Exam Report: 2.6.7 Practice Questions

Date: 1/14/2020 10:24:01 am
Time Spent: 4:21

Candidate: Garsteck, Matthew
Login: mGarsteck

## Overall Performance

Your Score: 69%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

## Individual Responses

**Question 1:** Correct

After an intrusion has occurred and the intruder has been removed from the system, which of the following is the best next step or action to take?

○ Restore and repair any damage

➡ ◉ Back up all logs and audits regarding the incident

○ Update the security policy

○ Deploy new countermeasures

### Explanation

The first step after an intrusion is to retain the documentation about the incident. Making backups of the logs and audits will ensure that future investigations will have sufficient information regarding the incident. If you were unable to discover the identity of the perpetrator or means of attack, future review of the evidence or comparison with other incidents may reveal important details or patterns.

After audit trails are secured, then repairing damage, deploying new countermeasures, and updating the security policy are reasonable activities to perform.

### References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_01]

**Question 2:** Correct

Which of the following is an important aspect of evidence gathering?

○ Purging transaction logs

○ Restoring damaged data from backup media

➡ ◉ Backing up all log files and audit trails

○ Monitoring user access to compromised systems

### Explanation

When gathering evidence, it is important to make backup copies of all log files and audit trails. These files will help reconstruct the events leading up to the security violation. They often include important clues to the intruder's identity.

Users should not have access to compromised systems while evidence gathering is taking place. Damaged data should not be restored while evidence gathering is taking place. Transaction logs should not be purged while evidence gathering is taking place.

### References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_02]

**Question 3:** Incorrect

During a recent site survey, you found a rogue wireless access point on your network. Which of the following actions should you take *first* to protect your network while still preserving evidence?

➡ ○ Disconnect the access point from the network

○ See who is connected to the access point and attempt to find the attacker

● ~~Run a packet sniffer to monitor traffic to and from the access point~~

○ Connect to the access point and examine its logs for information

## Explanation

The first step in responding to an incident is to take actions to stop the attack and contain or limit the damage. For example, if the attack involves a computer system attached to the network, the first step might be to disconnect it from the network. Although you want to preserve as much information as possible to assist in later investigations, it might be better to stop the attack, even if doing so alerts the attacker or results in the loss of evidence regarding the attack.

After containing a threat, forensic investigation can be performed on computer systems to gather evidence and identify the methods used in the attack.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_03]

**Question 4:** Incorrect

You have discovered a computer that is connected to your network and was used for an attack. You have disconnected the computer from the network to isolate it and stop the attack.

What should you do next?

○ Stop all running processes

➡ ○ Perform a memory dump

○ Clone the hard drive

● ~~Make a hash of the hard drive~~

## Explanation

Some evidence might exist in active memory and could be lost if the computer is shut down. Save the contents of memory by taking one of the following actions:

- Save and extract the page file.
- Do a complete memory dump to save the contents of physical RAM. This will lose the page file, but preserve the physical memory.

Stopping running processes if necessary, making a hash of the hard drive, and cloning the hard drive should be performed after volatile data (information in memory) is captured.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_04]

**Question 5:** Correct

You are conducting a forensic investigation. The attack has been stopped. Which of the following actions should you perform *first*?

➡ ● Document what's on the screen

○ Stop all running processes

○ Turn off the system

○ Remove the hard drive

## Explanation

Preserving evidence while conducting a forensic investigation is a trade-off. Any attempt to collect evidence may actually destroy the very data necessary to identify an attack or attacker. Of the choices given, documenting what's on the screen is the least intrusive and the least likely to destroy critical evidence. Halting, disassembling, or stopping running processes may erase the data you need to track the intruder.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_05]

▼ **Question 6:** Correct

Which method can you use to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive collected as evidence?

➡ ● Hashing

○ Serial number notation

○ File directory listing

○ Photographs

## Explanation

Hashing is the method used to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive collected as evidence.

File directory listings, photographs, and serial number notation are not sufficient methods for verifying hard drive cloning.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_06]

▼ **Question 7:** Correct

When duplicating a drive for forensic investigation purposes, which of the following copying methods is most appropriate?

○ File-by-file copying

○ Drive mirroring

➡ ● Bit-level cloning

○ Active sector cloning

## Explanation

Only bit-level cloning is recognized as a sufficient method for duplicating hard drives for forensic investigation purposes.

File-by-file copying, active sector cloning, and drive mirroring are all insufficient copying methods for forensic investigation purposes. These methods fail to duplicate data that has been deleted or that is stored in the slack space of the drive.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_07]

▼ **Question 8:** Correct

How can a criminal investigator ensure the integrity of a removable media device found while collecting evidence?

○ Reset the file attributes on the media to read-only

○ Enable write protection

○ Write a log file to the media

➡ ● Create a checksum using a hashing algorithm

## Explanation

To protect or ensure the integrity of collected digital evidence, an investigator should create a checksum using a hashing algorithm. In the future, the same hashing algorithm can be used to create another checksum. Then the two values are compared. If the checksums are identical, then the media was not altered.

Not all removable media has write protection switches, and it is possible for software to circumvent these physical restrictions. Writing a new file to the media or altering the settings on files on the media is a direct violation of integrity.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_08]

**Question 9:** Incorrect

You manage the network for your company. You have recently discovered information on a computer hard drive that might indicate evidence of illegal activity. You want to perform forensic activities on the disk to see what kind of information it contains.

What should you do *first*?

● ~~Run forensic tools to examine the hard drive contents~~

○ Fire the employee who uses the computer

○ Obtain a search warrant

➡ ○ Make a bit-level copy of the disk

## Explanation

Before conducting an investigation of data on a disk, you should create a hash of the disk, create a bit-level copy of the disk, and then create a hash of your copy of the disk. Perform any investigative activities on your copy of the disk, not on the original disk.

The hash of the original disk allows you to retain the original disk and prove that the original has not been altered, either by yourself during the investigations, or by someone else after the disk was discovered. The hash of your copy of the disk proves that your copy is the same as the original.

For business computers, you do not need a search warrant before examining the disk, although you should have a written policy that lets users know that you have this right for company property. You should only fire an employee after evidence has been gathered. Even then, it it is difficult to do without legal repercussions.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_09]

**Question 10:** Correct

What is the best definition of a security incident?

○ Interruption of productivity

➡ ● Violation of a security policy

○ Criminal activity

○ Compromise of the CIA of resources

## Explanation

The best definition of a security incident is a violation of a security policy.

Criminal activity, compromise of CIA, and productivity interruptions are all violations of security policy. Thus, they are specific examples of security incidents, rather than a universal definition.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_10]

▼ **Question 11:** Correct

What is the most important element related to evidence in addition to the evidence itself?

○ Photographs of the crime scene

○ Witness testimony

○ Completeness

➡ ● Chain of custody document

## Explanation

The chain of custody document is the most important item related to the evidence in addition to the evidence itself.

Nothing is more important than the chain of custody document, including photographs. Witness testimony can be helpful, but it is not more important than the chain of custody document. Completeness of the evidence is beneficial, but not as beneficial as a reliable chain of custody document.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_12]

▼ **Question 12:** Incorrect

The chain of custody is used for which purposes?

● ~~Retaining evidence integrity~~

➡ ○ Listing people coming into contact with evidence

○ Identifying the owner of the evidence

○ Detailing the timeline between creation and discovery of evidence

## Explanation

The chain of custody is used to track the people who came in contact with evidence. The chain of custody starts at the moment evidence is discovered. It lists the identity of the person who discovered, logged, gathered, protected, transported, stored, and presented the evidence. The chain of custody helps to ensure the admissibility of evidence in court.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_13]

▼ **Question 13:** Correct

You have been asked to draft a document related to evidence-gathering that contains details about personnel in possession and control of evidence from the time of discovery up through the time of presentation in court. What type of document is this?

➡ ● Chain of custody

○ CPS (certificate practice statement)

○ FIPS-140

○ Rules of evidence

## Explanation

The chain of custody is a document related to evidence-gathering that contains details about personnel in possession and control of evidence from the time of discovery up through the time of presentation in court.

A CPS (certificate practice statement) is a document written by a certificate authority outlining their certificate handling, management, and administration procedures. FIPS-140 is a government standard that defines procedures, hardware, and software that can be employed when performing forensic investigations of cyber crime. The rules of evidence are the restrictions that must be adhered to in order to ensure the admissibility of collected evidence.

## References

LabSim for Security Pro, Section 2.6.
[All Questions SecPro2017_v6.exm INCIDENT_RESP_14]