

# CCNA SECOPS (210-255) Dumps – Certification Practice Exam Answers

 [itexamanswers.net/ccna-secops-210-255-certification-practice-exam-answers.html](http://itexamanswers.net/ccna-secops-210-255-certification-practice-exam-answers.html)

May 24, 2019

**How to find:** Press “**Ctrl + F**” in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

**NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.**

**1. Which NIST-defined incident response stakeholder is responsible for coordinating incident response with other stakeholders and minimizing the damage of an incident?**

- human resources
- IT support
- the legal department
- **management**

The management team creates the policies, designs the budget, and is in charge of staffing all departments. Management is also responsible for coordinating the incident response with other stakeholders and minimizing the damage of an incident.

**2. What is defined in the policy element of the NIST incident response plan?**

- **how to handle incidents based on the mission and functions of an organization**
- a roadmap for updating the incident response capability
- the metrics used for measuring incident response capability in an organization
- how the incident response team of an organization will communicate with organization stakeholders

The policy element of the NIST incident response plan details how incidents should be handled based on the mission and function of the organization.

**3. Which three IPv4 header fields have no equivalent in an IPv6 header? (Choose three.)**

- **flag**

- **identification**
- TTL
- **fragment offset**
- version
- protocol

Unlike IPv4, IPv6 routers do not perform fragmentation. Therefore, all three fields supporting fragmentation in the IPv4 header are removed and have no equivalent in the IPv6 header. These three fields are fragment offset, flag, and identification. IPv6 does support host packet fragmentation through the use of extension headers, which are not part of the IPv6 header.

**4. What will a threat actor do to create a back door on a compromised target according to the Cyber Kill Chain model?**

- **Add services and autorun keys.**
- Obtain an automated tool to deliver the malware payload.
- Open a two-way communications channel to the CnC infrastructure.
- Collect and exfiltrate data.

Once a target system is compromised, the threat actor will establish a back door into the system to allow for continued access to the target. Adding services and autorun keys is a way to create a point of persistent access.

**5. Refer to the exhibit. A security specialist is checking if files in the directory contain ADS data. Which switch should be used to show that a file has ADS attached?**

```
Microsoft Windows [Version 10.0.16299.19]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\User\Public> dir <switch>
```

- /a
- /r
- /s
- /d

By using NTFS, Alternate Data Streams (ADSs) can be connected to a file as an attribute called \$DATA. The command `dir /r` can be used to see if a file contains ADS data.

**6. What is the responsibility of the human resources department when handling a security incident as defined by NIST?**

- Review the incident policies, plans, and procedures for local or federal guideline violations.
- **Perform disciplinary actions if an incident is caused by an employee.**
- Coordinate the incident response with other stakeholders and minimize the damage of an incident.
- Perform actions to minimize the effectiveness of the attack and preserve evidence.

The human resources department may be called upon to perform disciplinary measures if an incident is caused by an employee.

**7. In which top-level element of the VERIS schema does VERIS use the A4 threat model to describe an incident?**

- incident tracking
- **incident description**
- discovery and response
- impact assessment

In the top-level element incident description of the VERIS schema, VERIS uses the A4 threat model that was developed by the RISK team at Verizon to describe an incident completely.

**8. A company is applying the NIST.SP800-61 r2 incident handling process to security events. What are two examples of incidents that are in the category of precursor? (Choose two.)**

- multiple failed logins from an unknown source
- **log entries that show a response to a port scan**
- an IDS alert message being sent
- **a newly-discovered vulnerability in Apache web servers**
- a host that has been verified as infected with malware

As an incident category, the precursor is a sign that an incident might occur in the future. Examples of precursors are log entries that show a response to a port scan or a newly-discovered vulnerability in web servers using Apache.

**9. What is a goal of deploying an in-line security device that can analyze data as a normalized stream?**

- reduce the amount of event data
- satisfy compliance requirements
- **detect and block intrusions**
- decrease network latency and jitter

An IPS is an in-line security device that can analyze data as a normalized stream to reduce or eliminate the possibility of security evasions.

## 10. What is the VERIS Community Database (VCDB)?

- a collection of research of trend and potential security intrusions
- **a central location for the security community to learn from experience and help with decision making before, during, and after a security incident**
- a collection of incident data collected and categorized by a selected group of cybersecurity professionals
- an open and free collection of publicly-reported security incidents posted in a variety of data formats

The VERIS Community Database (VCDB) is an open and free collection of publicly-reported security incidents in VERIS format. The VCDB is in a universal format that allows for manipulation and transformation.

## 11. According to the Cyber Kill Chain model, after a weapon is delivered to a targeted system, what is the next step that a threat actor would take?

- action on objectives
- **exploitation**
- weaponization
- installation

The Cyber Kill Chain specifies seven steps (or phases) and sequences that a threat actor must complete to accomplish an attack:

- **Reconnaissance** – The threat actor performs research, gathers intelligence, and selects targets.
- **Weaponization** – The threat actor uses the information from the reconnaissance phase to develop a weapon against specific targeted systems.
- **Delivery** – The weapon is transmitted to the target using a delivery vector.
- **Exploitation** – The threat actor uses the weapon delivered to break the vulnerability and gain control of the target.
- **Installation** – The threat actor establishes a back door into the system to allow for continued access to the target.
- **Command and Control (CnC)** – The threat actor establishes command and control (CnC) with the target system.
- **Action on Objectives** – The threat actor is able to take action on the target system, thus achieving the original objective.

## 12. Which metric in the CVSS Base Metric Group is used with an attack vector?

- the determination whether the initial authority changes to a second authority during the exploit

- the presence or absence of the requirement for user interaction in order for an exploit to be successful
- **the proximity of the threat actor to the vulnerability**
- the number of components, software, hardware, or networks, that are beyond the control of the attacker and that must be present in order for a vulnerability to be successfully exploited

The attack vector is one of several metrics defined in the Common Vulnerability Scoring System (CVSS) Base Metric Group Exploitability metrics. The attack vector is how close the threat actor is to the vulnerable component. The farther away the threat actor is to the component, the higher the severity because threat actors close to the network are easier to detect and mitigate.

**13. Which statement describes the card verification value (CVV) for a credit card?**

- It is the credit card account number.
- **It is a security feature of the card.**
- It is a PIN number for the card.
- It is the bank account number.

The card verification value (CVV), or card verification code (CVC), or card security code (CSC) is a security feature of a credit card, usually 3 or 4 digits printed on the back of the card.

**14. Which three fields are found in both the TCP and UDP headers? (Choose three.)**

- window
- **checksum**
- options
- sequence number
- **destination port**
- **source port**

The UDP header has four fields. Three of these fields are in common with the TCP header. These three fields are the source port, destination port, and checksum.

**15. Which specification provides a common language for describing security incidents in a structured and repeatable way?**

- **VERIS schema**
- Cyber Kill Chain
- NIST Incident Response Life Cycle

- Diamond model

Vocabulary for Event Recording and Incident Sharing (VERIS) was created to provide a common language for describing security incidents. VERIS addresses the problems of dealing with different security tools and the tendency of humans to refer to incidents and events inconsistently.

**16. What is the responsibility of the IT support group when handing an incident as defined by NIST?**

- reviews the incident policies, plans, and procedures for local or federal guideline violations
- **performs actions to minimize the effectiveness of the attack and preserve evidence**
- coordinates the incident response with other stakeholders and minimizes the damage of an incident
- performs disciplinary measures if an incident is caused by an employee

IT support best understands the technology used in the organization and can perform the correct actions to minimize the effectiveness of the attack and preserve evidence.

**17. During the detection and analysis phase of the NIST incident response process life cycle, which sign category is used to describe that an incident might occur in the future?**

- attrition
- impersonation
- **precursor**
- indicator

There are two categories for the signs of an incident:

- **Precursor** – a sign that an incident might occur in the future
- **Indicator** – a sign that an incident might already have occurred or is currently occurring

**18. After a security monitoring tool identifies a malware attachment entering the network, what is the benefit of performing a retrospective analysis?**

- It can calculate the probability of a future incident.
- It can identify how the malware originally entered the network.
- It can determine which network host was first affected.
- **A retrospective analysis can help in tracking the behavior of the malware from the identification point forward.**

General security monitoring can identify when a malware attachment enters a network and which host is first infected. Retrospective analysis takes the next step and is the tracking of the behavior of the malware from that point forward.

**19. Which field in the IPv6 header points to optional network layer information that is carried in the IPv6 packet?**

- flow label
- version
- traffic class
- **next header**

Optional Layer 3 information about fragmentation, security, and mobility is carried inside of extension headers in an IPv6 packet. The next header field of the IPv6 header acts as a pointer to these optional extension headers if they are present.

**20. Refer to the exhibit. A security analyst issues the cat command to review the content of the file confidential2. Which encoding method was used to encode the file?**

```
[analyst@secOps]$ cat confidential2
434f4e4649444454e54494114c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
```

- 8-bit binary
- ASCII
- **Hex**
- Base64

Hex encodes binary data in hexadecimal string format. Base64 encodes binary data in an ASCII string format. In this case, the characters are 0-9 and a-f, typical hexadecimal numbers.

**21. How much overhead does the TCP header add to data from the application layer?**

- 8 bytes
- 16 bytes
- **20 bytes**
- 40 bytes

The Layer 4 header in a TCP segment is the TCP header, which is 20 bytes in length. This adds 20 bytes of overhead to the data from the application layer in the composition of a TCP segment.

**22. In which step of the NIST incident response process does the CSIRT perform an analysis to determine which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring?**

- incident notification
- **scoping**
- attacker identification
- detection

In the detection and analysis phase of the NIST incident response process life cycle, the CSIRT should immediately perform an initial analysis to determine the scope of the incident, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring.

**23. Refer to the exhibit. Which technology generated the event log?**

1265939281.764 19478 172.16.167.228 TCP\_MISS/200 864 GET  
http://www.example.com/images/home.png - NONE/- image/png

- **web proxy**
- NetFlow
- syslog
- Wireshark

The output shown is from a web proxy.

**24. When a server profile for an organization is being established, which element describes the TCP and UDP daemons and ports that are allowed to be open on the server?**

- **listening ports**
- service accounts
- critical asset address space
- software environment

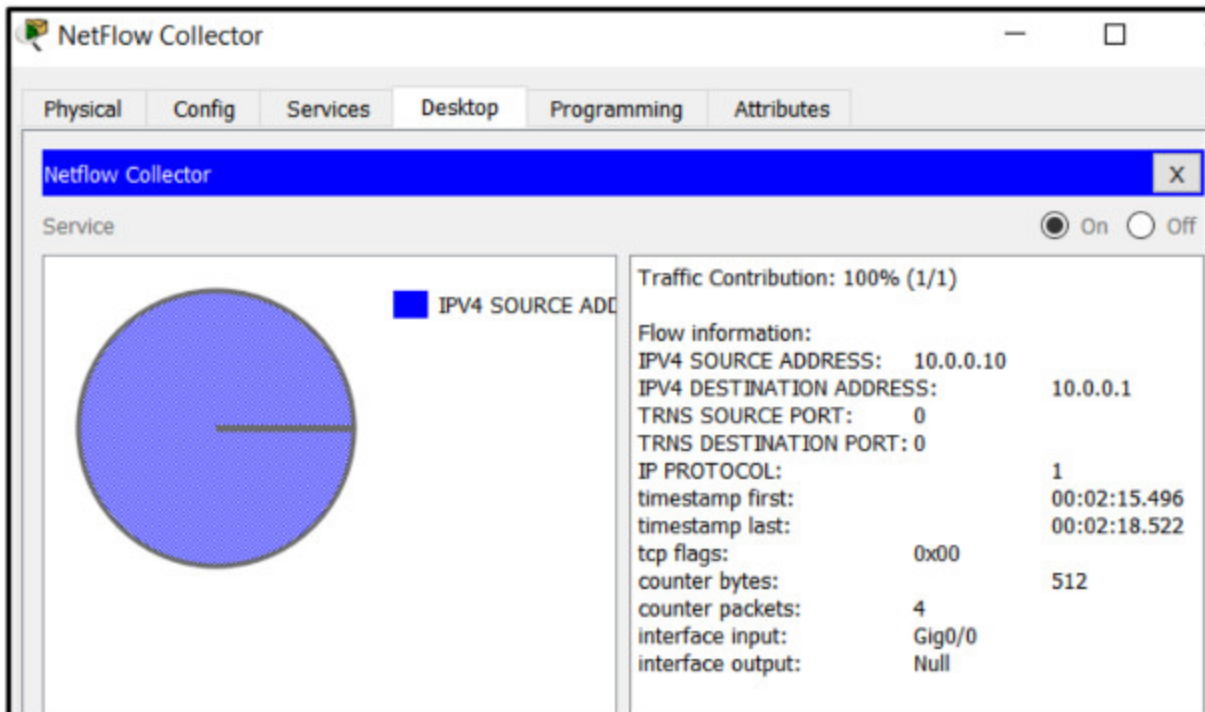
A server profile will often contain the following:

- **Listening ports** – the TCP and UDP daemons and ports that are allowed to be open on the server
- **User accounts** – the parameters defining user access and behavior



- **Service accounts** – the definitions of the type of service that an application is allowed to run on a server
- **Software environment** – the tasks, processes, and applications that are permitted to run on the server

**25. Refer to the exhibit. A network administrator is examining a NetFlow record. Why would the record indicate that both TRNS SOURCE PORT and TRNS DESTINATION PORT are 0?**



- The flow contains four packets and they use varying port numbers.
- **The flow does not include transport layer protocols.**
- The Giga/0 interface has not transmitted any packets.
- The source host uses a different transport layer protocol from the one used by the destination host.

The data flow recorded is ICMP traffic, indicated by the number 1 for IP PROTOCOL. Because ICMP is a Layer 3 protocol and has no need for a Layer 4 protocol such as TCP or UDP, the port numbers show a 0 within the NetFlow output.

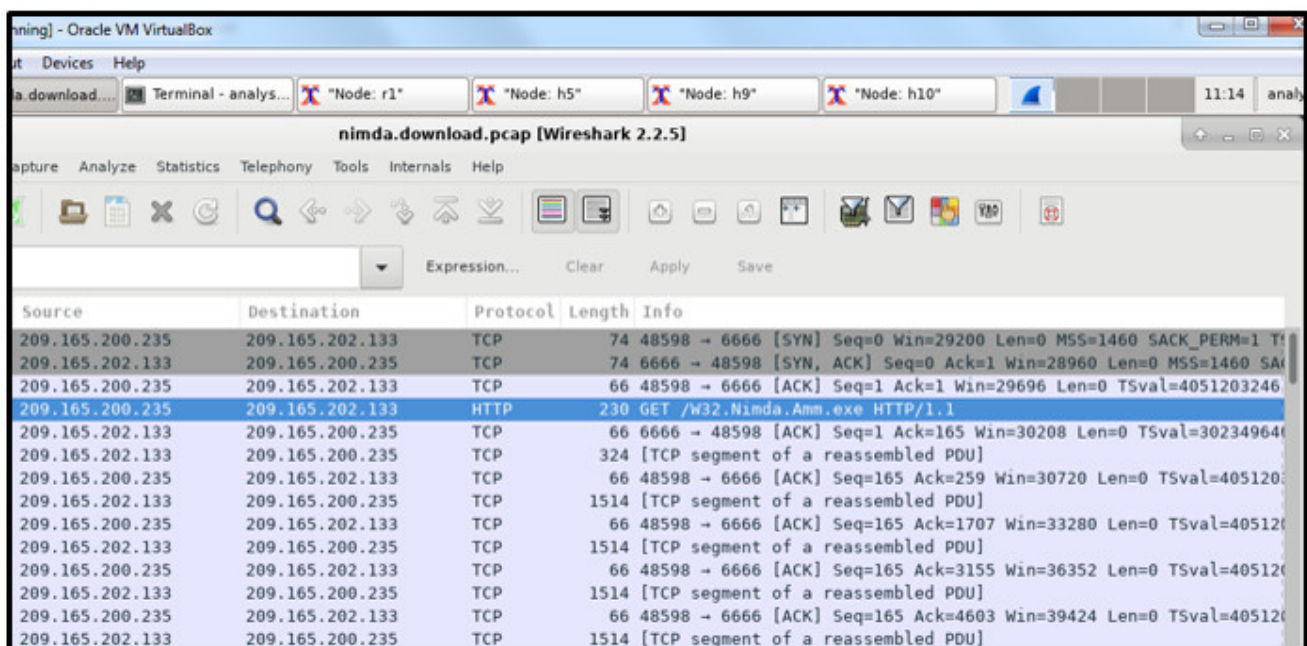
**26. When establishing a server profile for an organization, which element describes the type of service that an application is allowed to run on the server?**

- listening port
- user account
- software environment
- **service account**

A server profile should contain some important elements including these:

- **Listening ports** – the TCP and UDP daemons and ports that are allowed to be open on the server
- **User accounts** – the parameters defining user access and behavior
- **Service accounts** – the definitions of the type of service that an application is allowed to run on a server
- **Software environment** – the tasks, processes, and applications that are permitted to run on the server

**27. Refer to the exhibit. A security specialist is using Wireshark to review a PCAP file generated by *tcpdump* . When the client initiated a file download request, which source socket pair was used?**



The image shows a Wireshark 2.2.5 packet capture window. The title bar indicates the file is 'nimda.download.pcap'. The packet list on the left shows several TCP and HTTP packets. The selected packet (packet 10) is an HTTP GET request from 209.165.200.235 to 209.165.202.133. The packet details pane on the right shows the HTTP request structure.

Source	Destination	Protocol	Length	Info
209.165.200.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4051203246 TSecr=0
209.165.202.133	209.165.200.235	TCP	74	6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=302349640 TSecr=4051203246
209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=4051203246 TSecr=302349640
209.165.200.235	209.165.202.133	HTTP	230	GET /W32.Nimda.Amm.exe HTTP/1.1
209.165.202.133	209.165.200.235	TCP	66	6666 → 48598 [ACK] Seq=1 Ack=165 Win=30208 Len=0 TSval=302349640 TSecr=4051203246
209.165.202.133	209.165.200.235	TCP	324	[TCP segment of a reassembled PDU]
209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=259 Win=30720 Len=0 TSval=4051203246 TSecr=302349640
209.165.202.133	209.165.200.235	TCP	1514	[TCP segment of a reassembled PDU]
209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=1707 Win=33280 Len=0 TSval=4051203246 TSecr=302349640
209.165.202.133	209.165.200.235	TCP	1514	[TCP segment of a reassembled PDU]
209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=3155 Win=36352 Len=0 TSval=4051203246 TSecr=302349640
209.165.202.133	209.165.200.235	TCP	1514	[TCP segment of a reassembled PDU]
209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=4603 Win=39424 Len=0 TSval=4051203246 TSecr=302349640
209.165.202.133	209.165.200.235	TCP	1514	[TCP segment of a reassembled PDU]

- 209.165.202.133:6666
- 209.165.200.235:6666
- 209.165.202.133:48598
- **209.165.200.235:48598**

The combination of the source IP address and source port number, or the destination IP address and destination port number, is known as a socket. A socket is shown as the IP address and associated port number with a colon in between the two (IP\_address:port\_number).

**28. A cybersecurity analyst is performing a CVSS assessment on an attack where a web link was sent to several employees. Once clicked, an internal attack was launched. Which CVSS Base Metric Group Exploitability metric is used to document that the user had to click on the link in order for the attack to occur?**

- integrity requirement
- availability requirement
- **user interaction**
- scope

The CVSS Base Metric Group has the following metrics: attack vector, attack complexity, privileges required, user interaction, and scope. The user interaction metric expresses the presence or absence of the requirement for user interaction in order for an exploit to be successful.

### **29. What is the benefit of converting log file data into a common schema?**

- creates a data model based on fields of data from a source
- allows the implementation of partial normalization and inspection
- **allows easy processing and analysis of datasets**
- creates a set of regex-based field extractions

When data is converted into a universal format, it can be effectively structured for performing fast queries and event analysis.

### **30. What are the three impact metrics contained in the CVSS 3.0 Base Metric Group? (Choose three.)**

- **integrity**
- remediation level
- **confidentiality**
- exploit
- attack vector
- **availability**

The Common Vulnerability Scoring System (CVSS) is a vendor-neutral, industry standard, open framework for weighing the risks of a vulnerability using a variety of metrics. CVSS uses three groups of metrics to assess vulnerability, the Base Metric Group, Temporal Metric Group, and Environmental Metric Group. The Base Metric Group has two classes of metrics (exploitability and impact). The impact metrics are rooted in the following areas: confidentiality, integrity, and availability.

### **31. Which type of analysis relies on different methods to establish the likelihood that a security event has happened or will happen?**

- deterministic
- statistical
- log
- **probabilistic**

Probabilistic methods use powerful tools to create a probabilistic answer as a result of analyzing applications.

**32. When establishing a network profile for an organization, which element describes the time between the establishment of a data flow and its termination?**

- routing protocol convergence
- **session duration**
- bandwidth of the Internet connection
- total throughput

A network profile should include some important elements, such as the following:

- **Total throughput** – the amount of data passing from a given source to a given destination in a given period of time
- **Session duration** – the time between the establishment of a data flow and its termination
- **Ports used** – a list of TCP or UDP processes that are available to accept data
- **Critical asset address space** – the IP addresses or the logical location of essential systems or data

**33. When attempting to improve system performance for Linux computers with a limited amount of memory, why is increasing the size of the swap file system not considered the best solution?**

- A swap file system cannot be mounted on an MBR partition.
- A swap file system only supports the ex2 file system.
- A swap file system does not have a specific file system.
- **A swap file system uses hard disk space to store inactive RAM content.**

The swap file system is used by Linux when it runs out of physical memory. When needed, the kernel moves inactive RAM content to the swap partition on the hard disk. Storing and retrieving content in the swap partition is much slower than RAM is, and therefore using the swap partition should not be considered the best solution to improving system performance.

**34. What will match the regular expression `^83`?**

- any string that includes 83
- **any string that begins with 83**
- any string with values greater than 83
- any string that ends with 83

The expression `^83` indicates any string that begins with 83 will be matched.

**35. Which type of evidence cannot prove an IT security fact on its own?**

- best
- corroborative
- **indirect**
- hearsay

Indirect evidence cannot prove a fact on its own, but direct evidence can. Corroborative evidence is supporting information. Best evidence is most reliable because it is something concrete such as a signed contract.

**36. Which type of computer security incident response team is responsible for determining trends to help predict and provide warning of future security incidents?**

- coordination centers
- **analysis centers**
- vendor teams
- national CSIRT

There are many different types of computer security incident response teams (CSIRTs) and related information security organizations. Analysis centers use data from many sources to determine security incident trends that can help predict future incidents and provide early warning.

**37. Which two actions should be taken during the preparation phase of the incident response life cycle defined by NIST? (Choose two.)**

- Fully analyze the incident.
- Meet with all involved parties to discuss the incident that took place.
- Detect all the incidents that occurred.
- **Acquire and deploy the tools that are needed to investigate incidents.**
- **Create and train the CSIRT**

According to the guideline defined in the NIST Incident Response Life Cycle, several actions should be taken during the preparation phase including (1) creating and training the CSIRT and (2) acquiring and deploying the tools needed by the team to investigate incidents.

**38. Which technology is used by Cisco Advanced Malware Protection (AMP) in defending and protecting against known and emerging threats?**

- **threat intelligence**
- network admission control
- network profiling
- website filtering and blacklisting

Cisco AMP uses threat intelligence along with known file signatures to identify and block policy-violating file types and exploitations.

**39. Which two actions can help identify an attacking host during a security incident? (Choose two.)**

- **Use an Internet search engine to gain additional information about the attack.**
- Log the time and date that the evidence was collected and the incident remediated.
- Determine the location of the recovery and storage of all evidence.
- **Validate the IP address of the threat actor to determine if it is viable.**
- Develop identifying criteria for all evidence such as serial number, hostname, and IP address

The following actions can help identify an attacking host during a security incident: Use incident databases to research related activity.

Validate the IP address of the threat actor to determine if it is a viable one.

Use an Internet search engine to gain additional information about the attack.

Monitor the communication channels that some threat actors use, such as IRC.

**40. What classification is used for an alert that correctly identifies that an exploit has occurred?**

- false negative
- false positive
- **true positive**
- true negative

A true positive occurs when an IDS and IPS signature is correctly fired and an alarm is generated when offending traffic is detected.

**41. Which type of analysis relies on predefined conditions and can analyze applications that only use well-known fixed ports?**

- statistical
- **deterministic**
- log
- probabilistic

Deterministic analysis uses predefined conditions to analyze applications that conform to specification standards, such as performing a port-based analysis.

**42. What are security event logs commonly based on when sourced by traditional firewalls?**

- application analysis
- static filtering
- signatures
- **5-tuples**

Traditional firewalls commonly provide security event logs based on the 5-tuples of source IP address and port number, destination IP address and port number, and the protocol in use.

**43. Using Tcpdump and Wireshark, a security analyst extracts a downloaded file from a pcap file. The analyst suspects that the file is a virus and wants to know the file type for further examination. Which Linux command can be used to determine the file type?**

- **file**
- tail
- nano
- ls -l

The Linux file command can be used to determine a file type, such as whether it is executable, ASCII text, or zip.

**44. Which three things will a threat actor do to prepare a DDoS attack against a target system on the Internet? (Choose three.)**

- Install a black door on the target system.
- Collect and exfiltrate data.
- **Compromise many hosts on the Internet.**
- Obtain an automated tool to deliver the malware payload.
- **Establish two-way communications channels to the CnC infrastructure with zombies.**
- **Install attack software on zombies.**

To prepare for launching a DDoS attack, a threat actor will compromise many hosts on the Internet, called zombies. The threat actor will then install attack software on zombies and establish a two-way communications channel to CnC infrastructure with zombies. The threat actor will issue the command to zombies through the CnC to launch a DDoS attack against a target system.

**45. After containing an incident that infected user workstations with malware, what are three effective remediation procedures that an organization can take for eradication? (Choose three.)**

- Change assigned names and passwords for all devices.
- **Update and patch the operating system and installed software of all hosts.**

- **Rebuild hosts with installation media if no backups are available.**
- Rebuild DHCP servers using clean installation media.
- Disconnect or disable all wired and wireless network adapters until the remediation is complete.
- **Use clean and recent backups to recover hosts.**

To recover infected user workstations, use clean and recent backups or rebuild the PCs with installation media if no backups are available or they have been compromised. Also, fully update and patch the operating system and installed software of all hosts. All users are encouraged to change their passwords for the workstation or workstations they use. Rebuilding DHCP servers is needed only if they are affected by the incident. Also not all devices need to change the name and password configuration setting unless they are affected by the incident.

**46. A cybersecurity analyst has been called to a crime scene that contains several technology items including a computer. Which technique will be used so that the information found on the computer can be used in court?**

- rootkit
- log collection
- **unaltered disk image**
- Tor

A normal file copy does not recover all data on a storage device so an unaltered disk image is commonly made. An unaltered disk image preserves the original evidence, thus preventing inadvertent alteration during the discovery phase. It also allows recreation of the original evidence.

**47. What is specified in the plan element of the NIST incident response plan?**

- incident handling based on the mission of the organization
- organizational structure and the definition of roles, responsibilities, and levels of authority
- priority and severity ratings of incidents
- **metrics for measuring the incident response capability and effectiveness**

NIST recommends creating policies, plans, and procedures for establishing and maintaining a CSIRC. One component of the plan element is to develop metrics for measuring the incident response capability and its effectiveness.

**48. A network administrator is creating a network profile to generate a network baseline. What is included in the critical asset address space element?**

- the TCP and UDP daemons and ports that are allowed to be open on the server



- **the IP addresses or the logical location of essential systems or data**
- the list of TCP or UDP processes that are available to accept data
- the time between the establishment of a data flow and its termination

A network profile should include some important elements, such as the following:

- **Total throughput** – the amount of data passing from a given source to a given destination in a given period of time
- **Session duration** – the time between the establishment of a data flow and its termination
- **Ports used** – a list of TCP or UDP processes that are available to accept data
- **Critical asset address space** – the IP addresses or the logical location of essential systems or data

**49. What are two sources of data in the operation of a security information and event management (SIEM) system? (Choose two.)**

- **firewalls**
- dashboards and reports
- **antimalware devices**
- automation and alerts
- incident management systems

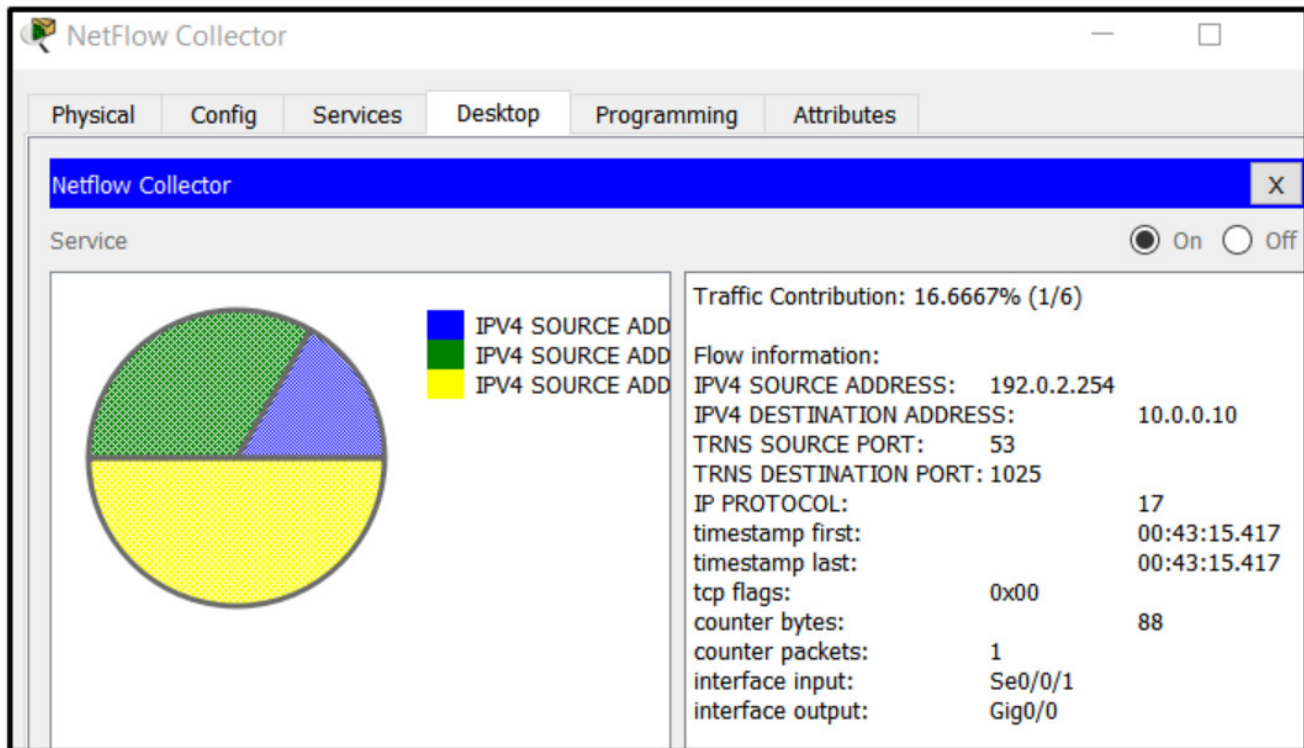
Security information and event management (SIEM) systems receive data from IPS devices, firewalls, NetFlow devices, servers, endpoints, and syslog infrastructure devices.

**50. What are two of the 5-tuples? (Choose two.)**

- IPS
- **source port**
- IDS
- ACL
- **protocol**

The components of a 5-tuple include a source IP address and port number, destination IP address and port number, and the protocol in use.

**51. Refer to the exhibit. A network administrator is examining a NetFlow record. Which protocol is in use in the flow shown?**



- UDP
- ICMP
- TCP
- HTTP

The data flow shown is captured UDP traffic of a DNS response, indicated by the number 17 in the IP PROTOCOL output.

**52. When real-time reporting of security events from multiple sources is being received, which function in SIEM provides capturing and processing of data in a common format?**

- aggregation
- log collection
- **normalization**
- compliance

SIEM combines SEM and SIM tools to provide some useful functions, one of which is data normalization. Data normalization is the process of mapping log messages from different systems into a common data model in order to analyze related security events, even if they are initially logged in different source formats.

**53. What is the role of vendor teams as they relate to a computer security incident response team?**

- **They handle customer reports concerning security vulnerabilities.**

- They provide incident handling to other organizations as a fee-based service.
- They coordinate incident handling across multiple teams.
- They use data from many sources to determine incident activity trends.

There are many different types of computer security incident response teams (CSIRTs) and related information security organizations. Vendor CSIRT teams provide remediation for vulnerabilities in the software or hardware of an organization and often handle customer reports concerning security vulnerabilities.

**54. At the request of investors, a company is proceeding with cyber attribution with a particular attack that was conducted from an external source. Which security term is used to describe the person or device responsible for the attack?**

- **threat actor**
- fragmenter
- tunneler
- skeleton

Some people may use the common word of “hacker” to describe a threat actor. A threat actor is an entity that is involved with an incident that impacts or has the potential to impact an organization in such a way that it is considered a security risk or threat.

**55. What are three of the four interactive landscapes that VERIS schema use to define risk?**

- response
- evidence
- attack
- **threat**
- **impact**
- **control**

In the VERIS schema, risk is defined as the intersection of four landscapes of threat, asset, impact, and control. Information from each landscape helps to understand the level of risk to the organization.

## **New Questions for 210-255 Exam (Dump)**

---

**1. Which data element must be protected with regards to PCI?**

- past health condition
- geographic location

- **full name / full account number >>>> full name <<<** Came in the exam only
- recent payment amount

**2. What is Data mapping used for? (Choose two)**

- **data accuracy(integrity)**
- data availability
- data normalization
- data confidentiality
- **data visualization**

**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

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

- C2
- **Delivery**
- Installation
- Exploitation

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

- determining the number of attackers that are associated with a security incident
- ascertaining the number and types of vulnerabilities on your network

- **identifying the extent that a security incident is impacting protected resources on the network**
- **determining what and how much data may have been affected**
- identifying the attackers that are associated with a security incident

**6. What does the CSIRT incident response provider usually do?**

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

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

- **data normalization**
- data availability
- data protection
- data signature

**8. According to NIST what option is unnecessary for containment strategy?**

- **The delayed containment**
- **Monitoring with methods other than sandboxing**

**9. What is the difference between deterministic and probabilistic assessment method?**

- **At deterministic method we know the facts beforehand and at probabilistic method we make assumptions**
- At probabilistic method we know the facts beforehand and at deterministic method we make assumptions
- Probabilistic method has an absolute nature
- **Deterministic method has an absolute nature**

**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?**

- network file storing
- **free space fragmentation**
- alternate data streaming

- defragmentatio

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

- HTTPS traffic
- TCP traffic
- HTTP traffic
- **UDP traffic**

**12. Filtering ports in Wireshark?**

- **tcp.port == 80**
- tcp port equals 80
- tcp.port 80
- port 80

**13. What attribute belonging VERIS schema?**

- **confidentiality/possession**
- **integrity/authenticity**
- **availability/utility**

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

- **Communication to CnC servers**
- Configuration issues
- Routing problems
- **Malicious domain based on reputation**

**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?**

- weaponization
- exploitation
- installation
- **reconnaissance**

**16. Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?**

- local
- **physical**
- network
- adjacent

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

- **collection**
- examination
- reporting
- investigation

**18. What is the definition of confidentiality according to CVSSv3 framework?**

- **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.**
- This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
- This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

**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?**

- **Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident 6.0)**
- Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805
- Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 4.0.0) Gecko/20100101
- Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16

**20. Which netstat command show ports?**

- netstat -g
- **netstat -l**
- netstat -r
- netstat -v

**21. Which identifies both the source and destination location?**

- **IP address**
- URL

- ports
- MAC address

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

- **source**
- origination
- destination
- network

**23. Which of the following is one of the main goals of the CSIRT?**

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

**24. Which goal of data normalization is true?**

- **Reduce data redundancy.**
- Increase data redundancy.
- Reduce data availability.
- Increase data availability

**25. Which of the following is not an example of reconnaissance?**

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

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

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

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

- **examination**
- reporting

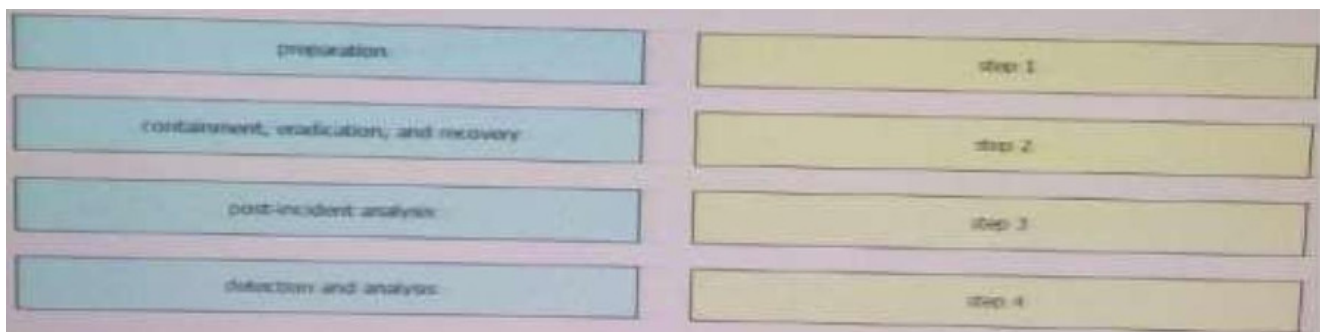


- collection
- investigation

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

- **File > Export Objects**
- Analyze > Extract
- Tools > Export > TCP
- View > Extract

**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

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

- Configure the organization's firewall
- Monitor security logs
- Investigate security incidents in a SOC
- **Disclosure vulnerabilities in the organization's products and services**

**31. Which of the following is an example of a coordination center?**

- Cisco PSIRT
- Microsoft MSRC
- **CERT division of the SEI**
- FIRST

**32. Choose the option that best describes NIST data integrity**

- use only sha-1
- use only md5
- **you must hash data & backup and compare hashes**
- no need to hash data & backup and compare hashes

**33. What is NAC?**

- Non-Admin Closure
- **Network Access Control**
- Nepal Airline Corporations
- Network Address Control

**34. Which of the following is not true about listening ports?**

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

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

- Scanning vendor customer network
- **incident classification and handling**
- **Information classification and protection**
- **Information dissemination**
- **Record retentions and destruction**

**36. Which element is included in an incident response plan?**

- **organization mission**
- junior analyst approval
- day-to-day firefighting
- siloed approach to communications

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

- ip.address == <address> or ip.network == <network>
- [tcp|udp] ip.[src|dst] port <port>
- ip.addr == <addr> or ip.name == <name>
- **ip.addr == <addr> or ip.host == <host>**

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

- descriptive
- casual
- **probabilistic**
- inferential

**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?**

- **internal CSIRT**
- national CSIRT
- coordination centers
- analysis centers
- vendor teams
- incident response providers

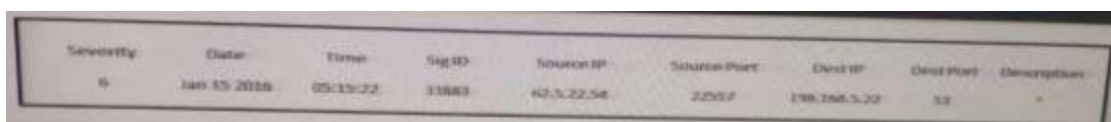
**40. Which regular expression matches “color” and “colour”?**

- col[0-9]+our
- colo?ur
- **colou?r**
- [a-z]{7}

**41. Which element is part of an incident response plan?**

- **organizational approach to incident response**
- organizational approach to security
- disaster recovery
- backups

**42. 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	31883	62.5.22.54	22557	198.168.5.22	80	-

- syslog
- NetFlow log
- proxy log
- **IDS log**

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

**Malware prevention software**

**44. Which option can be addressed when using retrospective security techniques?**

- if the affected host needs a software update
- **how the malware entered our network**
- why the malware is still in our network
- if the affected system needs replacement

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

- Coordination Center
- Internal CSIRT
- **National CSIRT**
- Analysis Center

**46. What protocol is related to NAC?**

- 802.1Q
- **802.1X**
- 802.1E
- 802.1F

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

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

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

**inspect other incident related to the incident**

**49. similar to this ... the same answer**

**Which of the following make the file unique?**

- file timestamp
- **file hash**
- file size

**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?**

- NTFS
- exFAT
- Ext5
- **Ext4**

**51. attacker using robots.txt is under which category?**

- **Reconnaissance**
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and control (C2)
- Actions on objectives

**52. What do the CSIRT incident analysis centers usually do?**

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

**53. 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 )

- **The website has been marked benign on all 68 checks.**
- The threat detection needs to run again.
- The website has 68 open threats.
- The website has been marked benign on 0 checks

**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?**

- TTLs
- **ports**
- SMTP replies
- IP addresses

**55. Which option is a misuse variety per VERIS enumerations?**

- snooping
- **hacking**
- theft
- assault

**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?**

- reconnaissance
- weaponization
- **delivery**
- installation

**57. What is the definition of integrity according to CVSSv3 framework?**

- 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.
- **This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.**
- This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

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

- Source IP address
- **Flow record ID**
- Source port
- **Gateway**
- Destination port

**59. Which netstat command show ports? (Choose two)**

- **netstat -a**
- **netstat -l >> came in the exam**
- netstat -v
- netstat -g

**60. Which of the following is not an example of weaponization**

- **Connecting to a CnC server**
- Wrapping software with a RAT
- Creating backdoor in an app
- Developing an automated script to inject commands on a USB device

**61.**

**%ASA-6-302015: Built inbound TCP connection 12879515 for outside:192.168.1.1/2196 to inside:192.168.2.2/22**

Drag and drop the items from the left onto the correct 5-tuples on the right.

192.168.1.1	Source Port
192.168.2.2	Protocol
2196	Source IP
22	Destination IP
TCP	Destination Port

**Answer:**

192.168.1.1	TCP
192.168.2.2	2196
2196	192.168.1.1
22	192.168.2.2
TCP	22

**Explanation**  
 192.168.1.1 = source ip  
 192.168.2.2 = destination ip  
 2196 = protocol  
 22 = Destination port  
 TCP = source port

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

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

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

- referrer
- **IP address**
- user-agent
- URL

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

- Reconnaissance
- Weaponization
- Delivery
- **Exploitation**
- Installation
- Command and control (C2)
- Actions on objectives

**65. Which statement about threat actors is true?**

- They are any company assets that are threatened.
- They are any assets that are threatened.
- **They are perpetrators of attacks.**
- They are victims of attacks.

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

- Incident tracking
- Victim demographics
- Incident descriptions
- **Incident forensics ID**

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

- **facilitators**
- practitioners
- leaders and managers
- decision makers

**68. What is accomplished in the identification phase of incident handling?**

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

**69. Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?**

- true positive
- true negative
- **false positive**
- false negative

**70. Which string matches the regular expression  $r(ege)+x$ ?**

- rx
- **regeegex**
- $r(ege)x$
- rege+x

**71. What is the definition of availability accord to CVSSv3 framework?**

- 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.
- This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
- **This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.**

**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?**

- Fraud, money laundering, and theft
- Drug-related crime
- Murder and acts of violence
- **All of the above**

**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?**

- Cisco CloudLock
- **Cisco's Active Threat Analytics (ATA)**
- Cisco Managed Firepower Service
- Cisco Jasper

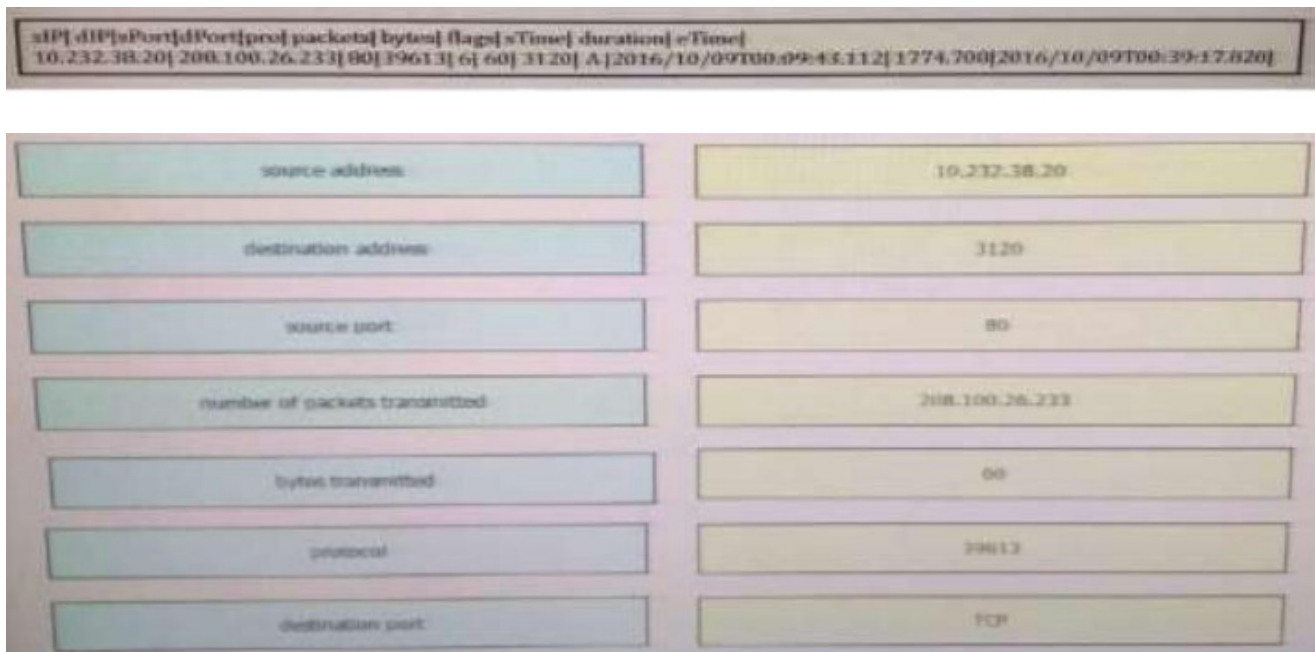
**74. Which information must be left out of a final incident report?**

- **server hardware configurations**
- exploit or vulnerability used
- impact and/or the financial loss
- how the incident was detected

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

- **port number**
- **destination IP address**
- data packet
- user name
- host logs

**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 its corresponding fields. The record is a single line of text: `sIP|dIP|sPort|dPort|prot|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|1774.700|2016/10/09T00:39:17.820|`

Field Name	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

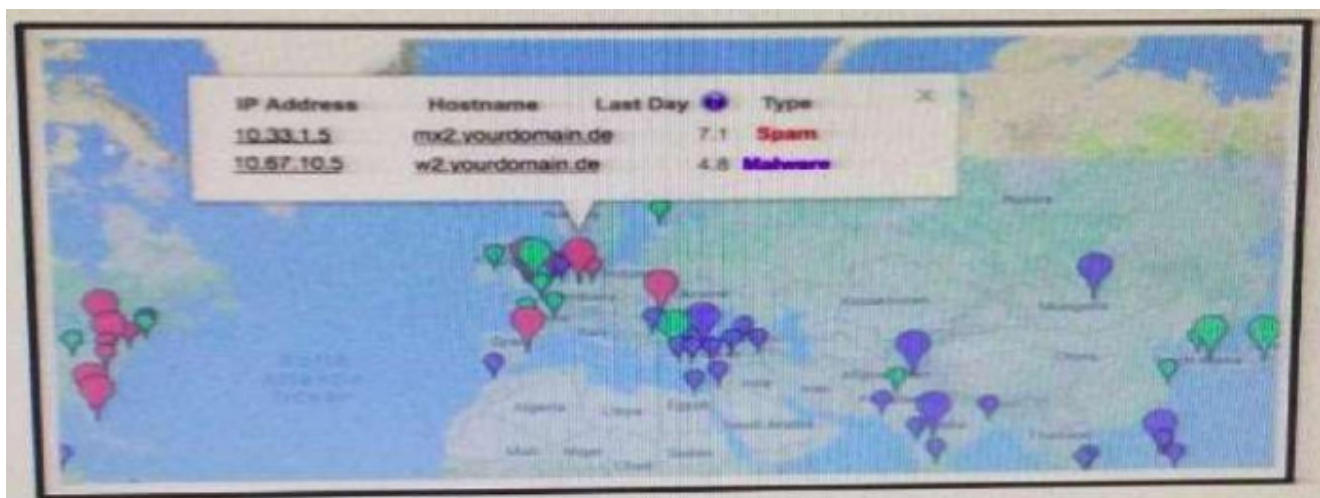
**Correct Answer:**

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

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

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

**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?**



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

**79. may be this came in inverse the national in choices and the answer in the ... read and understand it**

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

- Provide solutions for bug bounties
- Provide vulnerability brokering to vendors within a country

- **Protect their citizens by providing security vulnerability info, security awareness training, best practices, and other info**
- Create regulations around cybersecurity within the country

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

- **Public, private, and individual investigations**
- Judiciary, private, and individual investigations
- Public, private, and corporate investigations
- Government, corporate, and private investigations

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

- preparation
- detection and analysis
- containment, eradication, and recovery
- **post-incident analysis**

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

- SNMP
- HTTP
- TNP
- **Fragmentation**

**83. Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?**

- confidentiality
- **integrity**
- availability
- complexity

**84. Which description of a retrospective malware detection is true?**

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

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

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

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

- Direction
- Result
- **Devices**
- Resources

**87. Which of the following is one of the main goals of data normalization?**

- To save duplicate logs for redundancy
- **To purge redundant data while maintaining data integrity**
- To correlate IPS and IDS logs with DNS
- To correlate IPS and IDS logs with Firewall logs

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

No.	Time	Source	Destination	Protocol	Length	Info
19	0.822656	192.124.249.9	10.0.2.15	TCP	52	443->50586 [SYN, ACK]
20	0.822702	10.0.2.15	192.124.249.9	TCP	56	50586->443 [ACK] Seq=1
21	0.822908	192.124.249.9	10.0.2.15	TCP	62	443->50586 [SYN, ACK]
22	0.822996	10.0.2.15	192.124.249.9	TCP	56	50586->443 [ACK] Seq=1
23	0.823212	10.0.2.15	192.124.249.9	TCP	261	50586->443 [PSH, ACK]
24	0.823373	192.124.249.9	10.0.2.15	TCP	52	443->50586 [ACK] Seq=1
25	0.823445	192.124.249.9	10.0.2.15	TCP	62	443->50586 [ACK] Seq=1
26	0.823617	192.124.249.9	10.0.2.15	TCP	62	443->50586 [ACK] Seq=1
27	0.837413	192.124.249.9	10.0.2.15	TCP	2792	443->50586 [PSH, ACK]
28	0.847206	10.0.2.15	192.124.249.9	TCP	56	50586->443 [ACK] Seq=1

Frame 24: 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: 50586 (50586), Dst Port: 443 (443), Seq: 1, Ack: 443, Len: 260  
 Data: [260 bytes]  
 Data: 16030106c8010000c403030e06ead078d17676c13ab46ebf...  
 [Length: 260]

0000	00 04 00 01 00 06 08 00	27 7a 3c 93 00 00 00 00	.....2e.....
0010	45 00 00 f5 40 7b 40 00	40 00 2b f3 0a 00 02 0f	E...H{0.0+.....
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 00 78	d1 76 76 c1 3a b4 6a bf	.....x.vv...n.
0050	e6 b8 b8 b2 ba 08 d0 d0	0d 38 fb 91 45 de fc aa	.....x...8...E.
0060	0b 6a f8 00 00 1e c0 2b	c0 2f cc a9 cc a8 c0 2c	n.....*/.....
0070	c0 30 c0 8a 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 0e	75 78 0d 69 0e 74 2e 63	.....www.lin-uxmint.c
00a0	6f 6d 80 17 00 00 ff 01	00 01 00 00 94 00 00 00	on.....
00b0	06 00 17 00 18 00 19 00	0b 00 62 01 00 00 23 00	.....@.....
00c0	00 32 74 00 00 00 10 00	17 00 15 02 68 32 08 73	.....yt.....h2.s
00d0	70 64 79 2f 33 2e 31 00	00 74 74 70 2f 31 2e 31	poly3.1.http://1
00e0	00 05 00 05 01 00 00 00	00 00 00 00 18 00 16 04	.....
00f0	01 05 01 06 01 02 01 04	03 05 03 00 03 02 03 05	.....
0100	02 04 02 02 02		.....

- TCP



- SSH
- HTTP
- SSL

**89. What is the correct about listening port?**

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

**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/ntpametag.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

- 1986
- 2318
- **2542**
- 2317

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

- **user-agent**
- **host**
- connection
- language
- handshake type

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

- **deterministic**
- exploratory
- probabilistic
- descriptive

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

- attack vector
- attack complexity
- **privileges required**
- user interaction

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

Date	Time Start	Duration	Proto	Src IP Addr:Port	→	Dest IP Addr:Port	Packets	Bytes	Flows
2018-10-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→	252.168.0.1:20151	1	82	1

- IDS log
- proxy log
- **NetFlow log**
- syslog

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

- confidentiality
- integrity
- **availability**
- complexity

**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

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

- True positive
- True negative
- **False positive**
- False negative

**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	0.011641	10.0.2.15	192.124.249.9	TCP	76	50588->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->50588 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50588->443 [ACK] Seq=1 Ack=
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->50588 [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	50588->443 [ACK] Seq=2086 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....43 {.....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	.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	.....#.....
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 32 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		.....

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  
 Internet Protocol v4 – Network protocol  
 TLSv1.2 – Application protocol

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

- Baseline score
- **Base score**
- **Environmental score**
- **Temporal score**

**100. Filtering ports in wireshark?**

- tcp.port = 80
- tcp.port equals 80
- **tcp.port != 80**
- tcp.port equal 80

**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?**

- **delivery**
- reconnaissance
- action on objectives
- installation
- exploitation

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

- CSIRT
- ICASI
- USIRP
- **PSIRT**

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

- Analysis Center
- National CSIRT
- **Internal CSIRT**
- Physical Security

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

- **install software to detect malware**

- **update antivirus signature**

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

- URL
- **hash**
- IP address
- destination port

**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?**

- Indicator
- **Precursor**
- online assault
- trigger

**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?**

- reconnaissance
- weaponization
- delivery
- **action on objectives**

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

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

**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.)**

- file size
- **domain names**
- dropped files
- signatures
- **host IP addresses**

**110. Which data type is protected under the PCI compliance framework?**

- credit card type
- **primary account number**
- health conditions
- provision of individual care

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

- tcp|udp] [src|dst] port
- [src|dst] net [{mask }|{len }]
- ether [src|dst] host
- **gateway host**

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

- **direct**
- corroborative
- indirect
- circumstantial
- textual

**113. What mechanism does the Linux operating system provide to control access to files?**

- privileges required
- user interaction
- **file permissions**
- access complexity

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

- PCAP
- tracer
- **running processes**
- hard drive configuration
- **applications**

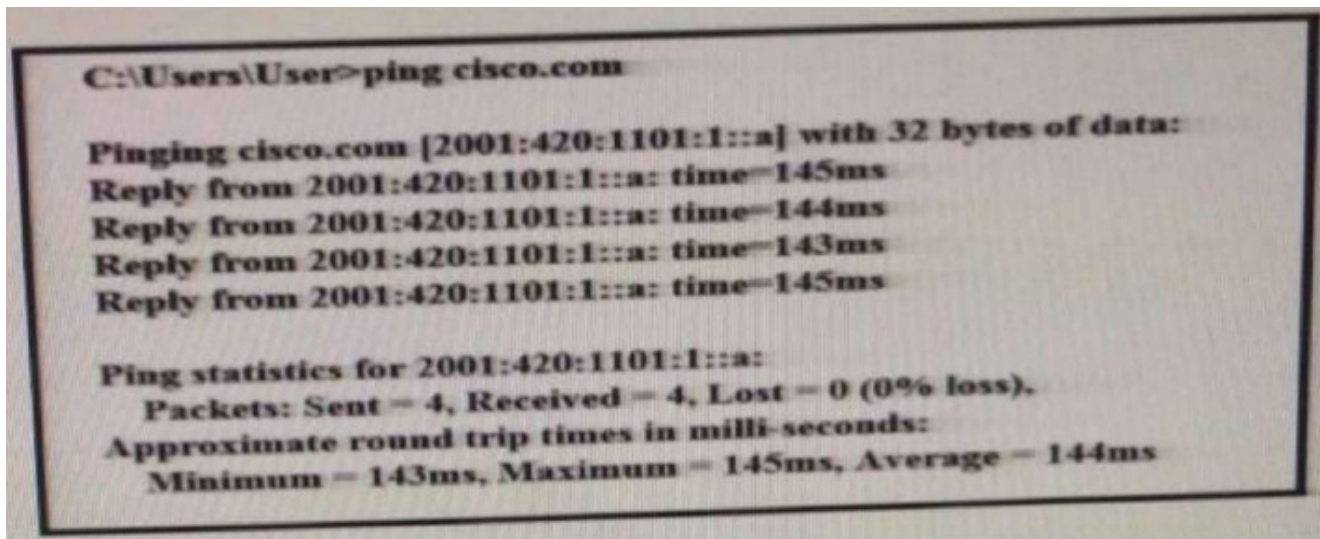
**115. In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model’?**

- victim demographics, incident description, incident details, discovery & response
- victim demographics, incident details, indicators of compromise, impact assessment
- actors, attributes, impact, remediation
- **actors, actions, assets, attributes**

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

- CPU utilization
- security policy
- temporary internet files
- **listening ports**

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



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

**120. Which option is unnecessary for determining the appropriate containment strategy according to NIST.SP80061r2?**

- **attack vector used to compromise the system**
- time and resources needed to implement strategy
- need for evidence preservation
- effectiveness of the strategy

**121. To which category do attributes belong within the VERIS schema**

- victim demographics
- incident tracking
- Discovery and response
- **incident description**

**123. How do you enforce network access control automatically?**

- IGMP
- SNMP
- **802.1X**
- Port Security

**124. Which Linux file system allows unlimited folder subdirectory structure**

- **ext4**
- ext3
- ext2
- NTFS

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

- Federal CSIRT
- Federal PSIRT
- **National CSIRT**
- National PSIRT

**126. Which type verification typically consists of using tools to compute the message digest of the original and copies data, then Fs to make sure that they are the same?**

- evidence collection order
- **data integrity**
- data preservation
- volatile data collection

**127. What define the roadmap for implementing the incident response correlation?**

- **Incident response plan**
- Incident response policy
- Incident response procedures

**128. Which expression creates a filter on a host IP address or name?**

- **[src|dst] host**
- [tcp|udp] [src|dst] port
- ether [src|dst] host
- gateway host

**129. Which analyzing technique describe the outcome as well as how likely each outcome is?**

- deterministic
- exploratory
- **probabilistic**
- descriptive

**130. Which value in profiling servers in a system is true?**

- it can identify when network performance has decreased
- **it can identify servers that have been exploited**
- it can identify when network ports have been connected
- it can protect the address space of critical hosts.

**131. Which event artifact can be used to identify HTTP GET requests for a specific file?**

- HTTP status code
- TCP ACK
- destination IP
- **URI**

**132. Which CVSSv3 metric value increases when conditions beyond the attacker's control must exist in order to exploit the vulnerability.**

- confidentiality
- attack vector
- availability
- **attack complexity**

**133. What is the common artifact that is used to uniquely identify a detected file?**

- **Hash**
- Timestamp
- File size



134. Refer to exhibit

%ASA-6-302015: Built inbound TCP connection 12879515 for outside:192.168.1.1/2196 to inside:192.168.2.2/22

Drag and drop the items from the left onto the correct 5-tuples on the right.

192.168.1.1	Source Port
192.168.2.2	Protocol
2196	Source IP
22	Destination IP
TCP	Destination Port

Answer:

192.168.1.1	TCP
192.168.2.2	2196
2196	192.168.1.1
22	192.168.2.2
TCP	22

**Explanation:**

192.168.1.1 = source ip

192.168.2.2 = destination ip

2196 = protocol

22 = Destination port

TCP = source port

**135. What are the metric values of the confidentiality based on the CVSS framework?**

- Low-high
- Low –Medium-high
- **High-Low-none**

**136. Which signature type results in a legitimate alert been dismissed?**

- True negative
- **False negative**
- True Positive
- False Positive

**137. Which incident handling is focused on minimizing the impact of an incident?**

- Scoping
- Reporting
- **Containment**
- Eradication
- Remediation

**139. According to NIST 86, which action describes the volatile data collection?**

- **Collect data before rebooting**
- Collect data while rebooting
- Collect data after rebooting
- Collect data that contains malware

**140. Which statement about collecting data evidence when performing digital forensics is true?**

- Allowing unrestricted access to impacted devices
- Not allowing items of evidence to be physically touch
- Powering off the device after collecting the data
- **It must be preserved and integrity checked**

**141. 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?**

- data analytics

- asset attribution
- **threat actor attribution**
- evidence collection

**142. You have a video of suspect entering your office the day your data has being stolen?**

- Direct evidence
- **Indirect**

**143. What define the roadmap for implementing the incident response correlative?**

- **Incident response plan**
- Incident response policy
- Incident response procedures

**145. Which precursor example is true?**

- Admin finds their password has been changed
- **A log scan indicating a port scan against a host**
- A network device configuration has been changed

**146. Which option can be addressed when using retrospective security techniques?**

- if the affected host needs a software update
- **how the malware entered our network**
- why the malware is still in our network
- if the affected system needs replacement

**147. What can be addressed when using retrospective security techniques?**

- if the affected host needs a software update
- **what is the malware working now**
- if the affected system needs replacement
- why the malware is still in our network

**148. What can be addressed when using retrospective security techniques?**

- if the affected host needs a software update
- **what system are affected**
- if the affected system needs replacement
- why the malware is still in our network

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

- Federal CSIRT
- Federal PSIRT
- **NationalCSIT**
- National PSIRT

**150. Which option is the logical source device for these events?**

<input type="checkbox"/>	POLICY-OTHER Outbound Teredo traffic detected (1:12065:5)	high	Potential Corporate Policy Violation
<input type="checkbox"/>	INDICATOR-SHELLCODE x86 inc ecx NOOP (1:1394:17)	high	Executable Code was Detected
<input type="checkbox"/>	INDICATOR-SHELLCODE x86 NOOP (1:648:18)	high	Executable Code was Detected
<input type="checkbox"/>	INDICATOR-SHELLCODE x86 inc ebx NOOP (1:1390:17)	high	Executable Code was Detected
<input type="checkbox"/>	INDICATOR-SHELLCODE base64 x86 NOOP (1:12800:10)	high	Executable Code was Detected
<input type="checkbox"/>	SERVER-OTHER Novell eDirectory LDAP server buffer overflow attempt (1:44604:1)	high	Attempted User Privilege Gain
<input type="checkbox"/>	SERVER-OTHER Microsoft Internet Authentication Service EAP-MSCHAPv2 authentication bypass attempt (1:16329:7)	high	Attempted User Privilege Gain

- web server
- NetFlow collector
- proxy server
- **IDS/IPS**

**151.**

**DOMAINS**

**-100 TO 100**

**THE HIGHER NUMBER IS SAFER**

ABC.COM

100

DEF.COM

-75

123.COM

0

**DOMAIN NAME**

**IP ADDRESSE**

ABC.COM

10.0.0.1

DEF.COM

209.165.201.130

123.COM

209.165.200.120

<b>MACHINE</b>	<b>LINK</b>
<b>10.1.0.1</b>	<b>209.165.201.130/443</b>
<b>172.11.5.5</b>	<b>10.0.0.1/80</b>
<b>XXXXX</b>	<b>209.165.200.130/80</b>

**Which machine risk to be infected or something like that ?**

- **10.1.0.1**
- 172.11.5.5

**152. Where HTTP normally used on forensic to find the browser type of the attacker?**

- **User agent**
- Referrer
- Host
- something language

**154. Which purpose of data mapping is true?**

- **Visualize data.**
- Find extra vulnerabilities.
- Discover the identities of attackers
- Check that data is correct

**155. 32 bit file system related to allocation address table ,which file system?**

- EXT4
- NTFS
- FAT16
- **FAT32**

**154. Which statement about collecting data evidence when performing digital forensics is true?**

- Allowing unrestricted access to impacted devices
- Not allowing items of evidence to be physically touch
- Powering off the device after collecting the data
- **It must be preserved and integrity checked**

**154. What is accomplished in the identification phase of incident handling?**

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

**155. What is the definition of confidentiality according to CVSSv3 framework?**

- It a metric that impact confidentiality of information managed by a software due to unsuccessful exploited vulnerability
- It a metric that impact confidentiality of information managed by a person due to successful exploited vulnerability
- **It a metric that impact confidentiality of information managed by a software due to successful exploited vulnerability**
- It a metric that impact confidentiality of information managed by a person due to unsuccessful exploited vulnerability

**156. Which statement describes the function provided by the Tor network?**

- It distributes user packets through load balancing.
- **It allows users to browse the Internet anonymously.**
- It conceals packet contents by establishing end-to-end tunnels.
- It manipulates packets by mapping IP addresses between two networks.

**Explanation:** Tor is a software platform and network of P2P hosts that function as Internet routers on the Tor network. The Tor network allows users to browse the Internet anonymously.

**157. Which two attacks target web servers through exploiting possible vulnerabilities of input functions used by an application? (Choose two.)**

- **SQL injection**
- port scanning
- port redirection
- trust exploitation
- **cross-site scripting**

**Explanation:** When a web application uses input fields to collect data from clients, threat actors may exploit possible vulnerabilities for entering malicious commands. The malicious commands that are executed through the web application might affect the OS on the web server. SQL injection and cross-site scripting are two different types of command injection attacks.