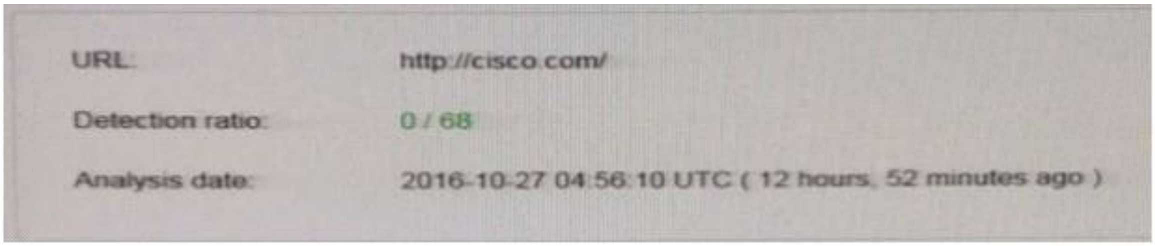
Vendor: Cisco

Exam Code: 210-255

Exam Name: Implementing Cisco Cybersecurity Operations (SECOPS)

Version: Demo

QUESTION 1
Refer to the exhibit. We have performed a malware detection on the Cisco website. Which statement about the result is true?



URL:	http://cisco.com/
Detection ratio:	0 / 68
Analysis date:	2016-10-27 04:56:10 UTC (12 hours, 52 minutes ago)

A. The website has been marked benign on all 68 checks.
B. The threat detection needs to run again.
C. The website has 68 open threats.
D. The website has been marked benign on 0 checks.

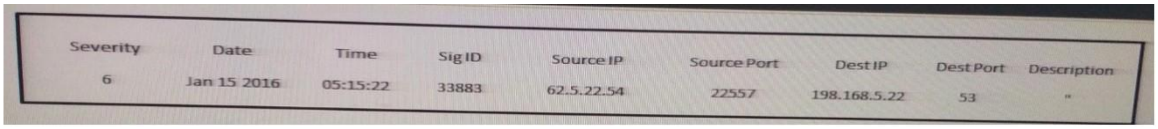
Correct Answer: A

QUESTION 2
Which information must be left out of a final incident report?

A. server hardware configurations
B. exploit or vulnerability used
C. impact and/or the financial loss
D. how the incident was detected

Correct Answer: B

QUESTION 3
Refer to the exhibit. Which type of log is this an example of?

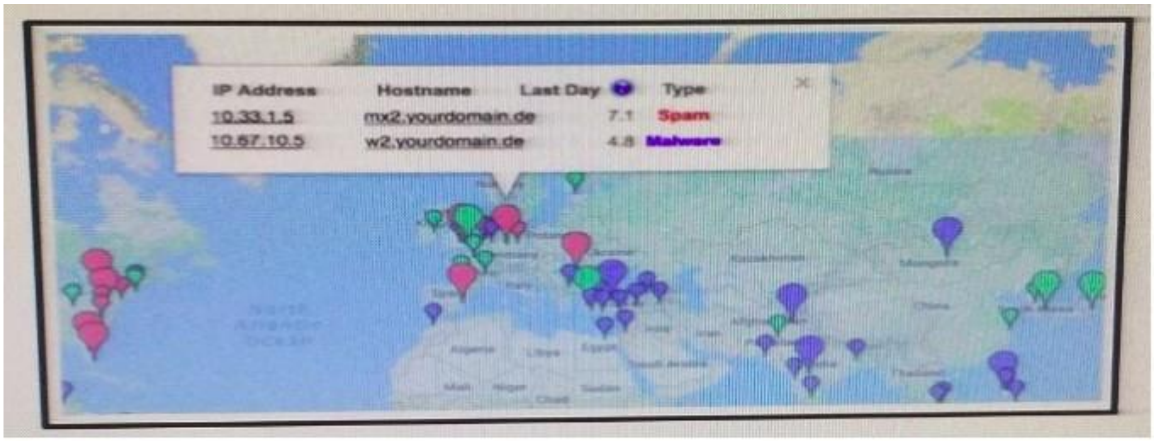


Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2016	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	"

A. syslog
B. NetFlow log
C. proxy log
D. IDS log

Correct Answer: A

QUESTION 4
Refer to the Exhibit. A customer reports that they cannot access your organization's website. Which option is a possible reason that the customer cannot access the website?



IP Address	Hostname	Last Day	Type
10.33.1.5	mx2.yourdomain.de	7.1	Spam
10.67.10.5	w2.yourdomain.de	4.8	Malware

A. The server at 10.33.1.5 is using up too much bandwidth causing a denial- of-service.
B. The server at 10.67.10.5 has a virus.
C. A vulnerability scanner has shown that 10.67.10.5 has been compromised.
D. Web traffic sent from 10.67.10.5 has been identified as malicious by Internet sensors.

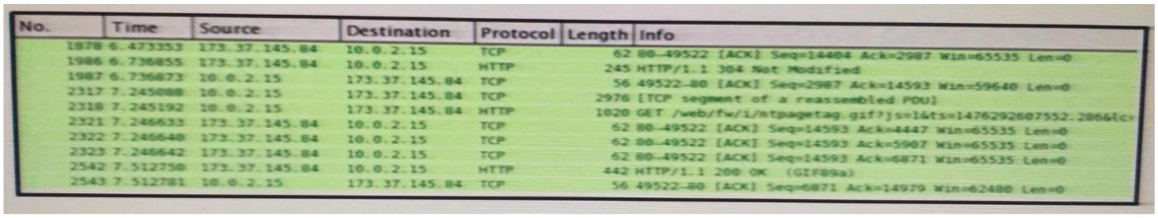
Correct Answer: C

QUESTION 5
Which CVSSv3 metric captures the level of access that is required for a successful attack?

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

Correct Answer: C

QUESTION 6
Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?



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=1476292607552.286&lc=
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

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

Correct Answer: D

QUESTION 7
Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?

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

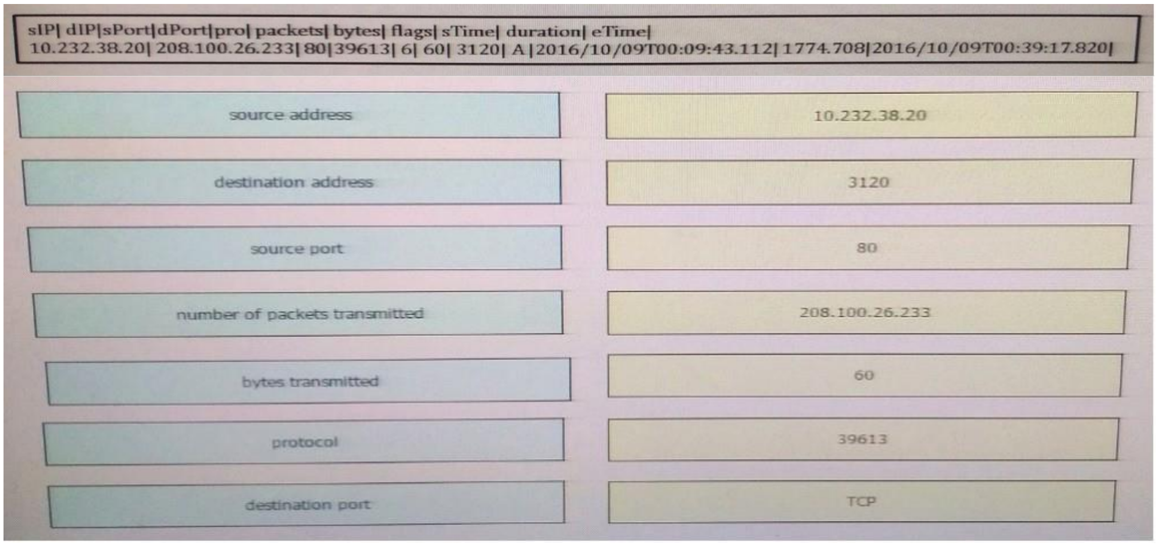
Correct Answer: A

QUESTION 8
What mechanism does the Linux operating system provide to control access to files?

A. privileges required
B. user interaction
C. file permissions
D. access complexity

Correct Answer: C

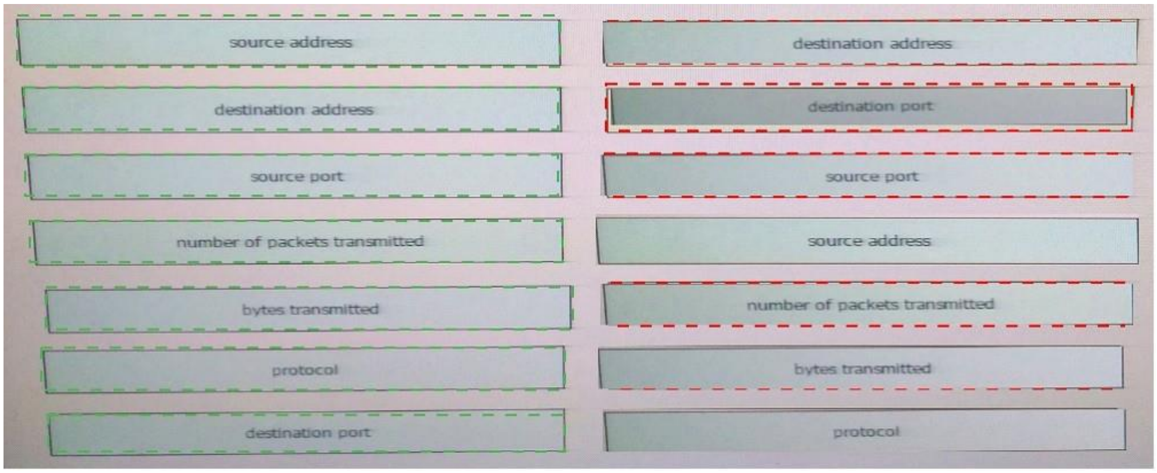
QUESTION 9
DRAG DROP
Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the NetFlow v5 record from a security event on the right.



```
sIP| dIP|sPort|dPort|pro| packets| bytes| flags| sTime| duration| eTime|
10.232.38.20| 208.100.26.233| 80|39613| 6| 60| 3120| A|2016/10/09T00:09:43.112| 1774.708|2016/10/09T00:39:17.820|
```

source address	10.232.38.20
destination address	3120
source port	80
number of packets transmitted	208.100.26.233
bytes transmitted	60
protocol	39613
destination port	TCP

Correct Answer:



source address	destination address
destination address	destination port
source port	source port
number of packets transmitted	source address
bytes transmitted	number of packets transmitted
protocol	bytes transmitted
destination port	protocol

QUESTION 10
Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?

A. local
B. physical
C. network
D. adjacent

Correct Answer: D

QUESTION 11
Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?

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

Correct Answer: A

QUESTION 12
In the context of incident handling phases, which two activities fall under scoping? (Choose two.)

A. determining the number of attackers that are associated with a security incident
B. ascertaining the number and types of vulnerabilities on your network
C. identifying the extent that a security incident is impacting protected resources on the network
D. determining what and how much data may have been affected
E. identifying the attackers that are associated with a security incident

Correct Answer: DE