CCNA Cyber Ops (Version 1.1) – Chapter 12 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-12-exam-answers-full.html

May 13, 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 two technologies are used in the ELSA tool? (Choose two.)

- **MySQL** *
- CapME
- Suricata
- **Sphinx Search** *
- Security Onion

A, D. Enterprise Log Search and Archive (ELSA) is an enterprise-level tool for allowing searching and archiving of NSM data that originates from multiple sources. ELSA receives logs over Syslog-NG, stores logs in MySQL databases, and indexes using Sphinx Search.

2. What is the host-based intrusion detection tool that is integrated into Security Onion?

- **OSSEC** *
- Snort
- Sguil
- Wireshark

A. Integrated into the Security Onion, OSSEC is a host-based intrusion detection system (HIDS) that can conduct file integrity monitoring, local log monitoring, system process monitoring, and rootkit detection.

3. According to NIST, which step in the digital forensics process involves drawing conclusions from data?

- Data collection
- Examination

- **Analysis** *
- Reporting

C. NIST describes the digital forensics process as involving the following four steps:
Data collection: The identification of potential sources of forensic data and acquisition, handling, and storage of that data.
Examination: Assessing and extracting relevant information from the collected data. This may involve decompression or decryption of the data.
Analysis: Drawing conclusions from the data. Salient features, such as people, places, times, events, and so on, should be documented.
Reporting: Preparing and presenting information that resulted from the analysis. Reporting should be impartial and alternative explanations should be offered if appropriate.

4. Which two strings will be matched by the regular expression [24]? (Choose two.)

- Level1
- **Level2** *
- Level3
- **Level4** *
- Level5

B, D. Regular expressions allow forensics analysts to search through large quantities of text information for patterns of data. Some common operators used in regular expressions are the following:
$ End of a line
[] Any single value within the square brackets
* Preceding sub-expression zero or more times
[^1] Any character except those bound by the [^ and the]

5. Which alert classification indicates that exploits are not being detected by installed security systems?

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

A. A false negative classification indicates that a security system has not detected an actual exploit.

6. A cybersecurity analyst is going to verify security alerts using the Security Onion. Which tool should the analyst visit first?

- Bro
- **Sguil** *
- ELSA
- CapME

B. The primary duty of a cybersecurity analyst is the verification of security alerts. In the Security Onion, the first place that a cybersecurity analyst will go to verify alerts is Sguil because it provides a high-level console for investigating security alerts from a wide variety of sources.

7. What is the purpose for data normalization?

- To reduce the amount of alert data
- To make the alert data transmission fast
- **To simplify searching for correlated events** *
- To enhance the secure transmission of alert data

C. With data normalization various sources of data are combined into a common display format, which simplifies the searching for similar or relevant events.

8. Which term describes evidence that is in its original state?

- Corroborating evidence
- **Best evidence** *
- Indirect evidence
- Direct evidence

B. Evidence can be classified as follows:
Best evidence: This is evidence that is in its original state. It might be storage devices used by an accused or archives of files that can be proven to be unaltered.
Corroborating evidence: This is evidence that supports a propositionalready supported by initial evidence, therefore confirming the original proposition.
Indirect evidence: This evidence acts in combination with other facts to establish a hypothesis.

9. How is the hash value of files useful in network security investigations?

- **It helps identify malware signatures.**
- It is used to decode files.
- It is used as a key for encryption.
- It verifies confidentiality of files.

When ELSA is used to investigate downloaded files, the hash value of each file is created and stored with other information about the file. If a cybersecurity analyst is suspicious of the file, the hash value can be submitted to an online malware repository site to determine if the file is known malware.

10. Which tool is a Security Onion integrated host-based intrusion detection system?

- **OSSEC**
- Sguil
- ELSA
- Snort

OSSEC is a host-based intrusion detection system (HIDS) that is integrated into Security Onion and actively monitors host system operation.

11. Which type of evidence supports an assertion based on previously obtained evidence?

- direct evidence
- **corroborating evidence**
- best evidence
- indirect evidence

Corroborating evidence is evidence that supports a proposition already supported by initial evidence, therefore confirming the original proposition. Circumstantial evidence is evidence other than first-hand accounts of events provided by witnesses.

12. Which tool is developed by Cisco and provides an interactive dashboard that allows investigation of the threat landscape?

- Wireshark
- **Talos**
- Sguil
- Snort

Cisco Talos provides an interactive dashboard that allows investigation of the threat landscape.

13. Which term is used to describe the process of converting log entries into a common format?

- standardization
- **normalization**
- classification
- systemization

For processing log entries, data normalization can organize and convert data values in datasets from difference sources into common format. The normalization makes it easy for further data analysis and reporting.

14. According to NIST, which step in the digital forensics process involves extracting relevant information from data?

- collection
- **examination**
- analysis
- reporting

NIST describes the digital forensics process as involving the following four steps:

- Collection – the identification of potential sources of forensic data and acquisition, handling, and storage of that data.
- Examination – assessing and extracting relevant information from the collected data. This may involve decompression or decryption of the data.
- Analysis – drawing conclusions from the data. Salient features such as people, places, times, events, and so on should be documented.
- Reporting – preparing and presenting information that resulted from the analysis. Reporting should be impartial and alternative explanations should be offered if appropriate.

15. A law office uses a Linux host as the firewall device for the network. The IT administrator is adding a rule to the firewall iptables to block internal hosts from connecting to a remote device that has the IP address 209.165.202.133. Which command should the administrator use?

- **iptables -I FORWARD -p tcp -d 209.165.202.133 –dport 7777 -j DROP**
- iptables -I INPUT -p tcp -d 209.165.202.133 –dport 7777 -j DROP
- iptables -I PASS -p tcp -d 209.165.202.133 –dport 7777 -j DROP
- iptables -I OUTPUT -p tcp -d 209.165.202.133 –dport 7777 -j DROP

The firewall iptables uses the concepts of chains and rules to filter traffic:

- INPUT chain – handles traffic entering the firewall and destined to the firewall device itself
- OUTPUT chain – handles traffic originating within the firewall device itself and destined to somewhere else
- FORWARD chain – handles traffic originated somewhere else and passing through the firewall device

16. What procedure should be avoided in a digital forensics investigation?

- Secure physical access to the computer under investigation.
- **Reboot the affected system upon arrival.**
- Make a copy of the hard drive.
- Recover deleted files.

Digital forensic investigation is the science of collecting and examining electronic evidence that can evaluate damage to a computer as a result of an electronic attack or that can recover lost information from a system in order to prosecute a criminal. To prevent tampering and alteration of the suspect data, a data forensic analysis should be conducted on a copy of the suspect computer. Furthermore, restarting a computer may change or overwrite files and inadvertently destroy evidence.

17. Which statement describes a feature of timestamps in Linux?

- Human readable timestamps measure the number of seconds that have passed since January 1, 1970.
- All devices generate human readable and Unix Epoch timestamps.
- **It is easier to work with Unix Epoch timestamps for addition and subtraction operations.**
- Unix Epoch timestamps are easier for humans to interpret.

18. Which tool is included with Security Onion that is used by Snort to automatically download new rules?

- Sguil
- Wireshark
- ELSA
- **PulledPork**

PulledPork is a rule management utility included with Security Onion to automatically download rules for Snort.

19. Which tool would an analyst use to start a workflow investigation?

- ELSA
- Bro
- **Sguil**
- Snort

Sguil is a GUI-based application used by security analysts to analyze network security events.

20. What is indicated by a Snort signature ID that is below 3464?

- **The SID was created by Sourcefire and distributed under a GPL agreement.**

- This is a custom signature developed by the organization to address locally observed rules.
- The SID was created by members of EmergingThreats.
- The SID was created by the Snort community and is maintained in Community Rules.

Snort is an open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) developed by Sourcefire. It has the ability to perform real time traffic analysis and packet logging on Internet Protocol (IP) networks and can also be used to detect probes or attacks.

21. How does an application program interact with the operating system?

- accessing BIOS or UEFI
- **making API calls**
- sending files
- using processes

Application programs interact with an operating system through system calls to the OS application programming interface (API). These system calls allow access to many aspects of system operation such as software process control, file management, device management, and network access.

22. A threat actor has successfully breached the network firewall without being detected by the IDS system. What condition describes the lack of alert?

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

A false negative is where no alert exists and exploits are not being detected by the security systems that are in place.

23. Use the following scenario to answer the questions. A company has just had a cybersecurity incident. The threat actor or actors appeared to have a goal of network disruption and appeared to use a common security hack tool that overwhelmed a particular server with a large amount of traffic, which rendered the server inoperable.

a. How would a certified cybersecurity analyst classify this type of threat actor?

- **amateur**
- hacktivist
- state-sponsored
- terrorist

Explanation: Amateur or script kiddies use common existing tools found on the internet to launch attacks. Hacktivists disrupt services in protest against organizations or governments for a particular political or social idea. State-sponsored threat actors use cyberspace for industrial espionage or interfering with another country in some way. Terrorist groups attack for a specific cause.

b. The security team at this company has removed the compromised server and preserved it with the security hack still embedded. What type of evidence is this?

- **best**
- classified
- corroborating
- indirect

Explanation: Evidence is classified as direct or indirect. Direct evidence is that the accused was caught in the act, there is an eyewitness, or the evidence is indisputable. Three other types of evidence are best, corroborating, and indirect. Best is evidence in its original state. Corroborating evidence supports an assertion developed from best evidence. Indirect evidence provides support for a hypothesis.

c. Which type of attack was achieved?

- access
- **DoS**
- DDoS
- social engineering

Explanation: A denial-of-service attack results in an interruption of service to users, devices, or applications or all three. A direct DoS attack uses zombies and bots in order to have a coordinated attack from a multitude of sources. An access attack exploit known vulnerabilities in servers. Social engineering is a specific type of access attack toward an individual in an effort to get that individual to divulge information.

d. What would be the threat attribution in this case?

- evaluating the server alert data
- obtaining the most volatile evidence
- **determining who is responsible for the attack**
- reporting the incident to the proper authorities

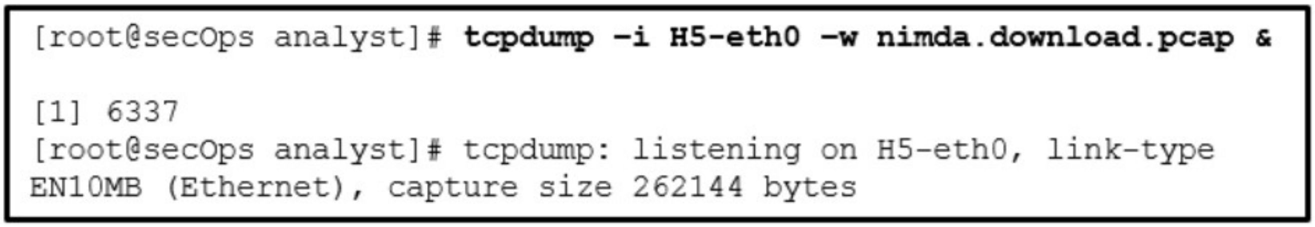
Explanation: Threat attribution refers to determining the individual, organization, or nation responsible for a successful intrusion or attack incident. The security investigation team correlates all the evidence in order to identify commonalities between tactics, techniques, and procedures (TPPs) for known and unknown threat actors.

e. What are three common tools used to carry out this type of attack? (Choose three.)

- ping sweep
- **TCP SYN flood**
- **buffer overflow**
- IP, MAC, and DHCP spoofing
- **smurf attack**
- man-in-the-middle

Explanation: Three tools used to carry out this type of attack are TCP SYN flood, buffer overflow, and smurf attack. All three attacks send data in order to overwhelm another network device. A ping sweep is used in reconnaissance. Man-in-the middle occurs when the threat actor collects data in order to read, modify, or redirect that data. IP, MAC, and DHCP spoofing attacks are used to falsify address data.

24. Refer to the exhibit. A network security specialist issues the command *tcpdump* to capture events. What is the function provided by the ampersand symbol used in the command?



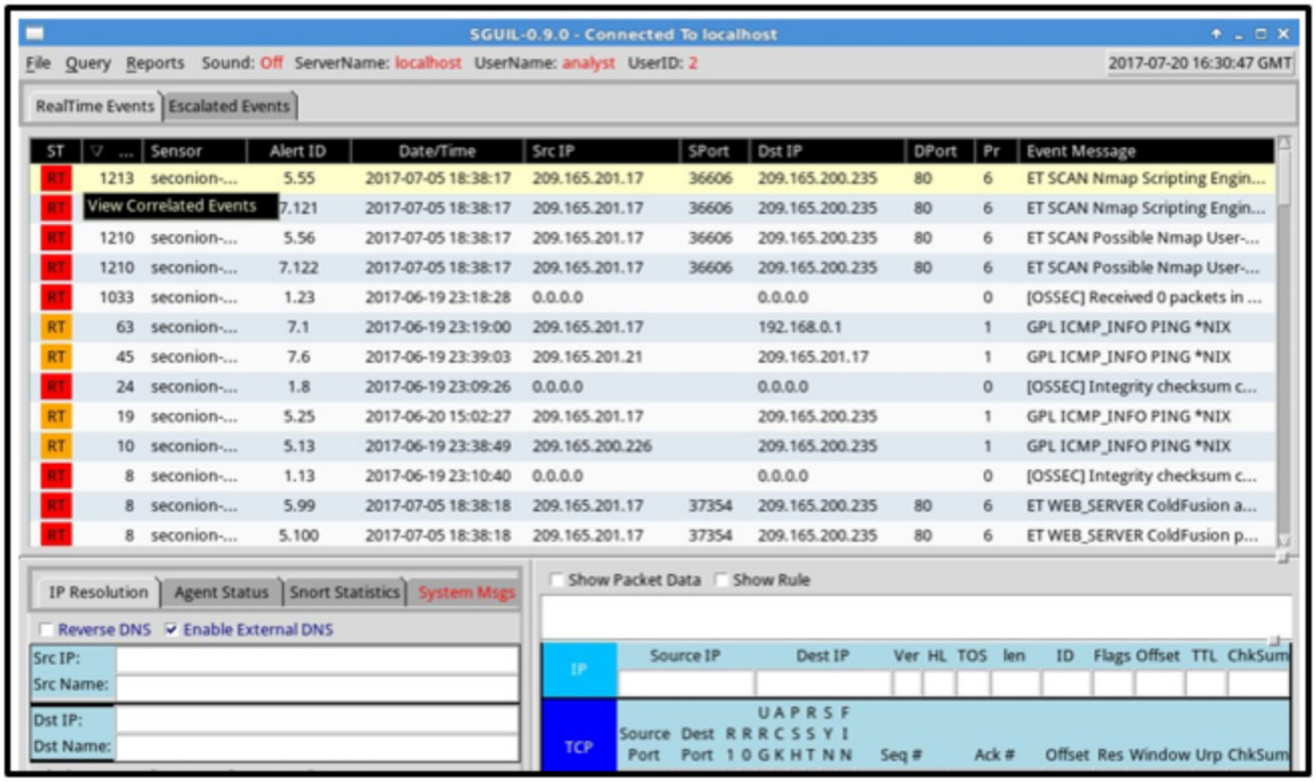
```
[root@secOps analyst]# tcpdump -i H5-eth0 -w nimda.download.pcap &

[1] 6337
[root@secOps analyst]# tcpdump: listening on H5-eth0, link-type
EN10MB (Ethernet), capture size 262144 bytes
```

- It instructs the tcpdump to capture data that starts with the symbol.
- **It tells the Linux shell to execute the tcpdump process in the background.**
- It tells the Linux shell to display the captured data on the console.
- It tells the Linux shell to execute the tcpdump process indefinitely.

The ampersand symbol tells the Linux shell to execute tcpdump in the background.

25. Refer to the exhibit. A cybersecurity analyst is using Sguil to verify security alerts. How is the current view sorted?



Sound: Off ServerName: localhost UserName: analyst UserID: 2

2017-07-20 16:30:47 GMT

ST	∇ ...	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1213	seconion-...	5.55	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Nmap Scripting Engin...
RT	View Correlated Events		7.121	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Nmap Scripting Engin...
RT	1210	seconion-...	5.56	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Possible Nmap User-...
RT	1210	seconion-...	7.122	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Possible Nmap User-...
RT	1033	seconion-...	1.23	2017-06-19 23:18:28	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in ...
RT	63	seconion-...	7.1	2017-06-19 23:19:00	209.165.201.17		192.168.0.1		1	GPL ICMP_INFO PING *NIX
RT	45	seconion-...	7.6	2017-06-19 23:39:03	209.165.201.21		209.165.201.17		1	GPL ICMP_INFO PING *NIX
RT	24	seconion-...	1.8	2017-06-19 23:09:26	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum c...
RT	19	seconion-...	5.25	2017-06-20 15:02:27	209.165.201.17		209.165.200.235		1	GPL ICMP_INFO PING *NIX
RT	10	seconion-...	5.13	2017-06-19 23:38:49	209.165.200.226		209.165.200.235		1	GPL ICMP_INFO PING *NIX
RT	8	seconion-...	1.13	2017-06-19 23:10:40	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum c...
RT	8	seconion-...	5.99	2017-07-05 18:38:18	209.165.201.17	37354	209.165.200.235	80	6	ET WEB_SERVER ColdFusion a...
RT	8	seconion-...	5.100	2017-07-05 18:38:18	209.165.201.17	37354	209.165.200.235	80	6	ET WEB_SERVER ColdFusion p...

☐ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

- by sensor number
- by source IP
- **by frequency**
- by date/time

The CNT column, between the ST and Sensor columns, displays the frequency of alerts. By sorting with frequency, the analyst will get a better sense of what has happened on the network.

26. Which three procedures in Sguil are provided to security analysts to address alerts? (Choose three.)

- **Expire false positives.**
- Pivot to other information sources and tools.
- Construct queries using Query Builder.
- **Escalate an uncertain alert.**
- Correlate similar alerts into a single line.
- **Categorize true positives.**

Sguil is a tool for addressing alerts. Three tasks can be completed in Sguil to manage alerts:

Alerts that have been found to be false positives can be expired.

An alert can be escalated if the cybersecurity analyst is uncertain how to handle it.

Events that have been identified as true positives can be categorized.

27. Which two strings will be matched by the regular expression? (Choose two.) Level[^12]

- **Level4**
- **Level3**
- Level2
- Level1
- Level12

Regular expressions allow forensics analysts to search through large quantities of text information for patterns of data. Some common operators used in regular expressions are as follows:

$ End of a line.
[] Any single value within the square brackets.
* Preceding sub-expression zero or more times.
[^1] Any character except those bound by the [^ and the].

28. Which statement describes the status after the Security Onion VM is started?

- SGUIL becomes enabled via the sudo sguil -e terminal command.
- Awk becomes enabled via the sudo awk terminal command.
- Pullpork is used by ELSA as an open source search engine.
- **Snort is enabled by default.**

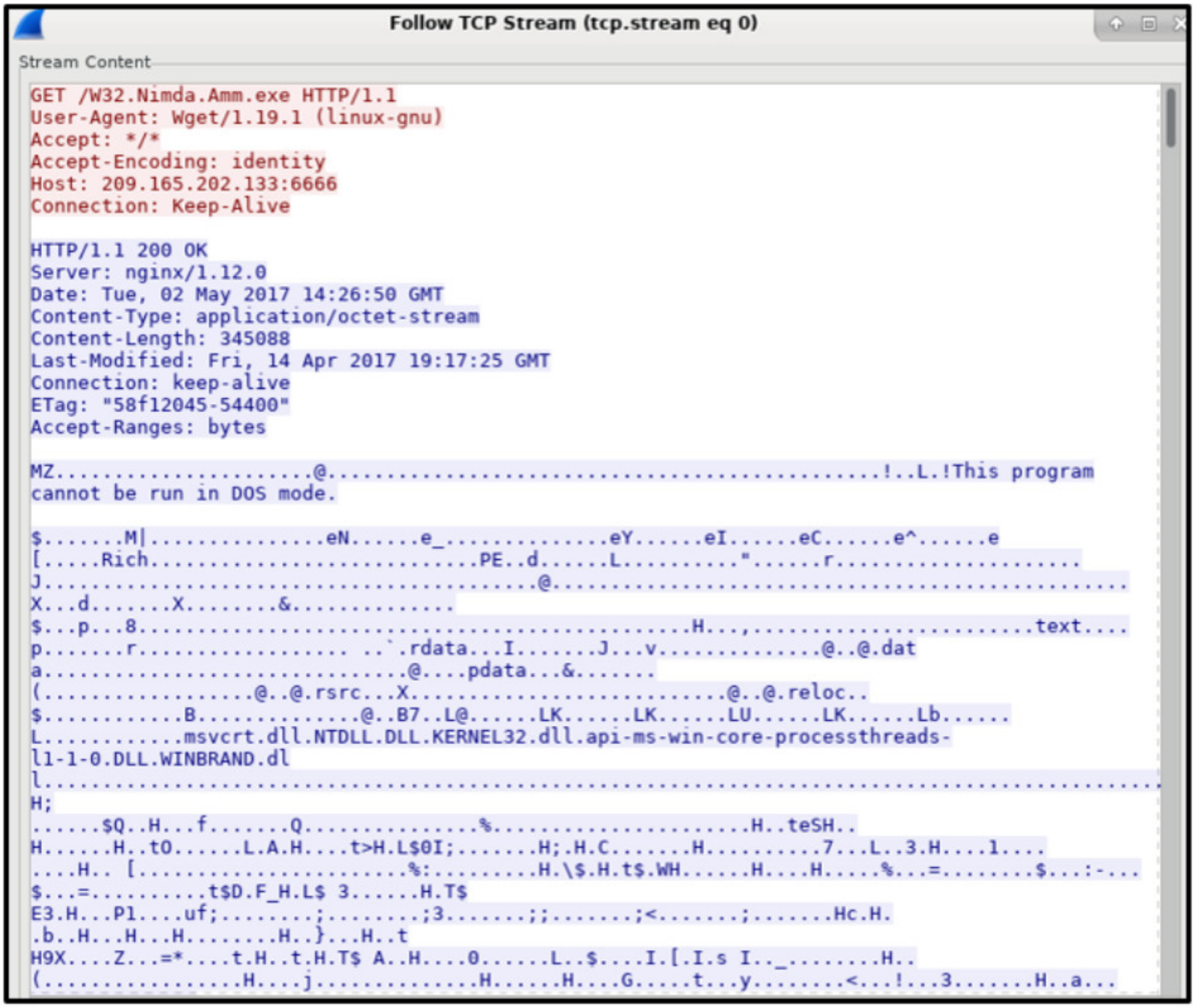
Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It contains many security tools like Snort, Suricata, Bro, and ELSA.

29. What are the three core functions provided by the Security Onion? (Choose three.)

- business continuity planning
- **full packet capture**
- **alert analysis**
- **intrusion detection**
- security device management
- threat containment

Security Onion is an open source suite of Network Security Monitoring (NSM) tools for evaluating cybersecurity alerts. For cybersecurity analysts the Security Onion provides full packet capture, network-based and host-based intrusion detection systems, and alert analysis tools.

30. Refer to the exhibit. A network security analyst is using the Follow TCP Stream feature in Wireshark to rebuild the TCP transaction. However, the transaction data seems indecipherable. What is the explanation for this?



```
GET /W32.Nimda.Amm.exe HTTP/1.1
User-Agent: Wget/1.19.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 209.165.202.133:6666
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.12.0
Date: Tue, 02 May 2017 14:26:50 GMT
Content-Type: application/octet-stream
Content-Length: 345088
Last-Modified: Fri, 14 Apr 2017 19:17:25 GMT
Connection: keep-alive
ETag: "58f12045-54400"
Accept-Ranges: bytes

MZ.....................@..............................................!..L.!This program
cannot be run in DOS mode.

$.......M|..............eN......e_..............eY......eI......eC......e^......e
[.....Rich..........................PE..d......L.........."......r....................
J.............................................@................................................
X...d.......X........&.............
$...p...8...............................................H...,.......................text....
p.......r................. ..`.rdata...I.......J...v..............@..@.dat
a...............................@....pdata...&.......
(..................@..@.rsrc...X..........................@..@.reloc..
$...........B..............@..B7..L@......LK......LK......LU......LK......Lb......
L...........msvcrt.dll.NTDLL.DLL.KERNEL32.dll.api-ms-win-core-processthreads-
l1-1-0.DLL.WINBRAND.dl
l..............................................................................................
H;
......$Q..H...f.......Q...............%.......................H..teSH..
H......H..tO......L.A.H....t>H.L$0I;.......H;.H.C.......H..........7...L..3.H....1....
....H.. [......................%:.........H.\$.H.t$.WH......H....H.....%...=........$...:-...
$...=.........t$D.F_H.L$ 3......H.T$
E3.H...Pl....uf;........;........;3.......;;.......;<.......;.......Hc.H.
.b..H...H...H........H..}...H..t
H9X....Z...=*....t.H..t.H.T$ A..H....0......L..$....I.[.I.s I.._........H..
(.................H....j.............H......H....G.....t...y........<...!...3.......H..a...
```

- The transaction data is encoded with Base64.
- **The transaction data is a binary file.**
- The data shown is line noise.
- The transaction data is corrupted.

The host is downloading W32.Nimda.Amm.exe, a binary file. Wireshark does not know how to represent it. The displayed symbols are the best guess at making sense of the binary data while decoding it as text.

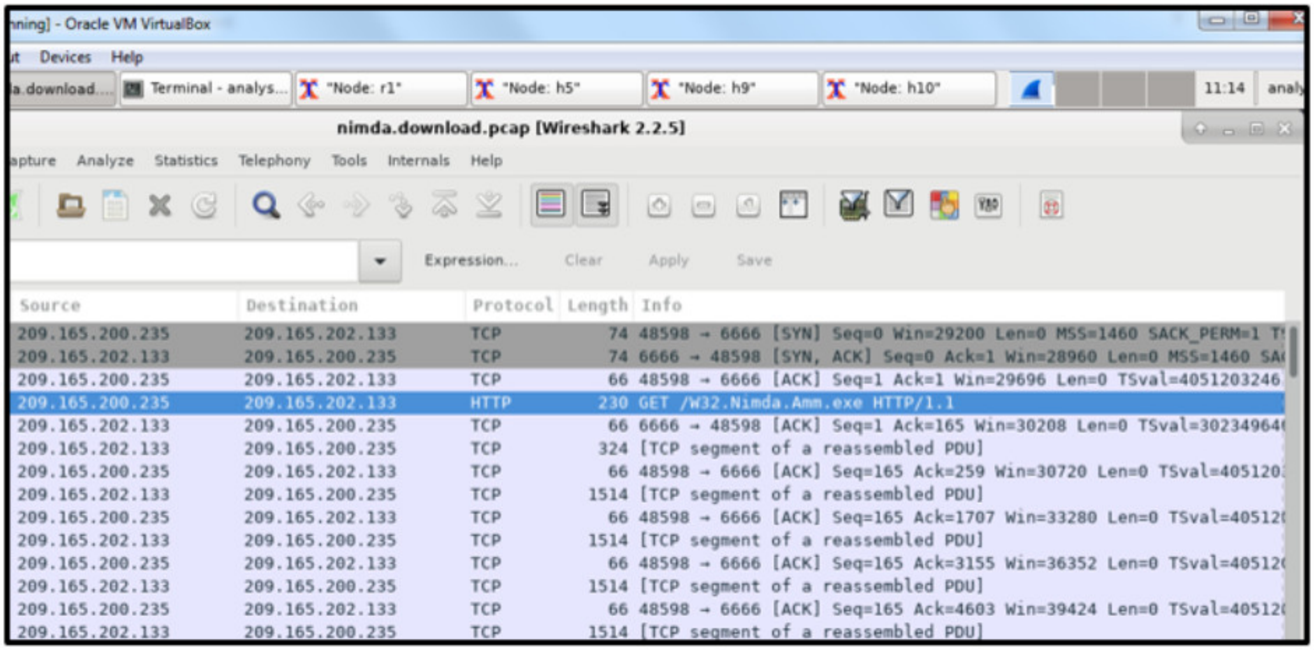
31. What is the tool that has alert records linked directly to the search functionality of the Enterprise Log Search and Archive (ELSA)?

- **Sguil**
- Wireshark

- CapME
- Snort

The Enterprise Log Search and Archive (ELSA) is an enterprise-level tool for allowing searching and archiving of NSM data. Searches can be executed by pivoting from Sguil to ELSA as its search functionality is directly linked to Sguil alert records.

32. Refer to the exhibit. A network security analyst is examining captured data using Wireshark. The captured frames indicate that a host is downloading malware from a server. Which source port is used by the host to request the download?


nning] - Oracle VM VirtualBox
t Devices Help
a.download... Terminal - analys... "Node: r1" "Node: h5" "Node: h9" "Node: h10" 11:14 analy
nimda.download.pcap [Wireshark 2.2.5]
apture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

```
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 T
209.165.202.133  209.165.200.235  TCP         74 6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA
209.165.200.235  209.165.202.133  TCP         66 48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=4051203246
209.165.200.235  209.165.202.133  HTTP       230 GET /W32.Nimda.Amn.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=30234964
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=405120
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=40512
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=40512
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=40512
209.165.202.133  209.165.200.235  TCP       1514 [TCP segment of a reassembled PDU]
```

- 66
- 1514
- 6666
- **48598**

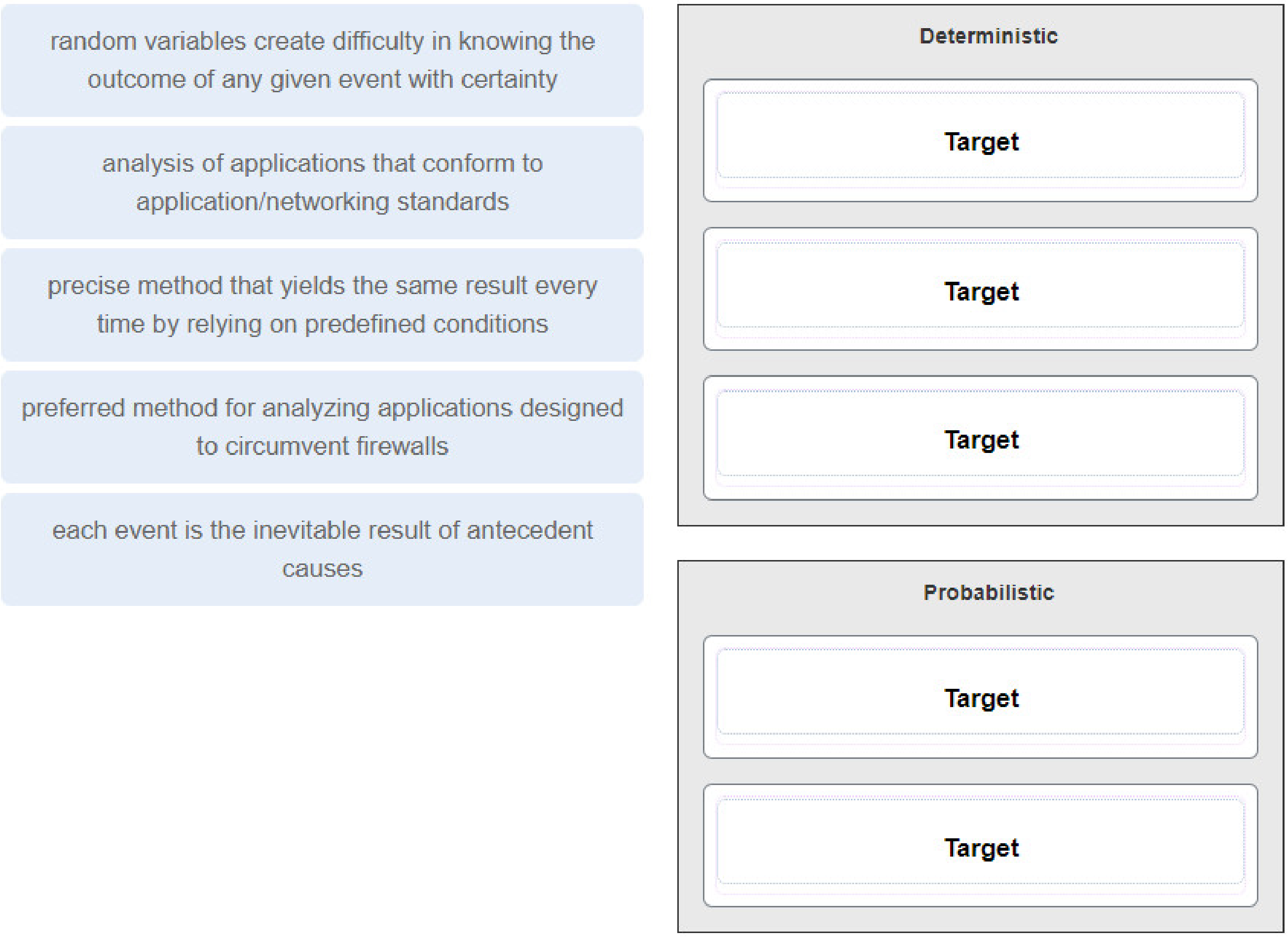
During the TCP three-way handshake process, the output shows that the host uses source port 48598 to initiate the connection and request the download.

33. Which two types of unreadable network traffic could be eliminated from data collected by NSM? (Choose two.)

- routing updates traffic
- STP traffic
- **SSL traffic**
- **IPsec traffic**
- broadcast traffic

To reduce the huge amount of data collected so that cybersecurity analysts can focus on critical threats, some less important or unusable data could be eliminated from the datasets. For example, encrypted data, such as IPsec and SSL traffic, could be eliminated because it is unreadable in a reasonable time frame.

34. Match the characteristic to the method of security analysis.



random variables create difficulty in knowing the outcome of any given event with certainty

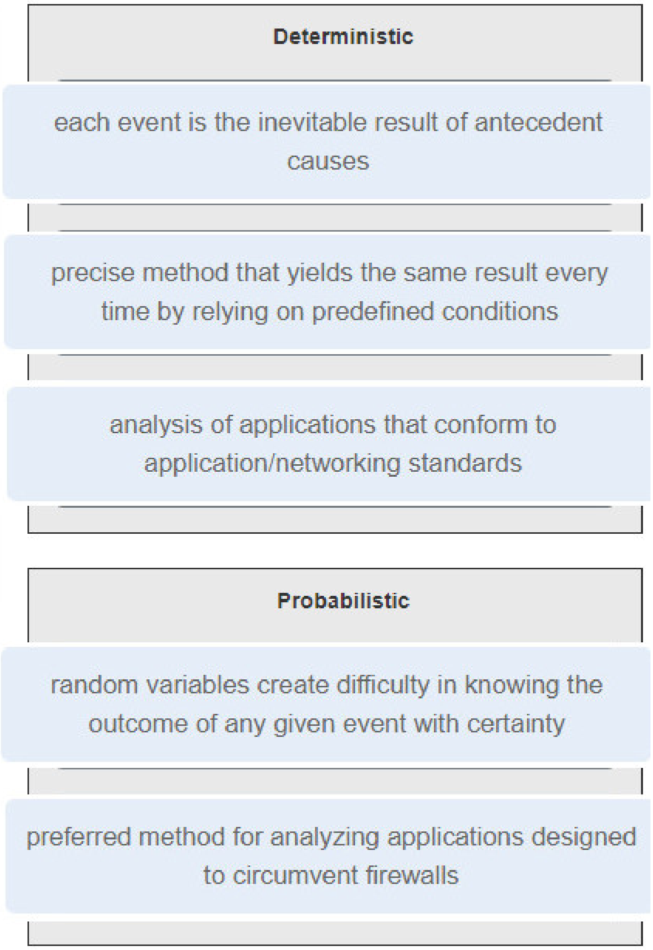
analysis of applications that conform to application/networking standards

precise method that yields the same result every time by relying on predefined conditions

preferred method for analyzing applications designed to circumvent firewalls

each event is the inevitable result of antecedent causes

Answer



Deterministic

each event is the inevitable result of antecedent causes

precise method that yields the same result every time by relying on predefined conditions

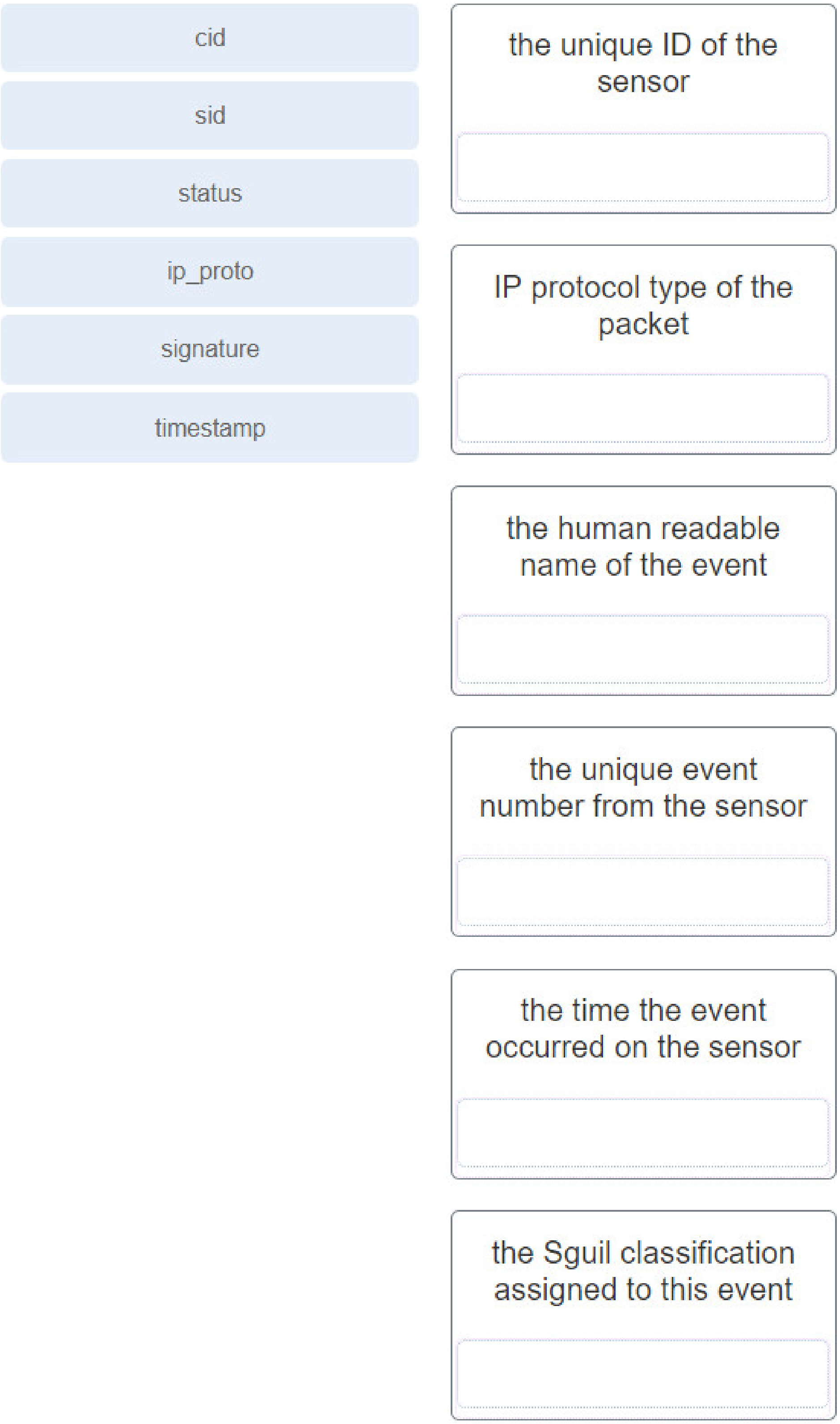
analysis of applications that conform to application/networking standards

Probabilistic

random variables create difficulty in knowing the outcome of any given event with certainty

preferred method for analyzing applications designed to circumvent firewalls

35. Match the field in the Event table of Sguil to the description.



cid

sid

status

ip_proto

signature

timestamp

the unique ID of the sensor

IP protocol type of the packet

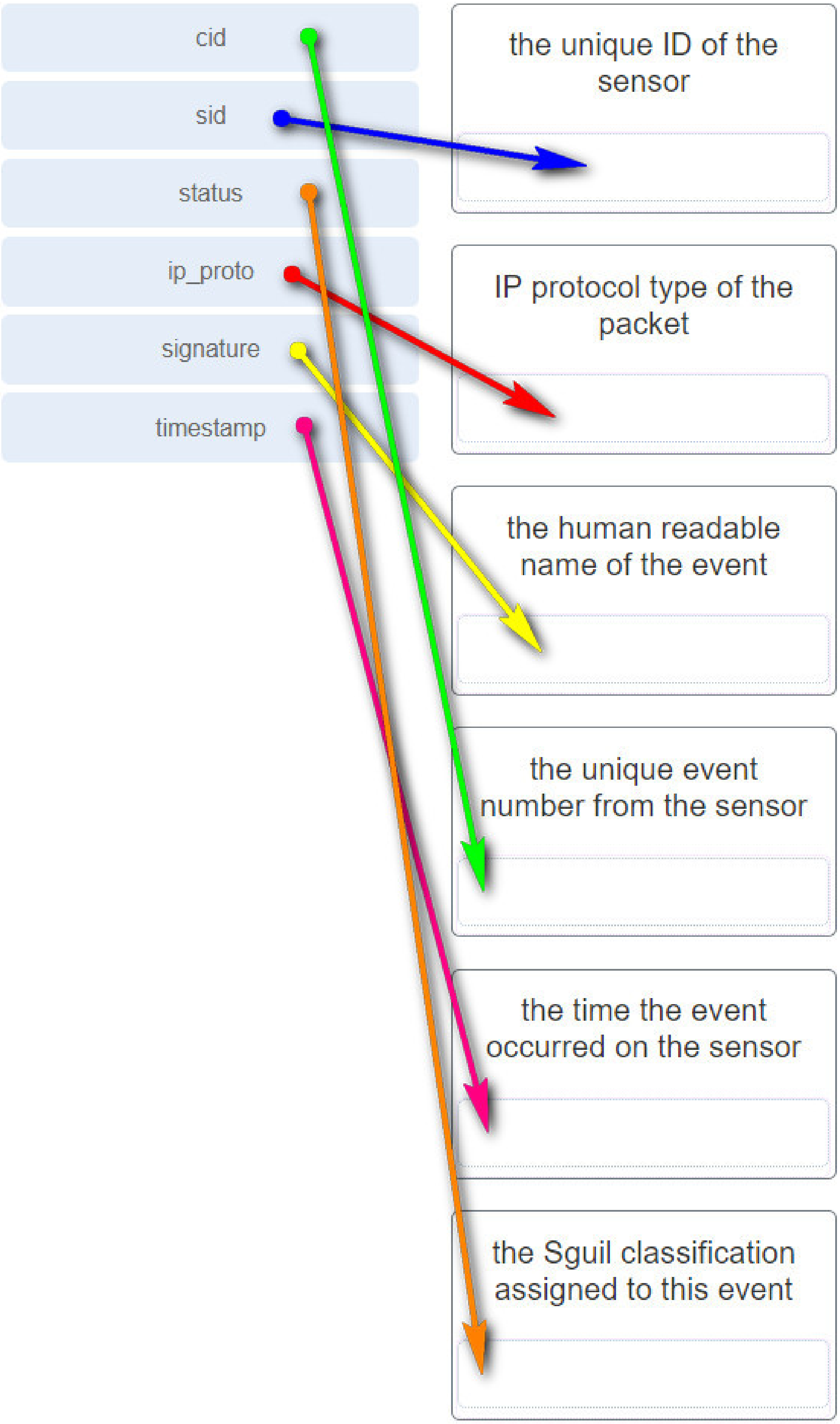
the human readable name of the event

the unique event number from the sensor

the time the event occurred on the sensor

the Sguil classification assigned to this event

Answer



cid

sid

status

ip_proto

signature

timestamp

the unique ID of the sensor

IP protocol type of the packet

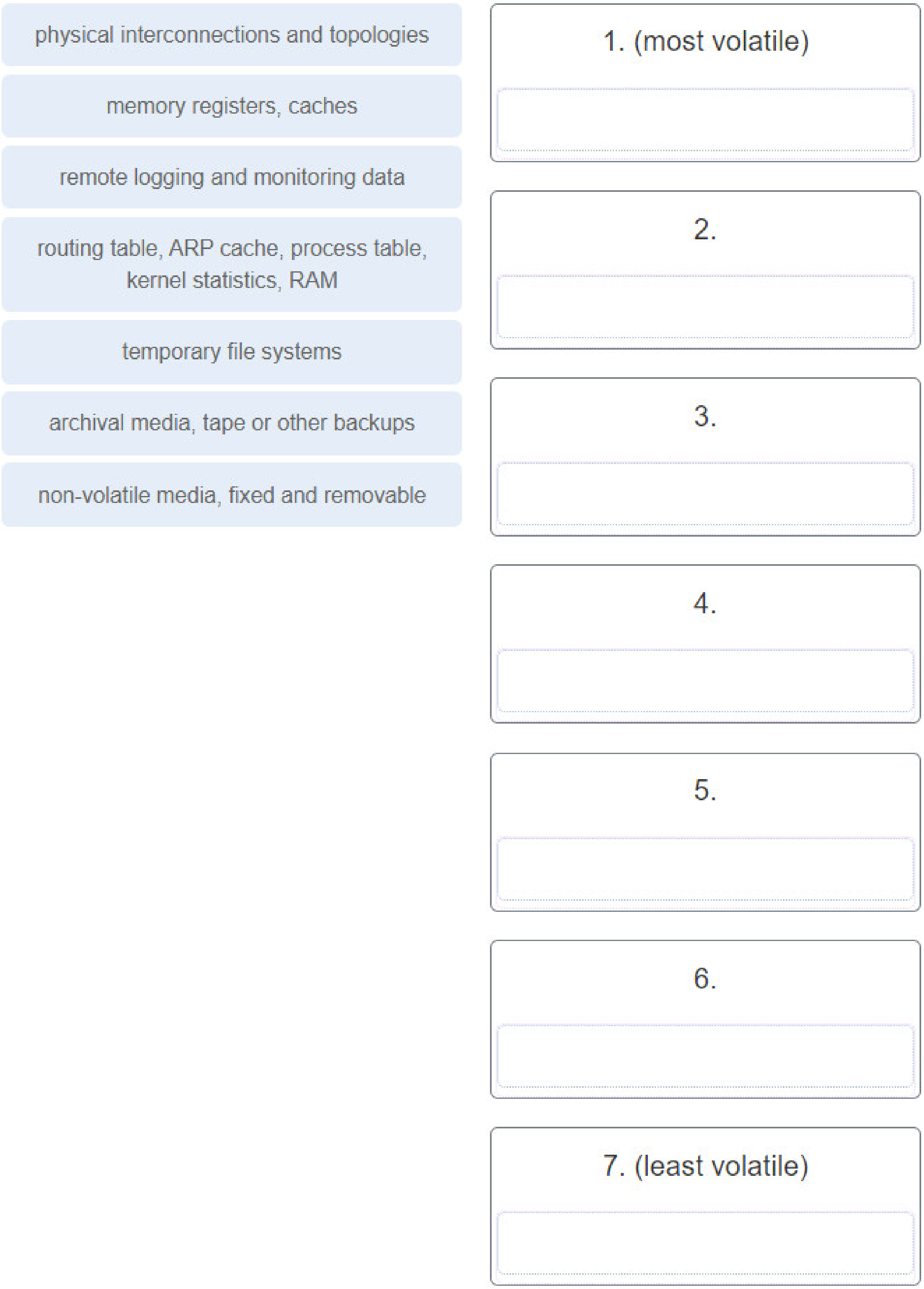
the human readable name of the event

the unique event number from the sensor

the time the event occurred on the sensor

the Sguil classification assigned to this event

36. Place the evidence collection priority from most volatile to least volatile as defined by the IETF guidelines.



physical interconnections and topologies

memory registers, caches

remote logging and monitoring data

routing table, ARP cache, process table, kernel statistics, RAM

temporary file systems

archival media, tape or other backups

non-volatile media, fixed and removable

1. (most volatile)

2.

3.

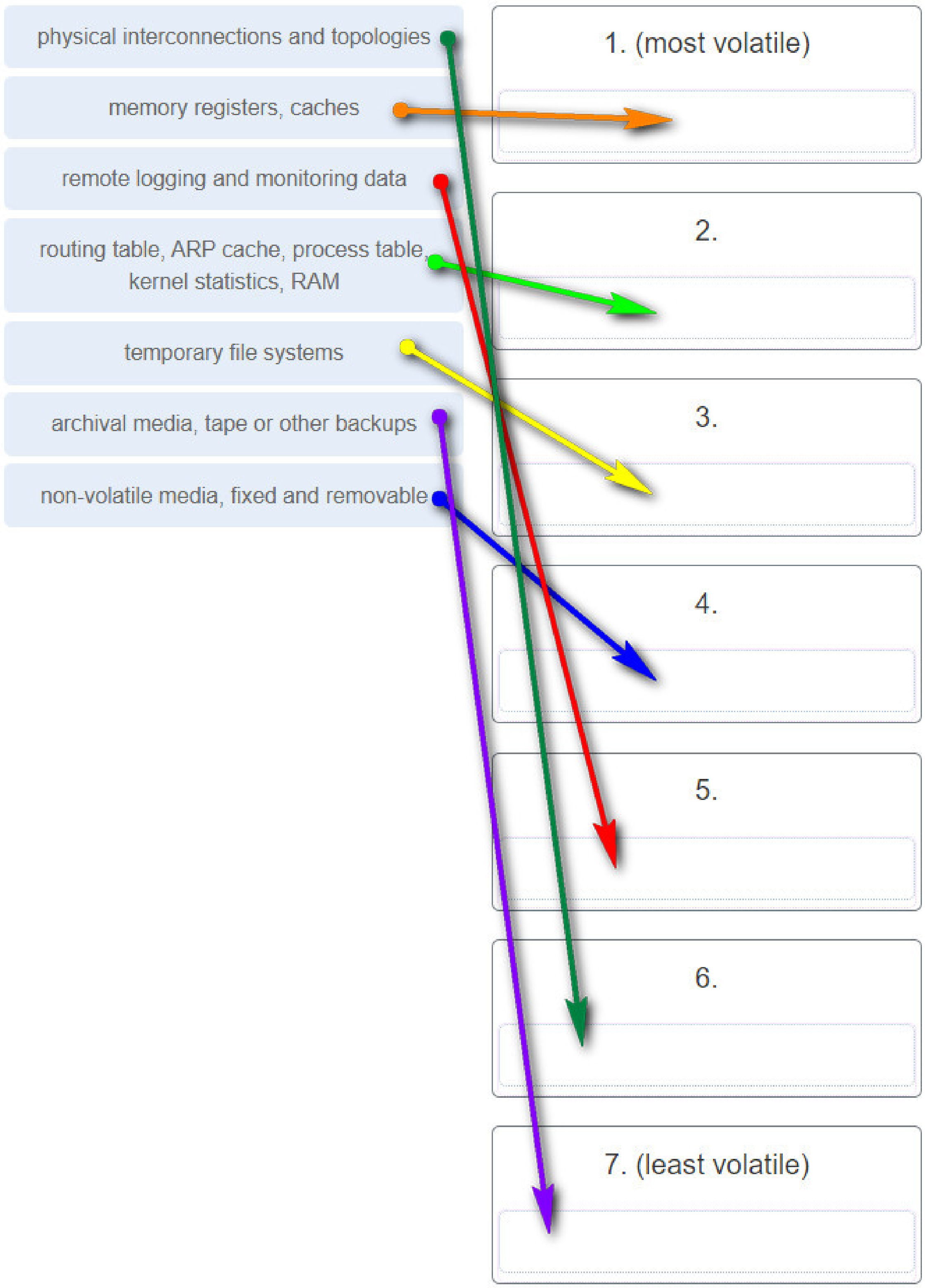
4.

5.

6.

7. (least volatile)

Answer



physical interconnections and topologies

memory registers, caches

remote logging and monitoring data

routing table, ARP cache, process table, kernel statistics, RAM

temporary file systems

archival media, tape or other backups

non-volatile media, fixed and removable

1. (most volatile)

2.

3.

4.

5.

6.

7. (least volatile)