Exam Report: 13.2.4 Practice Questions

Date: 4/15/2020 4:08:29 pm
Time Spent: 4:53

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 14%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

A security incident is currently occurring on the company network. You discover that the attack involves a computer system that is attached to the network. You're unsure what kind of damage is being done to the network systems or data.

Which of the following actions should you take FIRST?

● ~~Examine the active computer system to analyze the live network connection, memory contents, and running programs.~~

○ Document and photograph the entire scene of the crime including the current state of the attached computer system.

➡ ○ Stop the attack and contain the damage by disconnecting the system from the network.

○ Determine whether you have the expertise to conduct an investigation, or whether you need to call in additional help.

Explanation

The first step in responding to an incident should be to take actions to stop the attack and contain the damage. 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 is better to stop the attack, even if doing so alerts the attacker or results in the loss of evidence regarding the attack.

After containing the damage, subsequent steps you can take include, but are not limited to, the following:

- Examine the active computer system to analyze the live network connection, memory contents, and running programs.
- Document and photograph the entire scene of the crime, including the current state of the attached computer system.
- Determine whether you have the expertise to conduct an investigation, or whether you need to call in additional help.

References

TestOut PC Pro - 13.2 Incident Response
[e_response_pp6_exam.xml Q_RISK_RESP_FCTS_01]

The chain of custody is used for what purposes?

- ➡ ○ Retaining evidence integrity by identifying people coming into contact with evidence
- ○ Maintaining compliance with federal privacy laws
- ○ Detailing the timeline between creation and discovery of evidence
- ● ~~Identifying the owner 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 insure the admissibility of evidence in court.

References

TestOut PC Pro - 13.2 Incident Response
[e_response_pp6.exam.xml Q_RISK_RESP_FCTS_02]

▼ **Question 3:** Incorrect

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?

- ● ~~CPS (certificate practice statement)~~
- ○ Rules of evidence
- ➡ ○ Chain of custody
- ○ FIPS-140

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

TestOut PC Pro - 13.2 Incident Response
[e_response_pp6.exam.xml Q_RISK_RESP_FCTS_03]

▼ **Question 4:** Incorrect

A technician was able to stop a security attack on a user's computer.

○ Remove the hard drive

➡ ○ Document what's on the screen

● ~~Stop all running processes~~

○ Turn off the system

Explanation

Preserving evidence while conducting a forensic investigation is a trade-off. Any attempt to collect evidence may actually destroy the very data needed 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 evidence.

References

TestOut PC Pro - 13.2 Incident Response
[e_response_pp6.exam.xml Q_RISK_RESP_FCTS_04]

Question 5: Incorrect

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

➡ ○ Backing up all log files and audit trails

○ Monitoring user access to compromised systems

● ~~Restoring damaged data from backup media~~

○ Purging transaction logs

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 as to the identity of the attacker or intruder. Users should not be granted access to compromised systems while evidence gathering is taking place. Damaged data should not be restored, and transaction logs should not be purged while evidence gathering is taking place.

References

TestOut PC Pro - 13.2 Incident Response
[e_response_pp6.exam.xml Q_RISK_RESP_FCTS_05]

Question 6: Correct

A security technician is conducting a forensic analysis.

Which of the following actions is MOST likely to destroy critical evidence?

○ Restricting physical access to the system

➡ ● Shutting down the system

○ Disconnecting the system from the network

Explanation

Shutting down or rebooting a compromised system will erase the memory contents. An attacker may load and run a memory-resident program and immediately erase it from the disk. Shutting down or rebooting the system will destroy all evidence of the malicious program.

References

TestOut PC Pro - 13.2 Incident Response
[e_response_pp6.exam.xml Q_RISK_RESP_FCTS_06]

▼ **Question 7:** Incorrect

You work for a company that offers their services through the internet. Therefore, it is critical that your website performs well. As a member of the IT technician staff, you receive a call from a fellow employee who informs you that customers are complaining that they can't access your website. After doing a little research, you have determined that you are a victim of a denial of service attack.

As a first responder, which of the following is the next BEST step to perform?

● ~~Eradicate the issue.~~

○ Investigate how the attack occurred.

○ Identify the issue further.

➡ ○ Contain the issue.

Explanation

You have already identified the issue, so the next step is to take actions to stop the attack and contain the damage. Although it is important 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 the attack is contained, the forensic team should be contacted to investigate, eradicate the issue, and perform other tasks to bring this incident to a close.

References

TestOut PC Pro - 13.2 Incident Response
[e_response_pp6.exam.xml Q_RISK_RESP_FCTS_07]