



Following questions are built on a combination of multiple dumps  
The dump was updated by Oz Said on 7 June 2018. Total number of questions is 125.

**QUESTION 1**

Which data element must be protected with regards to PCI?

- A. past health condition
- B. geographic location
- C. full name / full account number
- D. recent payment amount

**Correct Answer: C**

**QUESTION 2**

What is Data mapping used for? (Choose two)

- A. data accuracy(integrity)
- B. data availability
- C. data normalization
- D. data confidentiality
- E. data visualization

**Correct Answer: AE**

**QUESTION 3**

Drag and drop the type of evidence from the left onto the correct description(s) of that evidence on the right.

direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

**Correct Answer:**

Corroborative evidence – NetFlow based spike in DNS traffic

Indirect evidence – firewall log showing successful communication and threat intelligence stating an IP is known to host malware

Direct evidence – log that shows a command and control check-in from verified malware

#### **QUESTION 4**

Which of the following steps in the kill chain would come before the others?

- A. C2
- B. Delivery
- C. Installation
- D. Exploitation

**Correct Answer: B**

#### **QUESTION 5**

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**

#### **QUESTION 6**

What does the CSIRT incident response provider usually do?

- A. provide incident handling services to their parent organization.
- B. provide incident handling services to a country
- C. coordinate and facilitate the handling of incidents across various CSIRTs
- D. focus on synthesizing data from various sources to determine trends and patterns in incident activity
- E. handle reports of vulnerabilities in their software or hardware products
- F. offer incident handling services as a for-fee service to other organizations

**Correct Answer: F**

#### **QUESTION 7**

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

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

**Correct Answer: A**

**QUESTION 8**

According to NIST what option is unnecessary for containment strategy?

- A. The delayed containment
- B. Monitoring with methods other than sandboxing

**Correct Answer: AB**

**QUESTION 9**

What is the difference between deterministic and probabilistic assessment method?

- A. At deterministic method we know the facts beforehand and at probabilistic method we make assumptions
- B. At probabilistic method we know the facts beforehand and at deterministic method we make assumptions
- C. Probabilistic method has an absolute nature
- D. Deterministic method has an absolute nature

**Correct Answer: AD**

**QUESTION 10**

In Microsoft Windows, as files are deleted the space they were allocated eventually is considered available for use by other files. This creates alternating used and unused areas of various sizes. What is this called?

- A. network file storing
- B. free space fragmentation
- C. alternate data streaming
- D. defragmentation

**Correct Answer: B**

**QUESTION 11**

When performing threat hunting against a DNS server, which traffic toward the affected domain is considered a starting point?

- A. HTTPS traffic
- B. TCP traffic
- C. HTTP traffic
- D. UDP traffic

**Correct Answer: D**

### QUESTION 12

Filtering ports in Wireshark?

- A. tcp.port == 80
- B. tcp port equals 80
- C. tcp.port 80
- D. port 80

**Correct Answer: A**

### QUESTION 13

What attribute belonging VERIS schema?

- A. confidentiality/possession
- B. integrity/authenticity
- C. availability/utility

**Correct Answer: ABC**

### QUESTION 14

Which of the following can be identified by correlating DNS intelligence and other security events? (Choose two)

- A. Communication to CnC servers
- B. Configuration issues
- C. Routing problems
- D. Malicious domain based on reputation

**Correct Answer: AD**

### QUESTION 15

A CMS plugin creates two files that are accessible from the Internet myplugin.html and exploitable.php. A newly discovered exploit takes advantage of an injection vulnerability in exploitable.php. To exploit the vulnerability, one must send an HTTP POST with specific variables to exploitable.php. You see traffic to your webserver that consists of only HTTP GET requests to myplugin.html. Which category best describes this activity?

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

**Correct Answer: B**

**QUESTION 16**

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: B**

**QUESTION 17**

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

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

**Correct Answer: A**

**QUESTION 18**

What is the definition of confidentiality according to CVSSv3 framework?

- A. This metric measures the impact to the confidentiality of the information resources that are managed by a software component due to a successfully exploited vulnerability.
- B. This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
- C. This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

**Correct Answer: A**

**QUESTION 19**

You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicious code is on an external site that is being visited by hosts on your network. Which user agent in the HTTP headers in the requests from your internal hosts warrants further investigation?

- A. Mozilla/5.0 (compatible, MSIE 10.0, Windows NT 6.2, Trident 6.0)
- B. Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805
- C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 400) Gecko/20100101
- D. Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16

**Correct Answer: A**

**QUESTION 20**

Which netstat command show ports?

- A. netstat -g
- B. netstat -l
- C. netstat -r
- D. netstat -v

**Correct Answer: B**

**QUESTION 21**

Which identifies both the source and destination location?

- A. IP address
- B. URL
- C. ports
- D. MAC address

**Correct Answer: A**

**QUESTION 22**

Which network device creates and sends the initial packet of a session?

- A. source
- B. origination
- C. destination
- D. network

**Correct Answer: A**

**QUESTION 23**

Which of the following is one of the main goals of the CSIRT?

- A. Configure the organization's firewall
- B. Monitor the organizations IPS devices
- C. Minimize and control the damage associated with incidents, provide guidance for mitigation and work to prevent future incidents
- D. Hire security professionals who will be part of the InfoSec team of the organization

**Correct Answer: C**

**QUESTION 24**

Which goal of data normalization is true?

- A. Reduce data redundancy.
- B. Increase data redundancy.
- C. Reduce data availability.
- D. Increase data availability

**Correct Answer: A**

**QUESTION 25**

Which of the following is not an example of reconnaissance?

- A. Searching the robots.txt file
- B. Redirecting users to a source and scanning traffic to learn about the target
- C. Scanning without completing the three-way handshake
- D. Communicating over social media

**Correct Answer: B**

**QUESTION 26**

From a security perspective, why is it important to employ a clock synchronization protocol on a network?

- A. so that everyone knows the local time
- B. to ensure employees adhere to work schedule
- C. to construct an accurate timeline of events when responding to an incident
- D. to guarantee that updates are pushed out according to schedule

**Correct Answer: C**

**QUESTION 27**

During which phase of the forensic process are tools and techniques used to extract the relevant information from the collective data?

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

**Correct Answer: A**

### QUESTION 28

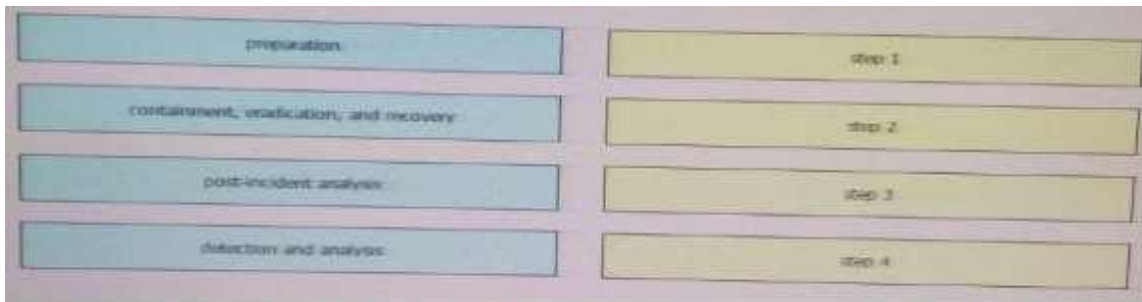
Which option allows a file to be extracted from a TCP stream within Wireshark?

- A. File > Export Objects
- B. Analyze > Extract
- C. Tools > Export > TCP
- D. View > Extract

**Correct Answer: A**

### QUESTION 29

Drag and drop the elements of incident handling from the left into the correct order on the right.



**Correct Answer:**

- 1-Preparation
- 2-Detection and analysis
- 3-Containment, eradication and recovery
- 4-Post incident analysis

### QUESTION 30

Which of the following is typically a responsibility of a PSIRT (Product SIRT)?

- A. Configure the organization's firewall
- B. Monitor security logs
- C. Investigate security incidents in a SOC
- D. Disclosure vulnerabilities in the organization's products and services

**Correct Answer: D**

### QUESTION 31

Which of the following is an example of a coordination center?

- A. Cisco PSIRT
- B. Microsoft MSRC
- C. CERT division of the SEI
- D. FIRST

**Correct Answer: C**



**QUESTION 32**

Choose the option that best describes NIST data integrity

- A. use only sha-1
- B. use only md5
- C. you must hash data & backup and compare hashes
- D. no need to hash data & backup and compare hashes

**Correct Answer: C**

**QUESTION 33**

What is NAC?

- A. Non-Admin Closure
- B. Network Access Control
- C. Nepal Airline Corporations
- D. Network Address Control

**Correct Answer: B**

**QUESTION 34**

Which of the following is not true about listening ports?

- A. A listening port is a port held open by a running application in order to accept inbound connections.
- B. Seeing traffic from a known port will identify the associated service.
- C. Listening ports use values that can range between 1 and 65535.
- D. TCP port 80 is commonly known for Internet traffic.

**Correct Answer: B**

**QUESTION 35**

Which of the following are examples of some of the responsibility of a corporate CSIRT and the policies it helps create? (Choose four)

- A. Scanning vendor customer network
- B. incident classification and handling
- C. Information classification and protection
- D. Information dissemination
- E. Record retentions and destruction

**Correct Answer: BCDE**

**QUESTION 36**

Which element is included in an incident response plan?

- A. organization mission
- B. junior analyst approval
- C. day-to-day firefighting
- D. siloed approach to communications

**Correct Answer: A**

**QUESTION 37**

Which option creates a display filter on Wireshark on a host IP address or name?

- A. `ip.address == <address> or ip.network == <network>`
- B. `[tcp|udp] ip.[src|dst] port <port>`
- C. `ip.addr == <addr> or ip.name == <name>`
- D. `ip.addr == <addr> or ip.host == <host>`

**Correct Answer: D**

**QUESTION 38**

Which type of analysis allows you to see how likely an exploit could affect your network?

- A. descriptive
- B. casual
- C. probabilistic
- D. inferential

**Correct Answer: C**

**QUESTION 39**

Which CSIRT category provides incident handling services to their parent organization such as a bank, a manufacturing company, a university, or a federal agency?

- A. internal CSIRT
- B. national CSIRT
- C. coordination centers
- D. analysis centers
- E. vendor teams
- F. incident response providers

**Correct Answer: A**

**QUESTION 40**

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

- A. col[0-9]+our
- B. colo?ur
- C. colou?r
- D. ]a-z]{7}

**Correct Answer: C**

**QUESTION 41**

Which element is part of an incident response plan?

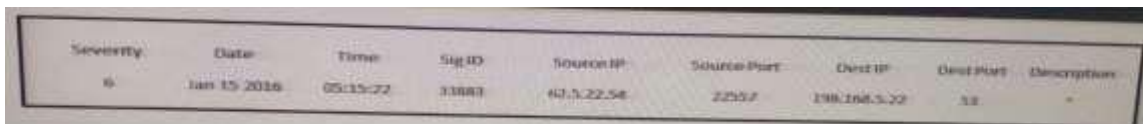
- A. organizational approach to incident response
- B. organizational approach to security
- C. disaster recovery
- D. backups

**Correct Answer: A**

**QUESTION 42**

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

Exhibit:



Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2016	05:15:22	33883	63.5.22.54	22557	198.168.5.22	52	-

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

**Correct Answer: D**

**QUESTION 43**

Based on nistsp800-61R2 what are the recommended protections against malware?

- A. Malware prevention software

**Correct Answer: A**

**QUESTION 44**

Which option can be addressed when using retrospective security techniques?

- A. if the affected host needs a software update
- B. how the malware entered our network
- C. why the malware is still in our network
- D. if the affected system needs replacement

**Correct Answer: B**

**QUESTION 45**

Which Security Operations Center's goal is to provide incident handling to a country?

- A. Coordination Center
- B. Internal CSIRT
- C. National CSIRT
- D. Analysis Center

**Correct Answer: C**

**QUESTION 46**

What protocol is related to NAC?

- A. 802.1Q
- B. 802.1X
- C. 802.1E
- D. 802.1F

**Correct Answer: B**

**QUESTION 47**

According to NIST what option(s) should be contained in issue tracking system?

- A. The current status of the incident
- B. A summary of the incident
- C. Indicators related to the incident
- D. Other incidents related to this incident
- E. Actions taken by all incident handlers on this incident
- F. Chain of custody, if applicable
- G. Impact assessments related to the incident
- H. Contact information for other involved parties (e.g., system owners, system administrators)
- I. A list of evidence gathered during the incident investigation
- J. Comments from incident handlers
- K. Next steps to be taken (e.g., rebuild the host, upgrade an application).

**Correct Answer:**  
ABCDEFGHIJK

**QUESTION 48**

According to NIST what option(s) should be contained in issue tracking system?

- A. inspect other incident related to the incident

**Correct Answer: A**

**QUESTION 49**

Which of the following make the file unique?

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

**Correct Answer: B**

**QUESTION 50**

Which of the following is one of the most used Linux file systems that has several improvements over its predecessors and that supports journaling?

- A. NTFS
- B. exFAT
- C. Ext5
- D. Ext4

**Correct Answer: D**

**QUESTION 51**

attacker using robots.txt is under which category?

- A. Reconnaissance
- B. Weaponization
- C. Delivery
- D. Exploitation
- E. Installation
- F. Command and control (C2)
- G. Actions on objectives

**Correct Answer: A**

**QUESTION 52**

What do the CSIRT incident analysis centers usually do?

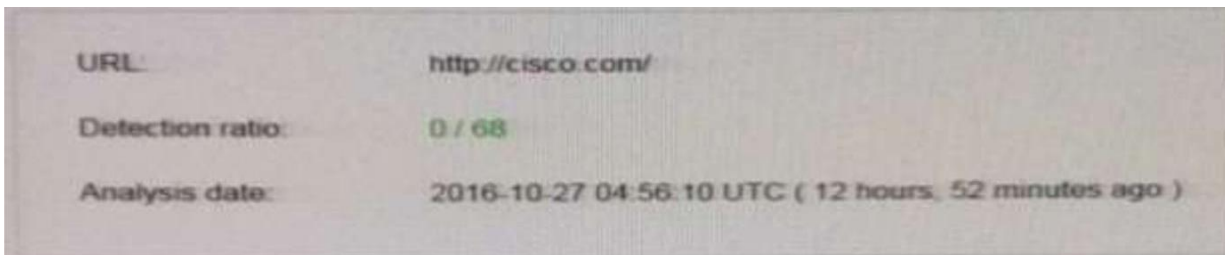
- A. provide incident handling services to their parent organization
- B. provide incident handling services to a country
- C. coordinate and facilitate the handling of incidents across various CSIRTs
- D. focus on synthesizing data from various sources to determine trends and patterns in incident activity
- E. handle reports of vulnerabilities in their software or hardware products
- F. offer incident handling services as a for-fee service to other organizations

**Correct Answer: D**

**QUESTION 53**

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

Exhibit:



- 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 54**

Which element can be used by a threat actor to discover a possible opening into a target network and can also be used by an analyst to determine the protocol of the malicious traffic?

- A. TTLs
- B. ports
- C. SMTP replies
- D. IP addresses

**Correct Answer: B**

**QUESTION 55**

Which option is a misuse variety per VERIS enumerations?

- A. snooping
- B. hacking
- C. theft
- D. assault

**Correct Answer: B**

**QUESTION 56**

A user on your network receives an email in their mailbox that contains a malicious attachment. There is no indication that the file was run. Which category as defined in the Kill-chain model does this activity fall under?

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

**Correct Answer: C**

**QUESTION 57**

What is the definition of integrity according to CVSSv3 framework?

- A. This metric measures the impact to the confidentiality of the information resources that are managed by a software component due to a successfully exploited vulnerability.
- B. This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
- C. This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

**Correct Answer: B**

**QUESTION 58**

Which of the following are not components of the 5-tuple of a flow in NetFlow? (Choose two)

- A. Source IP address
- B. Flow record ID
- C. Source port
- D. Gateway
- E. Destination port

**Correct Answer: BD**

**QUESTION 59**

Which netstat command show ports? (Choose two)

- A. netstat -a
- B. netstat -l
- C. netstat -v
- D. netstat -g

**Correct Answer: AB**

**QUESTION 60**

Which of the following is not an example of weaponization

- A. Connecting to a CnC server
- B. Wrapping software with a RAT
- C. Creating backdoor in an app
- D. Developing an automated script to inject commands on a USB device

**Correct Answer: A**

**QUESTION 61**

D&D: ASA outbound TCP connection from outside IPXX/port to inside IPXX/port , source/dest ip add/port

- A. question from ASA log to find the source and dest address,port.

**Correct Answer: A**

**QUESTION 62**

Refer to the following packet capture. Which of the following statements is true?

Exhibit:

```
00:00:04.549138 IP omar.cisco.com.34548 > 93.184.216.34.telnet:
Flags [S], seq 3152949738, win 29200,
options [mss 1460,sackOK,TS val 1193148797 ecr 0,nop,wscale 7], length 0
00:00:05.547084 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq
3152949738, win 29200,
options [mss 1460,sackOK,TS val 1193149047 ecr 0,nop,wscale 7], length 0
00:00:07.551078 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq
3152949738, win 29200,
options [mss 1460,sackOK,TS val 1193149548 ecr 0,nop,wscale 7], length 0
00:00:11.559081 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq
3152949738, win 29200,
options [mss 1460,sackOK,TS val 1193150550 ecr 0,nop,wscale 7], length 0
```

- A. The host with IP 93.184.216.34 is the source
- B. The host omar.cisco is the destination
- C. The server omar.cisco.com is responding to 93.184.216.34 with four packets
- D. This is a telnet transaction that is timing out and the server is not responding

**Correct Answer: D**



**QUESTION 63**

What information from HTTP logs can be used to find a threat actor?

- A. referrer
- B. IP address
- C. user-agent
- D. URL

**Correct Answer: B**

**QUESTION 64**

At which stage attacking the vulnerability belongs in Cyber kill chain?

- A. Reconnaissance
- B. Weaponization
- C. Delivery
- D. Exploitation
- E. Installation
- F. Command and control (C2)
- G. Actions on objectives

**Correct Answer: D**

**QUESTION 65**

Which statement about threat actors is true?

- A. They are any company assets that are threatened.
- B. They are any assets that are threatened.
- C. They are perpetrators of attacks.
- D. They are victims of attacks.

**Correct Answer: C**

**QUESTION 66**

Which of the following is not an example of the VERIS main schema categories?

- A. Incident tracking
- B. Victim demographics
- C. Incident descriptions
- D. Incident forensics ID

**Correct Answer: D**

**QUESTION 67**

Which stakeholder group is responsible for containment, eradication, and recovery in incident handling?

- A. facilitators
- B. practitioners
- C. leaders and managers
- D. decision makers

**Correct Answer: A**

**QUESTION 68**

What is accomplished in the identification phase of incident handling?

- A. determining the responsible user
- B. identifying source and destination IP addresses
- C. defining the limits of your authority related to a security event
- D. determining that a security event has occurred

**Correct Answer: D**

**QUESTION 69**

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: C**

**QUESTION 70**

Which string matches the regular expression  $r(ege)^+x$ ?

- A. rx
- B. regeegex
- C. r(ege)x
- D. rege+x

**Correct Answer: B**

**QUESTION 71**

What is the definition of availability accord to CVSSv3 framework?

- A. This metric measures the impact to the confidentiality of the information resources that are managed by a software component due to a successfully exploited vulnerability.
- B. This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
- C. This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

**Correct Answer: C**

**QUESTION 72**

In addition to cybercrime and attacks, evidence found on a system or network may be presented in a court of law to support accusations of crime or civil action, including which of the following?

- A. Fraud, money laundering, and theft
- B. Drug-related crime
- C. Murder and acts of violence
- D. All of the above

**Correct Answer: D**

**QUESTION 73**

Which of the following is an example of a managed security offering where incident response experts monitor and respond to security alerts in a SOC?

- A. Cisco CloudLock
- B. Cisco's Active Threat Analytics (ATA)
- C. Cisco Managed Firepower Service
- D. Cisco Jasper

**Correct Answer: B**

**QUESTION 74**

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: A**

### QUESTION 75

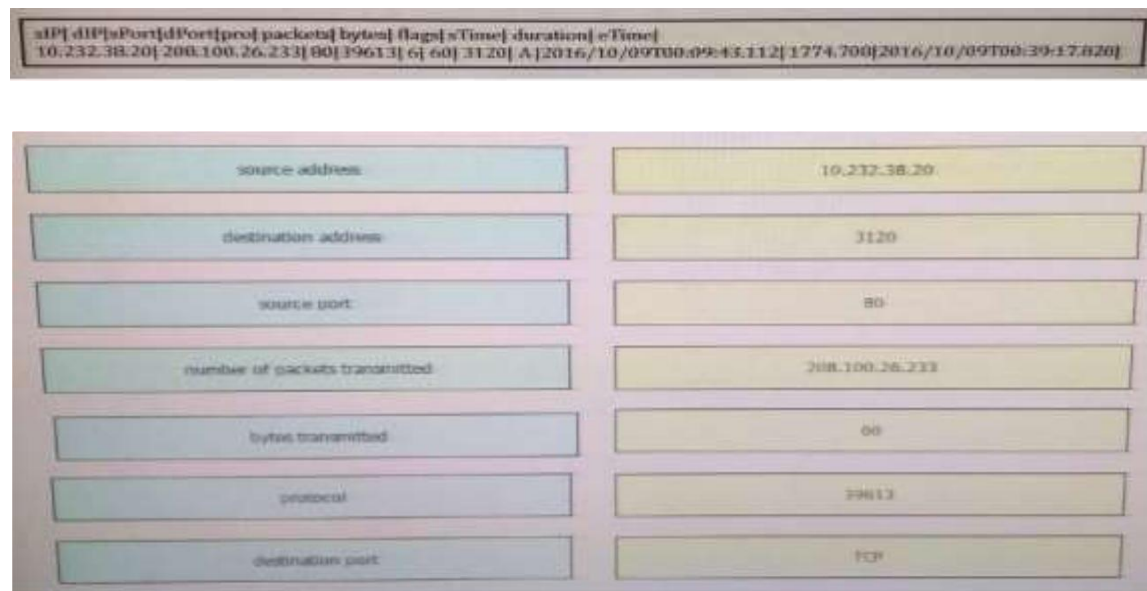
Which two components are included in a 5-tuple? (Choose two.)

- A. port number
- B. destination IP address
- C. data packet
- D. user name
- E. host logs

**Correct Answer: AB**

### QUESTION 76

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.



The exhibit shows a NetFlow v5 record and a drag-and-drop interface. The record is a single line of text: `sIP|dIP|sPort|dPort|prot|packets|bytes|flags|sTime|duration|eTime|` followed by the values: `10.232.38.20|208.100.26.233|80|39613|6|3120|A|2016/10/09T00:09:43.112|1774.700|2016/10/09T00:39:17.820|`. Below this, there is a table with two columns. The left column contains labels for the fields in the record, and the right column contains the corresponding values from the record.

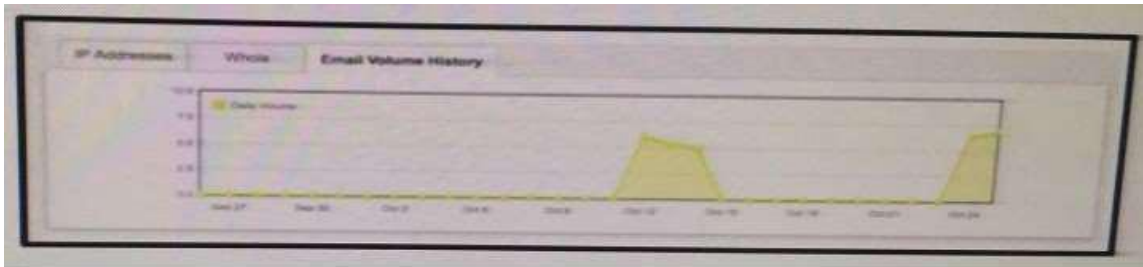
Field Label	Value
source address	10.232.38.20
destination address	3120
source port	80
number of packets transmitted	208.100.26.233
bytes transmitted	60
protocol	39613
destination port	TCP

**Correct Answer:**

- 10.232.38.20 – Source address
- 3120 - Bytes transmitted
- 80 - Source port
- 208.100.26.233 - Destination address
- 60 - Number of packets
- 39613 - Destination port
- TCP – Protocol

### QUESTION 77

Refer to the exhibit. You notice that the email volume history has been abnormally high. Which potential result is true?

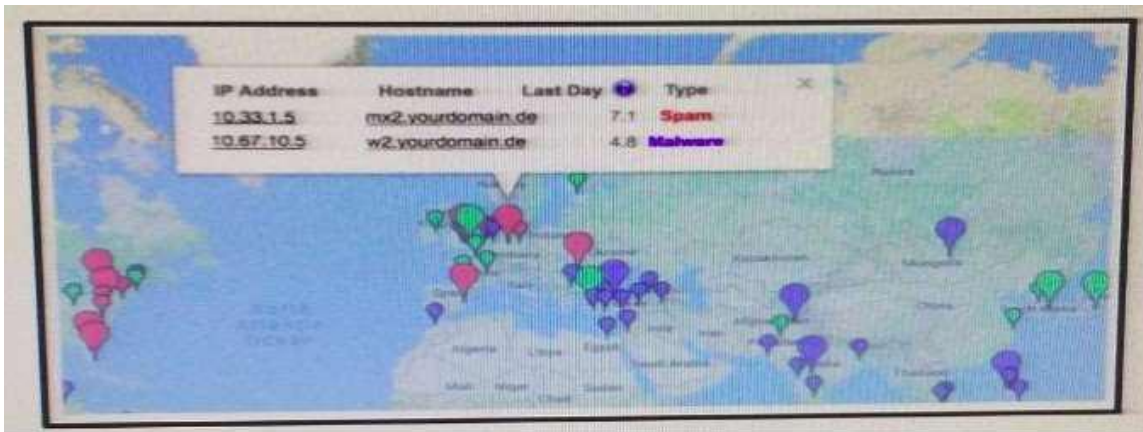


- A. Email sent from your domain might be filtered by the recipient.
- B. Messages sent to your domain may be queued up until traffic dies down.
- C. Several hosts in your network may be compromised.
- D. Packets may be dropped due to network congestion.

**Correct Answer: C**

### QUESTION 78

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?



- 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: D**

**QUESTION 79**

Which of the following are core responsibilities of a national CSIRT and CERT?

- A. Provide solutions for bug bounties
- B. Provide vulnerability brokering to vendors within a country
- C. Protect their citizens by providing security vulnerability info, security awareness training, best practices, and other info
- D. Create regulations around cybersecurity within the country

**Correct Answer: C**

**QUESTION 80**

Which of the following are the three broad categories of cybersecurity investigations?

- A. Public, private, and individual investigations
- B. Judiciary, private, and individual investigations
- C. Public, private, and corporate investigations
- D. Government, corporate, and private investigations

**Correct Answer: A**

**QUESTION 81**

Which component of the NIST SP800-61 r2 incident handling strategy reviews data?

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

**Correct Answer: D**

**QUESTION 82**

Which of the following has been used to evade IDS / IPS devices?

- A. SNMP
- B. HTTP
- C. TNP
- D. Fragmentation

**Correct Answer: D**

**QUESTION 83**

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: B**

**QUESTION 84**

Which description of a retrospective malware detection is true?

- A. You use Wireshark to identify the malware source.
- B. You use historical information from one or more sources to identify the affected host or file.
- C. You use information from a network analyzer to identify the malware source.
- D. You use Wireshark to identify the affected host or file.

**Correct Answer: B**

**QUESTION 85**

What is the process of remediation the system from attack so that responsible threat actor can be revealed?

- A. Validating the Attacking Host's IP Address
- B. Researching the Attacking Host through Search Engines.
- C. Using Incident Databases.
- D. Monitoring Possible Attacker Communication Channels.

**Correct Answer: ABCD**

**QUESTION 86**

Which of the following is not a metadata feature of the Diamond Model?

- A. Direction
- B. Result
- C. Devices
- D. Resources

**Correct Answer: C**

### QUESTION 87

Which of the following is one of the main goals of data normalization?

- A. To save duplicate logs for redundancy
- B. To purge redundant data while maintaining data integrity
- C. To correlate IPS and IDS logs with DNS
- D. To correlate IPS and IDS logs with Firewall logs

**Correct Answer: B**

### QUESTION 88

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

No.	Time	Source	Destination	Protocol	Length	Info
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50580 [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	56	50588-443 [ACK] Seq=1
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	50588-443 [ACK] Seq=1

Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)  
 Linux cooked capture  
 Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)  
 Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, Ack: 443  
 Data (205 bytes)  
 Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...  
 [Length: 205]

```

0000  00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00 .....Zc....
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.F...|.....
0040  c4 03 03 0e 06 ea 0d 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..B..E..
0060  8b 6e f8 00 00 1e c0 2b c0 2f cc a9 cc a8 c0 2c .@.....+.../.
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 .S.....}.....
0090  11 77 77 72 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63 www.lin-uxmint.c
00a0  6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 08 00 om.....#.....
00b0  0e 00 17 00 18 00 19 00 0b 00 02 01 00 00 23 00 .....#.....
00c0  00 32 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
  
```

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

**Correct Answer: D**



**QUESTION 89**

What is the correct about listening port?

- A. A listening port is a port open by a running application in order to accept inbound connections.
- B. A listening port is a port open by a running application in order to accept outbound connections.

**Correct Answer: A**

**QUESTION 90**

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/1/ntpamettag.gif?js=14ts=1476292607552.2866tc
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: C**

**QUESTION 91**

Which two HTTP header fields relate to intrusion analysis? (Choose two).

- A. user-agent
- B. host
- C. connection
- D. language
- E. handshake type

**Correct Answer: AB**

### QUESTION 92

Which type of analysis assigns values to scenarios to see what the outcome might be in each scenario?

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

**Correct Answer: A**

### QUESTION 93

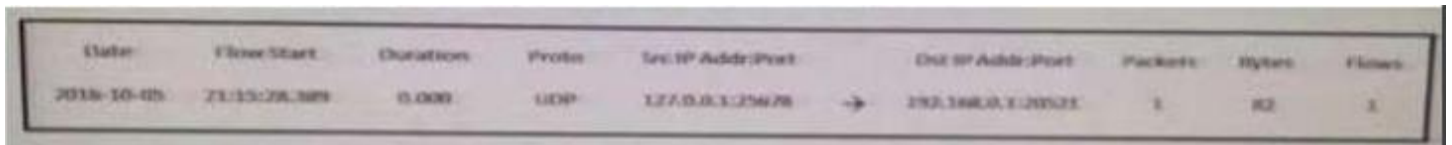
Which CVSSv3 metric captures the level of access that is required for a successful attack?

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

**Correct Answer: C**

### QUESTION 94

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



Date	Flow Start	Duration	Proto	Src IP Addr/Port	→	Dst IP Addr/Port	Packets	Bytes	Flows
2018-10-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→	192.168.0.1:20521	1	82	1

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

**Correct Answer: C**

### QUESTION 95

Which CVSSv3 metric value increases when attacks consume network bandwidth, processor cycles, or disk space?

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

**Correct Answer: C**

**QUESTION 96**

Select and Place:

Source Address	80
Destination Address	14846
Source Port	198.52.1.50
Destination Port	25.238.89.53

Correct Answer:

Built inbound TCP connection 463879 for outside:25.238.89.53/14846 (25.238.89.53/14846) to dmz:WWW\_Server/80 (198.52.1.50/80)

Source Address	25.238.89.53
Destination Address	198.52.1.50
Source Port	14846
Destination Port	80

**QUESTION 97**

Employee are allowed to access internal websites. Employee access an internal website but IDS report as a malicious behavior

- A. True positive
- B. True negative
- C. False positive
- D. False negative

**Correct Answer: C**

## QUESTION 98

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

No.	Time	Source	Destination	Protocol	Length	Info
17	0.011841	10.0.2.15	192.124.249.9	TCP	76	50588->443 [SYN] Seq=0 Win=0
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588->443 [SYN] Seq=0 Win=0
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=0
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443->50588 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50588->443 [ACK] Seq=1 Ack=0
23	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=0
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443->50588 [ACK] Seq=1 Ack=0
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	50588->443 [ACK] Seq=2005 Ack=0

Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits) on interface  
 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, Len: 261  
 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..f.. .....
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...43 {...f.....
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	.www.lin 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	.3t.....h2.s
00c0	00 33 74 00 00 00 10 00	17 00 15 02 68 32 08 73	pdy/3.1. http/1.1
00d0	70 64 79 2f 33 2e 31 08	68 74 74 70 2f 31 2e 31	.....
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		.....

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

### Correct Answer:

10.0.2.15 - Source address

50588 - Source port

443 - Destination port

192.124.249.9 - Destination address

TCP - Transport protocol

IPv4 - Network protocol

TLSv1.2 - Application protocol

**QUESTION 99**

Which of the following are the three metrics, or scores, of the CVSS?

- A. Baseline score
- B. Base score
- C. Environmental score
- D. Temporal score

**Correct Answer: BCD**

**QUESTION 100**

Filtering ports in wireshark?

- A. tcp.port = 80
- B. tcp.port equals 80
- C. tcp.port != 80
- D. tcp.port equal 80

**Correct Answer: C**

**QUESTION 101**

You see 100 HTTP GET and POST requests for various pages on one of your web servers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver.

Which category does this event fall under as defined in the Diamond Model of Intrusion?

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

**Correct Answer: A**

**QUESTION 102**

Which of the following is the team that handles the investigation, resolution, and disclosure of security vulnerabilities in vendor products and services?

- A. CSIRT
- B. ICASI
- C. USIRP
- D. PSIRT

**Correct Answer: D**

**QUESTION 103**

Which source provides reports of vulnerabilities in software and hardware to a Security Operations Center?

- A. Analysis Center
- B. National CSIRT
- C. Internal CSIRT
- D. Physical Security

**Correct Answer: C**

**QUESTION 104**

Nistsp800-61R2 what are the recommended protections against malware?

- A. install software to detect malware
- B. update antivirus signature

**Correct Answer: AB**

**QUESTION 105**

Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file?

- A. URL
- B. hash
- C. IP address
- D. destination port

**Correct Answer: B**

**QUESTION 106**

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. Which term defines the initial event in the NIST SP800-61 r2?

- A. Indicator
- B. Precursor
- C. online assault
- D. trigger

**Correct Answer: B**

**QUESTION 107**

You see confidential data being exfiltrated to an IP address that is attributed to a known Advanced Persistent Threat group. Assume that this is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Diamond Model of Intrusion?

- A. reconnaissance
- B. weaponization
- C. delivery
- D. action on objectives

**Correct Answer: D**

**QUESTION 108**

Which two statements correctly describe the victim demographics section of the VERIS schema? (Choose two.)

- A. The victim demographics section describes but does not identify the organization that is affected by the incident.
- B. The victim demographics section compares different types of organizations or departments within a single organization.
- C. The victim demographics section captures general information about the incident.
- D. The victim demographics section uses geolocation data to identify the organization name of the victim and the threat actor.

**Correct Answer: AB**

**QUESTION 109**

You have run a suspicious file in a sandbox analysis tool to see what the file does. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed or required to investigate the callouts? (Choose two.)

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

**Correct Answer: AE**

**QUESTION 110**

Which data type is protected under the PCI compliance framework?

- A. credit card type
- B. primary account number
- C. health conditions
- D. provision of individual care

**Correct Answer: B**

**QUESTION 111**

Which option filters a LibPCAP capture that used a host as a gateway?

- A. tcp|udp [src|dst] port <port>
- B. [src|dst] net <net> [{mask <mask>}|{len <len>}]
- C. ether [src|dst] host <ehost>
- D. gateway host <host>

**Correct Answer: D**

**QUESTION 112**

Which kind of evidence can be considered most reliable to arrive at an analytical assertion?

- A. direct
- B. corroborative
- C. indirect
- D. circumstantial
- E. textual

**Correct Answer: A**

**QUESTION 113**

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 114**

Which two options can be used by a threat actor to determine the role of a server? (Choose two.)

- A. PCAP
- B. tracer
- C. running processes
- D. hard drive configuration
- E. applications

**Correct Answer: CE**



### QUESTION 115

In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model'?

- A. victim demographics, incident description, incident details, discovery & response
- B. victim demographics, incident details, indicators of compromise, impact assessment
- C. actors, attributes, impact, remediation
- D. actors, actions, assets, attributes

**Correct Answer: D**

### QUESTION 116

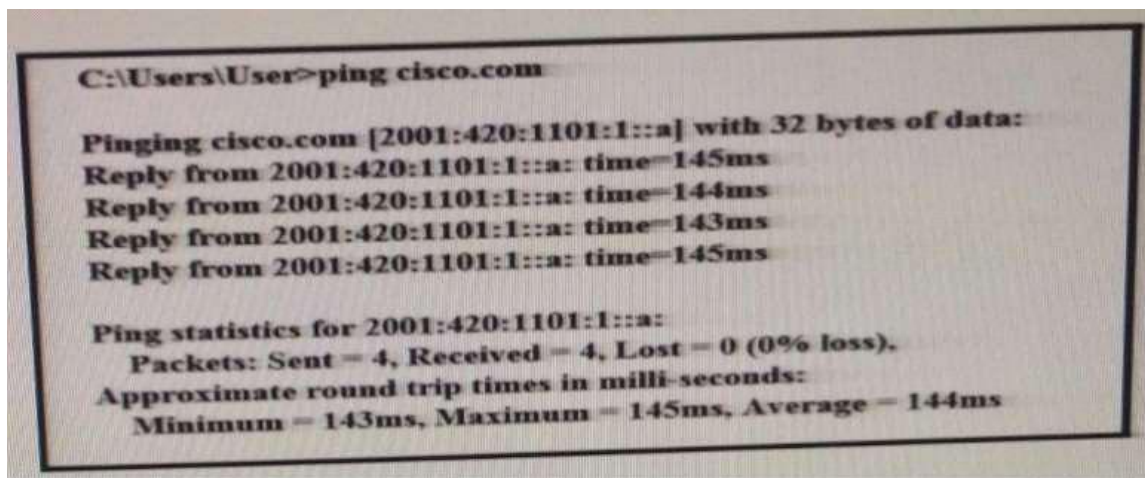
Which feature is used to find possible vulnerable services running on a server?

- A. CPU utilization
- B. security policy
- C. temporary internet files
- D. listening ports

**Correct Answer: D**

### QUESTION 117

Refer to the exhibit. What can be determined from this ping result?  
Exhibit:



- A. The public IP address of cisco.com is 2001:420:1101:1::a.
- B. The Cisco.com website is down.
- C. The Cisco.com website is responding with an internal IP.
- D. The public IP address of cisco.com is an IPv4 address.

**Correct Answer: A**

**QUESTION 120**

which option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?

- A. attack vector used to compromise the system
- B. time and resources needed to implement strategy
- C. need for evidence preservation
- D. effectiveness of the strategy

**Correct Answer: A**

**QUESTION 121**

To which category do attributes belong within the VERIS schema

- A. victim demographics
- B. incident tracking
- C. Discovery and response
- D. incident description

**Correct Answer: D**

**QUESTION 122**

Which option is the process of remediating the network and systems and/or reconstructing the attack so that the responsible threat actor can be revealed?

- A. data analytics
- B. asset attribution
- C. threat actor attribution
- D. evidence collection

**Correct Answer: C**

**QUESTION 123**

how do you enforce network access control automatically?

- A. IGMP
- B. SNMP
- C. 802.1X
- D. Port Security

**Correct Answer: C**

**QUESTION 124**

which Linux file system allows unlimited folder subdirectory structure

- A. ext4
- B. ext3
- C. ext2
- D. NTFS

**Correct Answer: A**

**QUESTION 125**

Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities. Which team?

- A. Federal CSIRT
- B. Federal PSIRT
- C. National CSIRT
- D. National PSIRT

**Correct Answer: C**