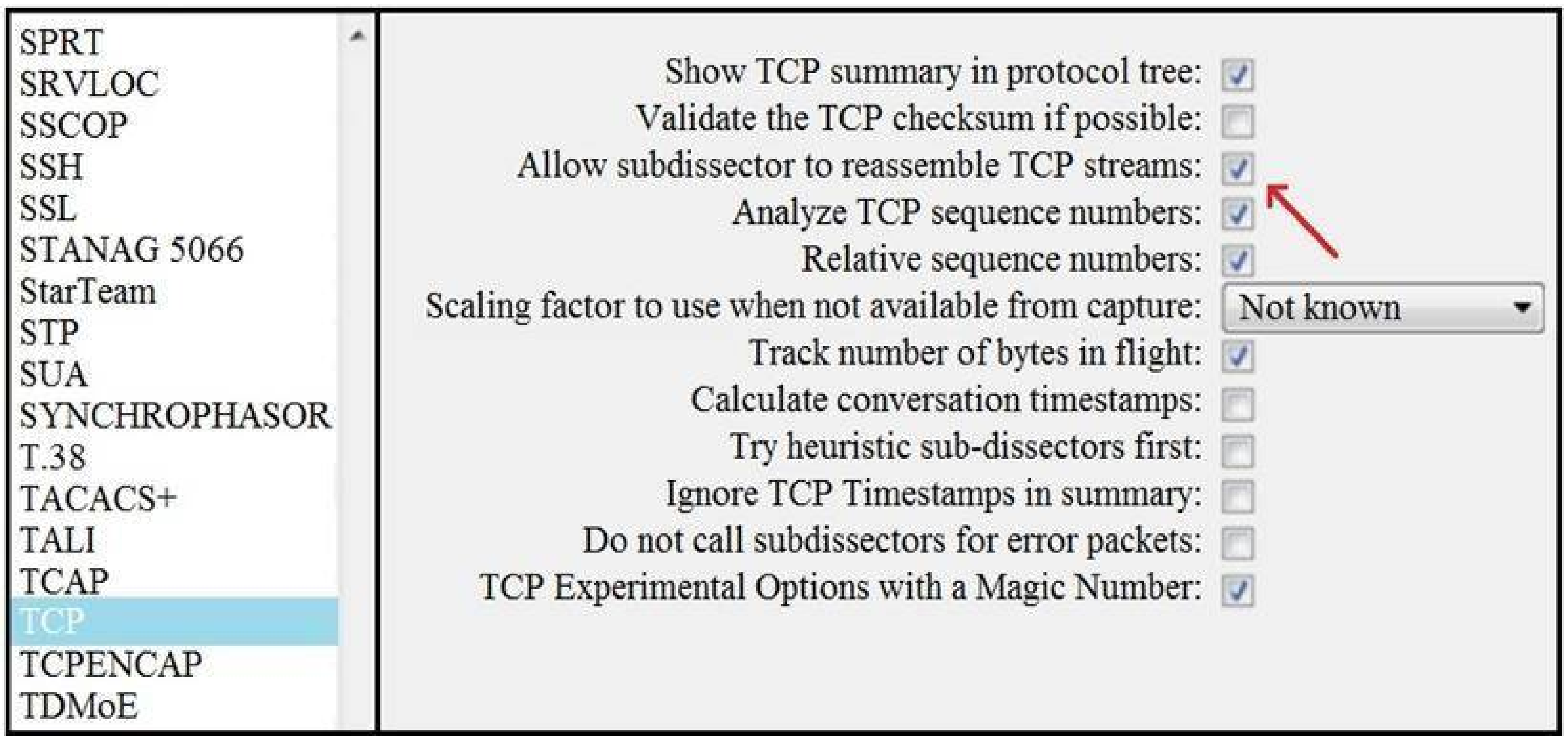
Answer: D

NEW QUESTION 95
How is attacking a vulnerability categorized?

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

Answer: C

NEW QUESTION 99
Refer to the exhibit.



SPRT
SRVLOC
SSCOP
SSH
SSL
STANAG 5066
StarTeam
STP
SUA
SYNCHROPHASOR
T.38
TACACS+
TALI
TCAP
TCP
TCPENCAP
TDMoE

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

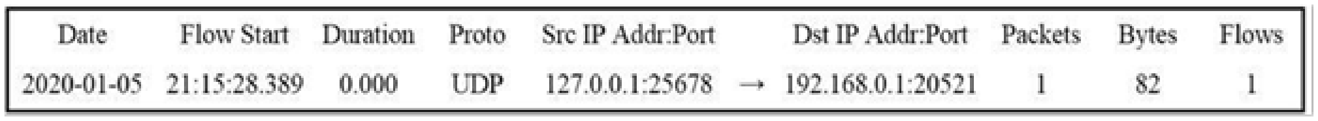
Answer: D

NEW QUESTION 100
How does an attacker observe network traffic exchanged between two users?

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

Answer: B

NEW QUESTION 105
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

NEW QUESTION 110
Which action prevents buffer overflow attacks?

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

Answer: C

NEW QUESTION 112
Which IETF standard technology is useful to detect and analyze a potential security incident by recording session flows that occurs between hosts?

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

Answer: D

NEW QUESTION 116
......

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

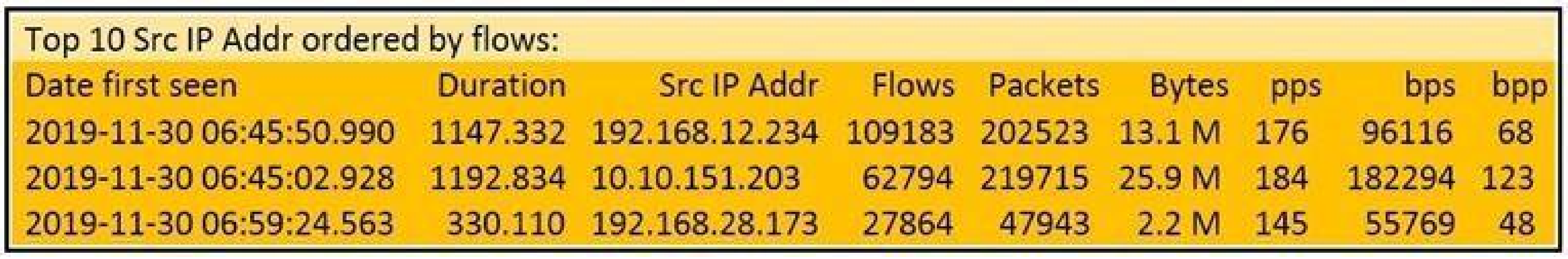
If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

A. syslog messages
B. full packet capture
C. NetFlow
D. firewall event logs

Answer: C

NEW QUESTION 2
Refer to the exhibit.



Top 10 Src IP Addr ordered by flows:

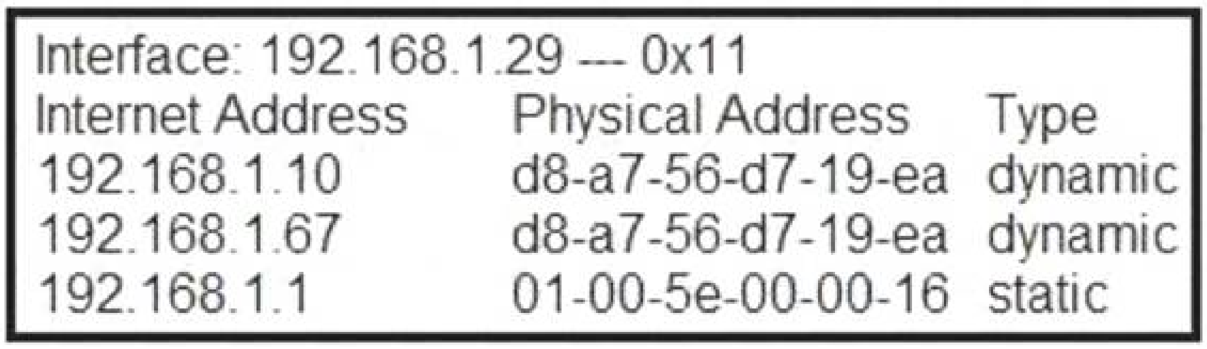
Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

What information is depicted?

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

Answer: B

NEW QUESTION 3
Refer to the exhibit.



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

What is occurring in this network?

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

Answer: A

NEW QUESTION 4
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

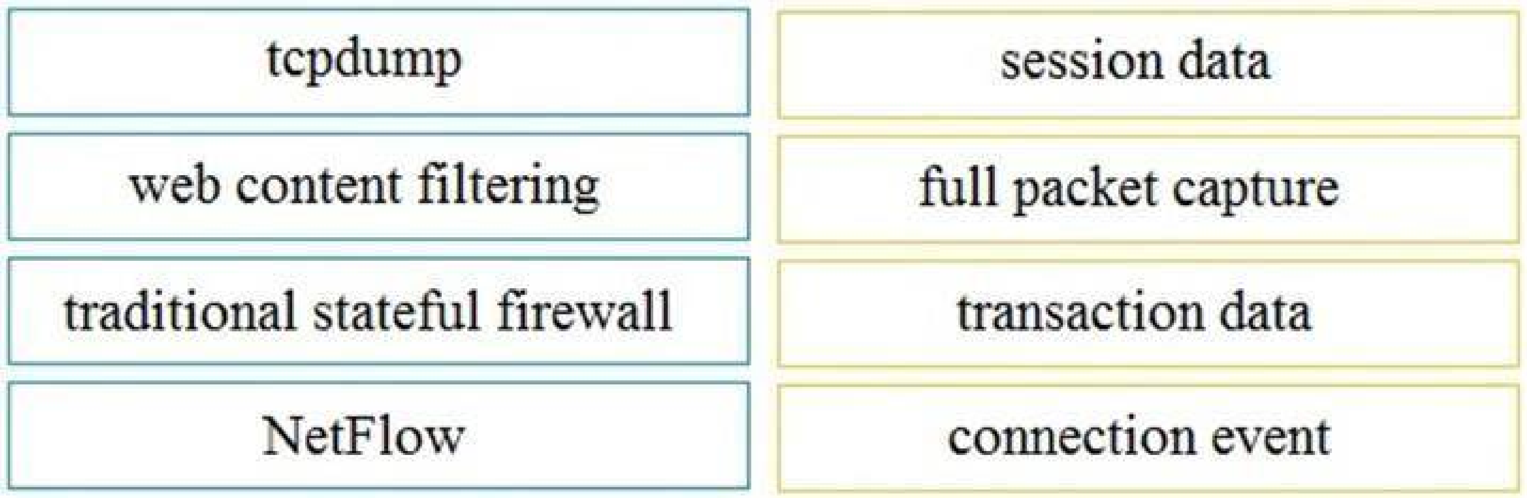
Answer: B

NEW QUESTION 5
Which process is used when IPS events are removed to improve data integrity?

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

Answer: B

NEW QUESTION 6
Drag and drop the technology on the left onto the data type the technology provides on the right.

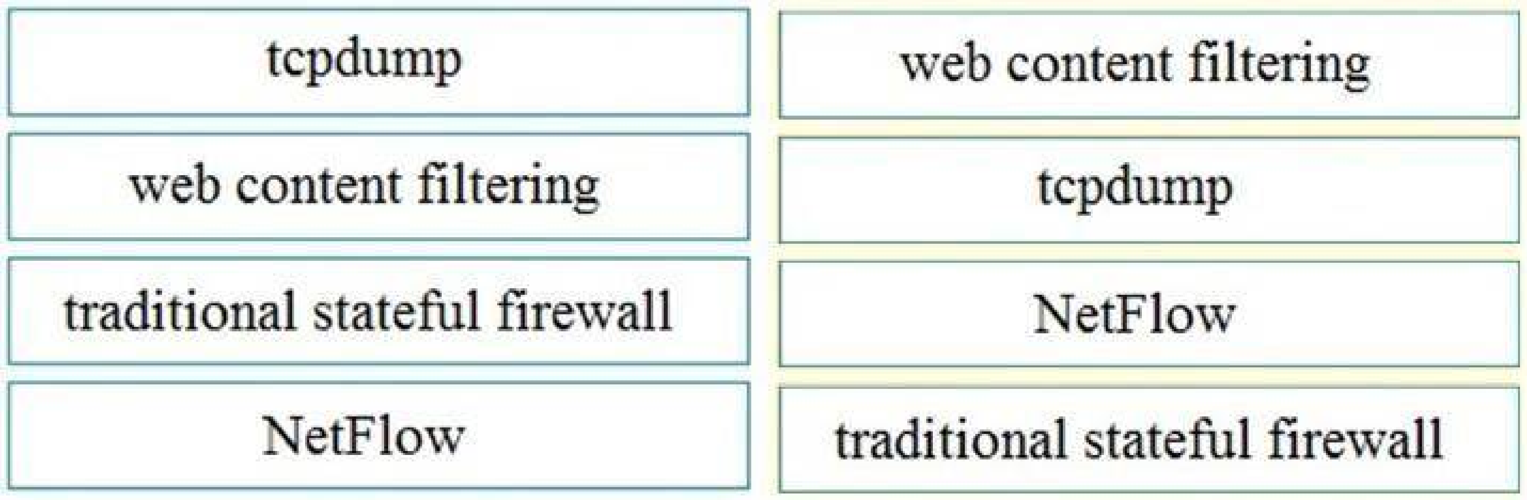


tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

A. Mastered
B. Not Mastered

Answer: A

Explanation:



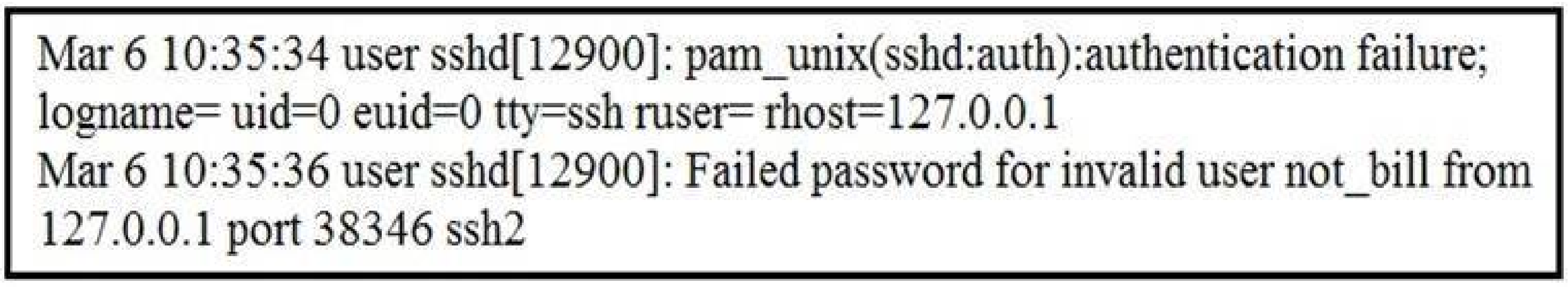
tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

NEW QUESTION 7
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: AB

NEW QUESTION 8
Refer to the exhibit.



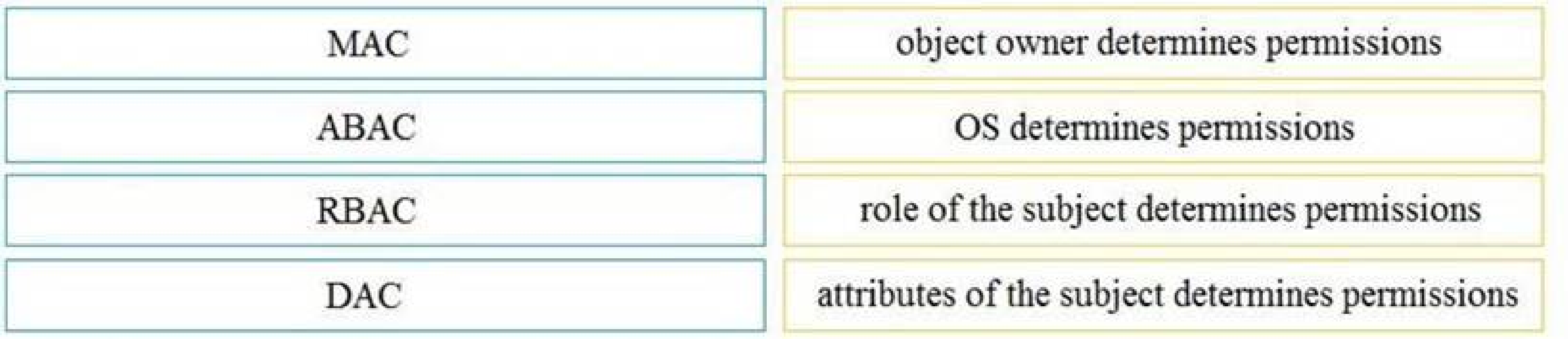
```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

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

NEW QUESTION 9
Drag and drop the access control models from the left onto the correct descriptions on the right.

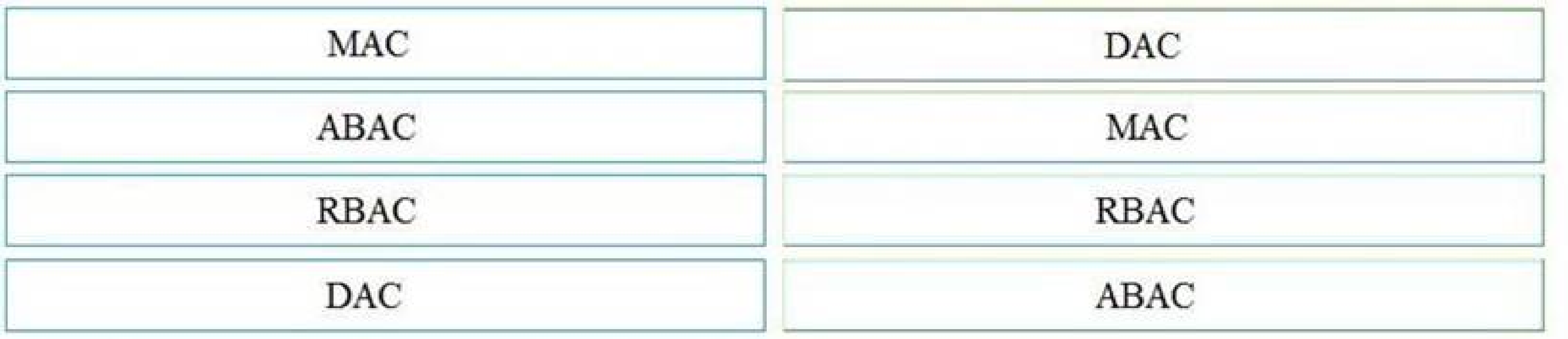


MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

A. Mastered
B. Not Mastered

Answer: A

Explanation:



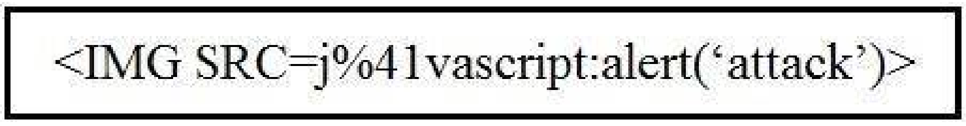
MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

NEW QUESTION 10
Which category relates to improper use or disclosure of PII data?

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

Answer: C

NEW QUESTION 10
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

NEW QUESTION 15
Which incidence response step includes identifying all hosts affected by an attack'?

A. post-incident activity
B. detection and analysis
C. containment eradication and recovery
D. preparation

Answer: A

NEW QUESTION 16
Which attack method intercepts traffic on a switched network?

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

Answer: C

NEW QUESTION 19

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

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

Answer: A

NEW QUESTION 23
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

NEW QUESTION 25
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

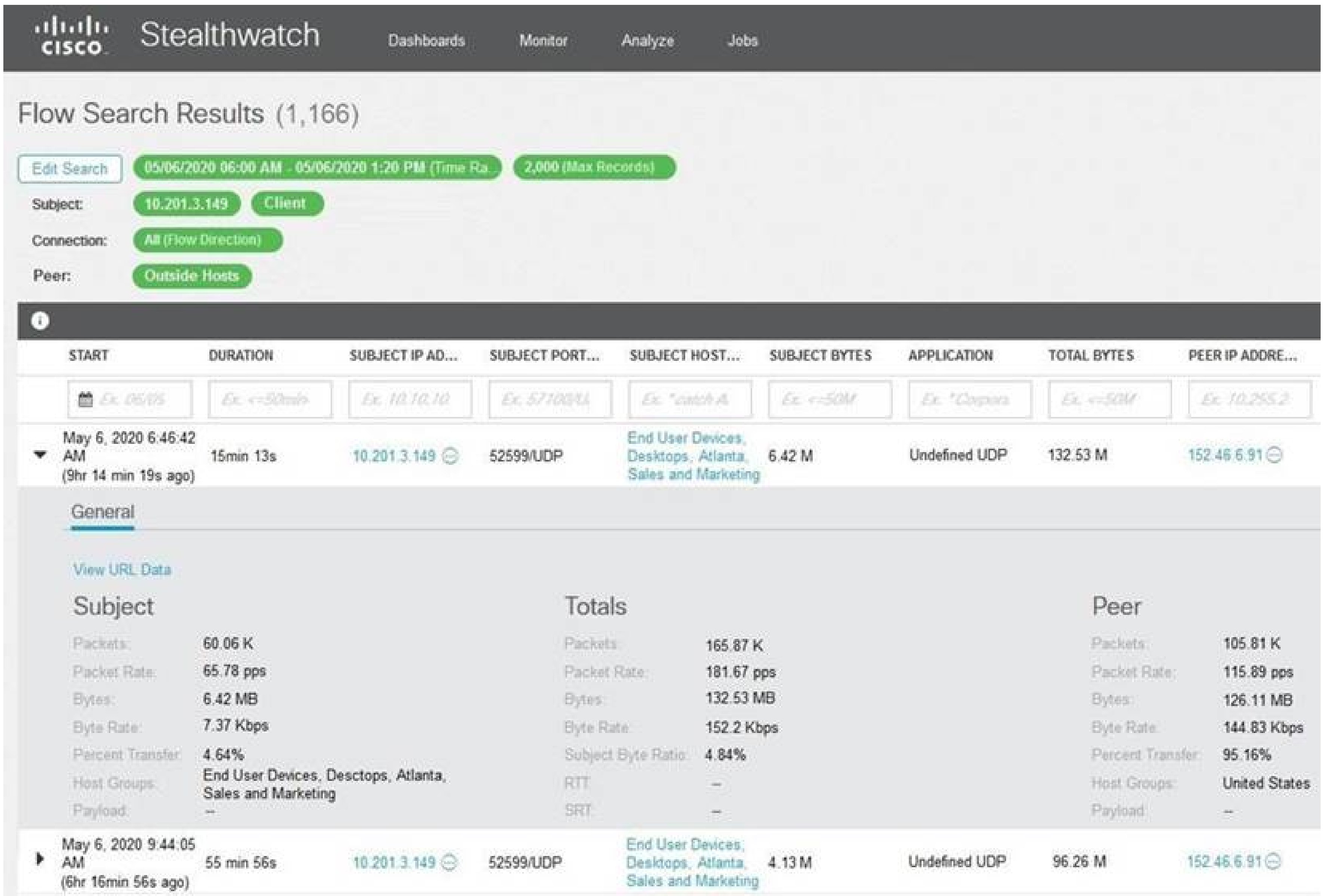
Answer: B

NEW QUESTION 27
Which metric is used to capture the level of access needed to launch a successful attack?

A. privileges required
B. user interaction
C. attack complexity
D. attack vector

Answer: A

NEW QUESTION 28
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...
Ex. 06/05	Ex. <=50min	Ex. 10.10.10	Ex. 57100/U...	Ex. *catch A	Ex. <=50M	Ex. *Corpora	Ex. <=50M	Ex. 10.255.2
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

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:	--

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDRE...
May 6, 2020 9:44:05 AM (6hr 16min 56s ago)	55 min 56s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	4.13 M	Undefined UDP	96.26 M	152.46.6.91

What is the potential threat identified in this Stealthwatch dashboard?

A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.

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

Answer: D

NEW QUESTION 30
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

NEW QUESTION 34
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. integrity
B. confidentiality
C. availability
D. scope

Answer: A

NEW QUESTION 36
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

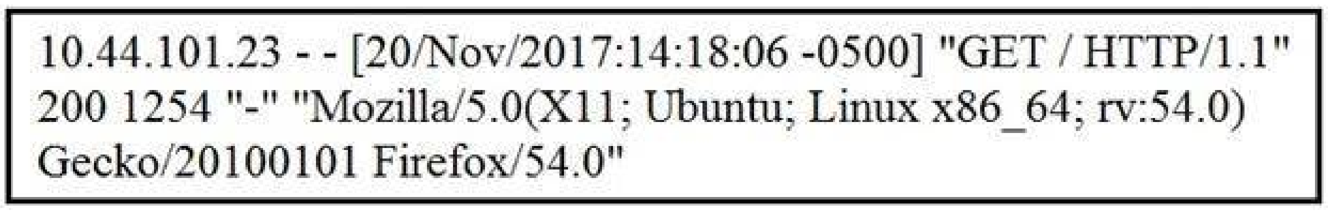
Answer: D

NEW QUESTION 39
A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

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

Answer: C

NEW QUESTION 42
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

NEW QUESTION 46
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

NEW QUESTION 49

What makes HTTPS traffic difficult to monitor?

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

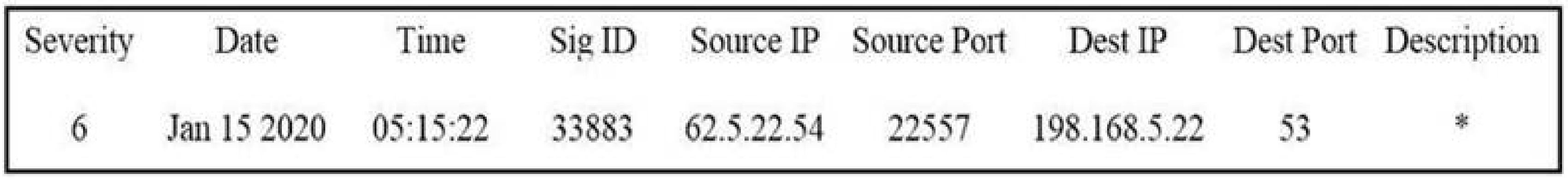
Answer: D

NEW QUESTION 54
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

NEW QUESTION 59
Refer to the exhibit.



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

Which type of log is displayed?

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

Answer: D

NEW QUESTION 64
What is an attack surface as compared to a vulnerability?

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

Answer: B

NEW QUESTION 66
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: CD

NEW QUESTION 68
What does cyber attribution identify in an investigation?

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

Answer: B

NEW QUESTION 69
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

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

Answer: B

NEW QUESTION 74
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: DE

NEW QUESTION 79
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

NEW QUESTION 82
Which security technology allows only a set of pre-approved applications to run on a system?

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

Answer: C

NEW QUESTION 84
A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?

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

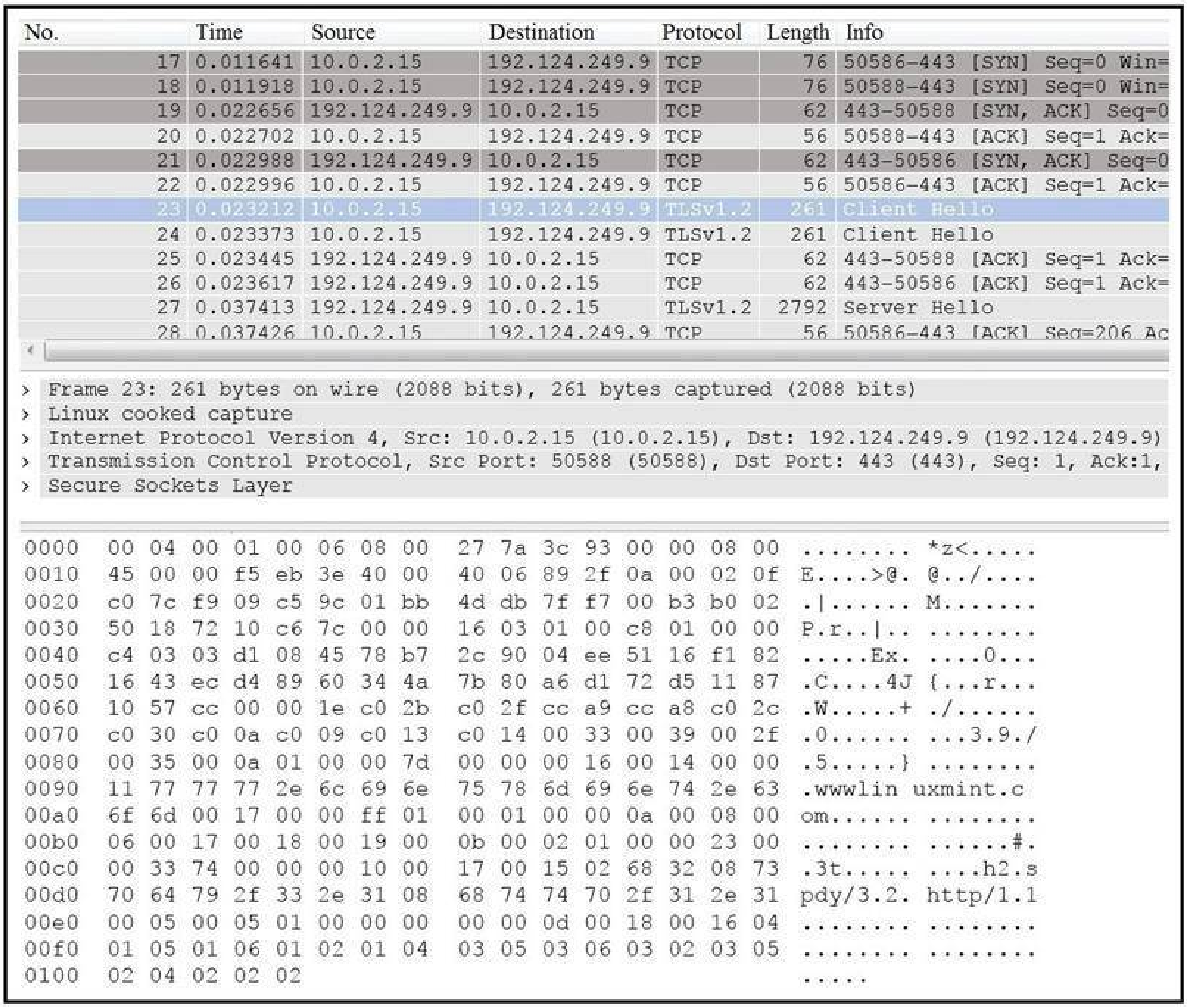
Answer: D

NEW QUESTION 87
An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

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

Answer: C

NEW QUESTION 92
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. ....Q...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87   .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c   .W.....+ ./.....,
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f   .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00   .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63   .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00   om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00   ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73   .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31   pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04   ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05   ........ ........
0100  02 04 02 02 02                                     .....
```

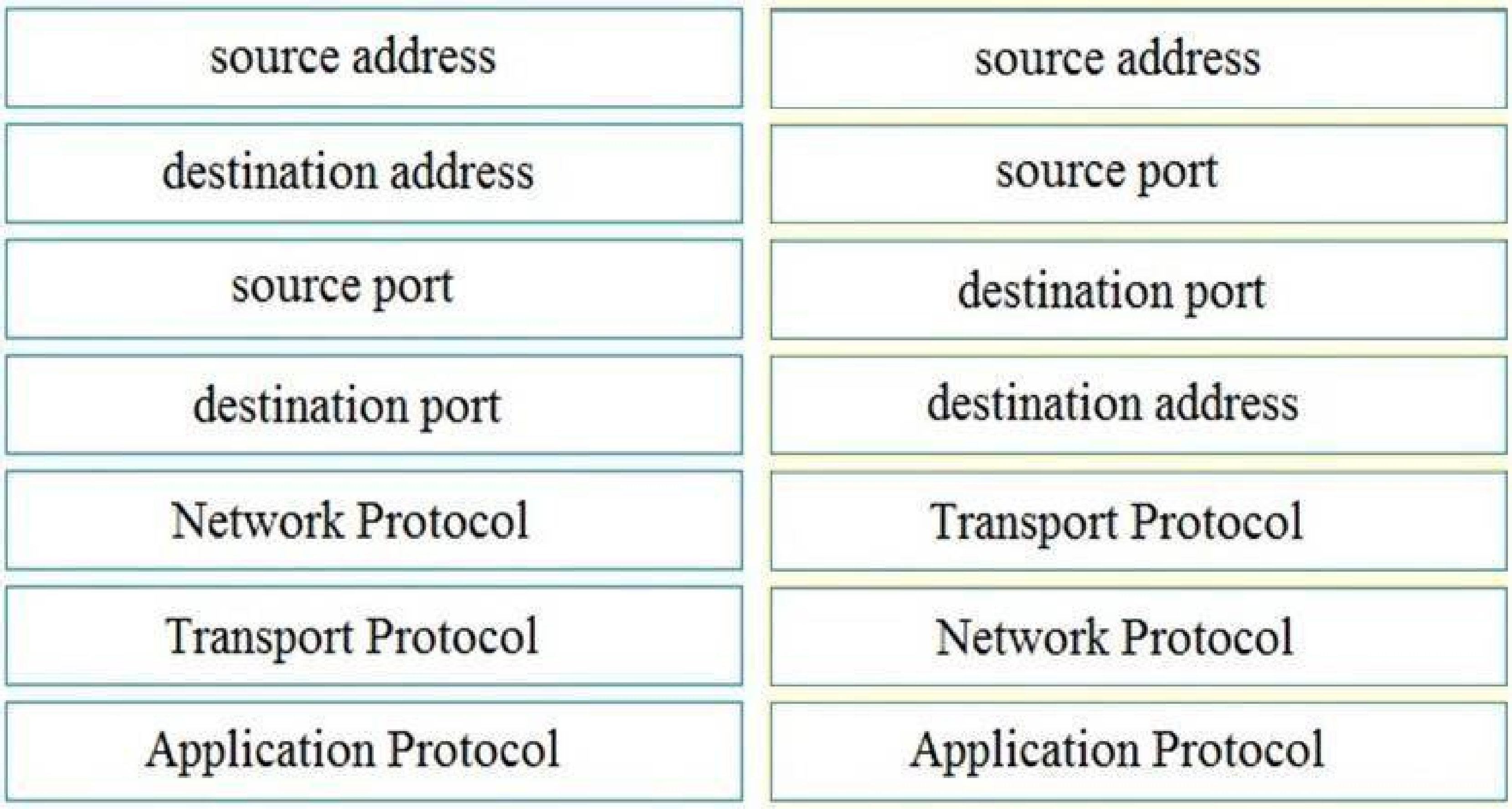
Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

NEW QUESTION 94
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

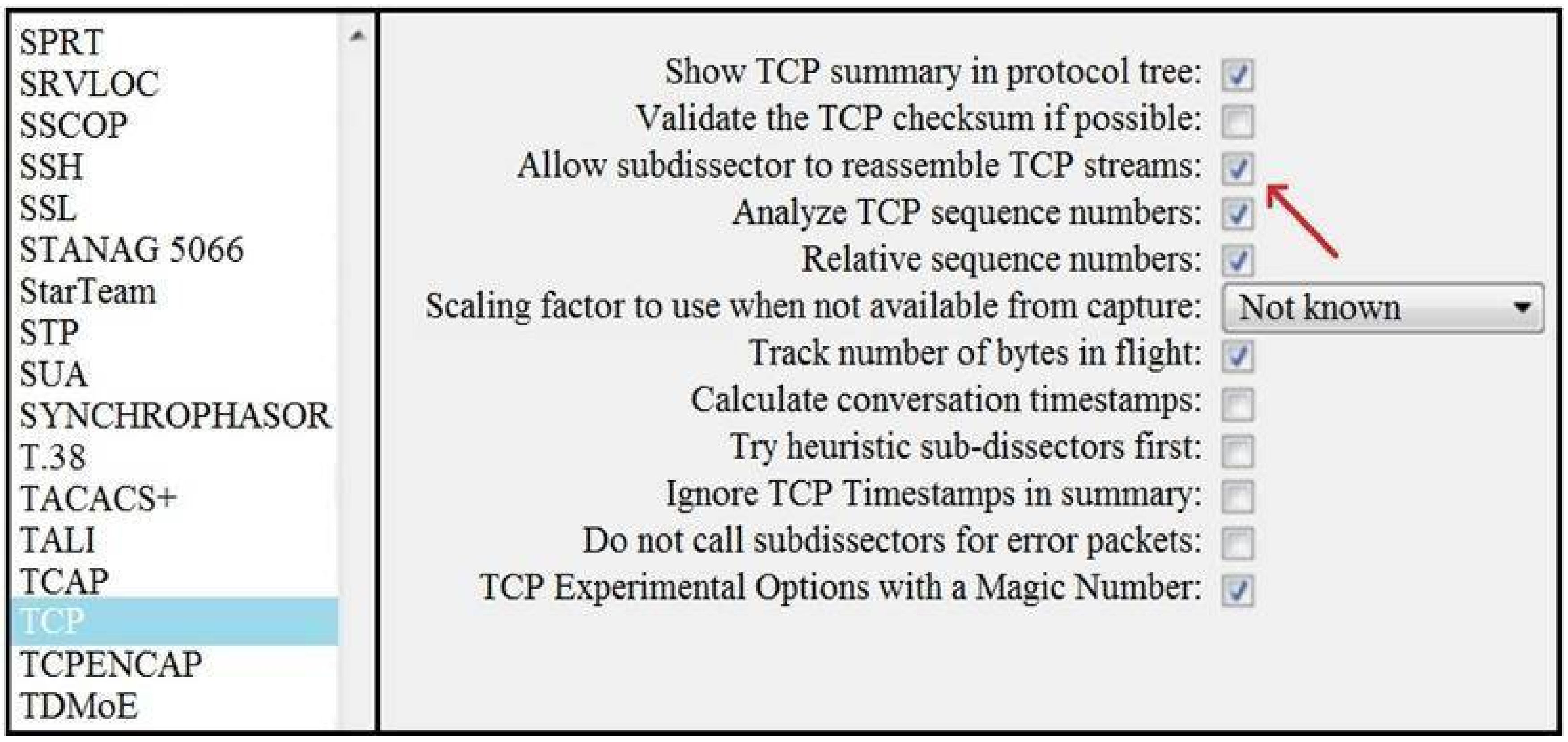
Answer: D

NEW QUESTION 95
How is attacking a vulnerability categorized?

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

Answer: C

NEW QUESTION 99
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

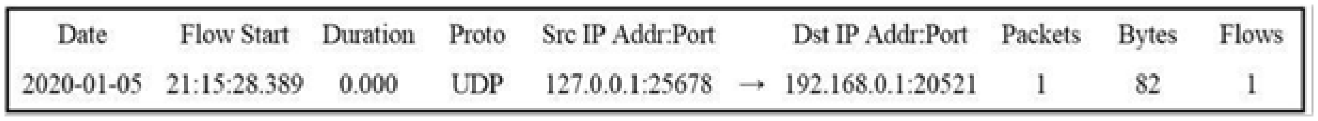
Answer: D

NEW QUESTION 100
How does an attacker observe network traffic exchanged between two users?

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

Answer: B

NEW QUESTION 105
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

NEW QUESTION 110
Which action prevents buffer overflow attacks?

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

Answer: C

NEW QUESTION 112
Which IETF standard technology is useful to detect and analyze a potential security incident by recording session flows that occurs between hosts?

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

Answer: D

NEW QUESTION 116
......

Relate Links

100% Pass Your 200-201 Exam with Exambible Prep Materials

https://www.exambible.com/200-201-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/