Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/18/2022 2:51:29 pm • Time spent: 03:10

Score: 80% Passing Score: 80%

Question 1: ✔ Correct

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.
- Connect to the access point and examine its logs for information.
- Run a packet sniffer to monitor traffic to and from the access point.
- See who is connected to the access point and attempt to find the attacker.

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 an attack involves a computer system attached to the network, the first step might be to disconnect the system 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, a forensic investigation can be performed on computer systems to gather evidence and identify the methods used in the attack.

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_contain_secp7.question.fex

Question 2: ✔ Correct

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

- Turn off the system.
- Stop all running processes.
- Remove the hard drive.
- Document what is on the screen.

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

12.1.2 Incident Response Process Facts

q_incident_resp_identify_01_secp7.question.fex

Question 3: ✔ Correct

When you conduct a forensic investigation, which of the following initial actions is appropriate for preserving evidence?

- Turn off the system.
- Document what is on the screen.
- Remove the hard drive.
- Stop all running processes.

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 is 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

12.1.2 Incident Response Process Facts

q_incident_resp_identify_02_secp7.question.fex

Question 4: ✔ Correct

What is the best definition of a security incident?

- ➡ (●) Violation of a security policy
- ( ) Criminal activity
- ( ) Compromise of the CIA
- ( ) Interruption of productivity

EXPLANATION

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

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

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_incident_01_secp7.question.fex

Question 5: ✔ Correct

What is the purpose of audit trails?

- ➡ To detect security-violating events.
- To correct system problems.
- To restore systems to normal operations.
- To prevent security breaches.

EXPLANATION

The purpose of audit trails is to detect security-violating events or actions.

Auditing itself is used to prevent security breaches, and audit trails are used for detective control. Neither auditing nor audit trails correct problems or restore systems to normal operations. That is done by the IT staff that inspects the contents of audit trails and creates a solution that is then implemented into the environment via the security policy.

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_incident_02_secp7.question.fex

Question 6: ✕ Incorrect

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

- Deploy new countermeasures.
- Update the security policy.
- ~~Restore and repair any damage.~~
- Back up all logs and audits regarding the incident.

EXPLANATION

The first step after an intrusion is to retain the documentation about the incident. Making backups of the logs and audits ensures that future investigations 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, repair damage, deploy new countermeasures, and then update the security.

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_log_01_secp7.question.fex

Question 7: ✔ Correct

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

- Restore damaged data from backup media.
- Back up all log files and audit trails.
- Purge transaction logs.
- Monitor 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 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. Along the same lines, damaged data should not be restored, nor transaction logs purged, while evidence-gathering is taking place.

REFERENCES

12.1.2 Incident Response Process Facts

q_incident_resp_log_02_secp7.question.fex

Question 8: ✔ Correct

As a security analyst, you suspect a threat actor used a certain tactic and technique to infiltrate your network. Which incident-response framework or approach would you utilize to see if other companies have had the same occurrence and what they did to remedy it?

- Communication plan with stakeholders
- Mitre Att@ck
- Cyber Kill Chain
- Diamond Model of Intrusion Analysis

EXPLANATION

You would use the Mitre Att@ck framework. This is a universally accessible, free database that contains techniques, tactics, and other operational information about malicious actors.

The Diamond Model of Intrusion Analysis defines adversary, victim, capabilities, and infrastructure. This model does not consider attacks other companies have experienced.

The Cyber Kill Chain exists to provide visibility to the hurdles of a malicious actor and make it easier to defend your assets.

Communicating with stakeholders would not produce solutions that other companies have created to fight the same threat.

REFERENCES

12.1.4 Incident Response Frameworks and Management Facts

q_incident_resp_fmwk_01_secp7.question.fex

Question 9: ✔ Correct

As a security analyst, you have discovered the victims of an malicious attack have several things in common. Which tools would you use to help you identify who might be behind the attacks and prevent potential future victims?

- [ ] Disaster recovery plan
- [x] Diamond Model of Intrusion Analysis
- [x] Mitre Att@cks
- [ ] Implement appropriate stakeholder management
- [ ] Cyber Kill Chain

EXPLANATION

You would choose the Diamond Model of Intrusion Analysis and use the Mitre Att@cks database to help you. For example, by identifying the types of victims and why they were attacked, the analyst/first responder can make an educated guess as to who is behind the attack and who are potential victims. This information can then be used to compare information in the Mitre Att@cks database. Since there are always unknowns, the database helps to fill in some of them.

Cyber Kill Chain provides visibility to the hurdles a malicious actor must overcome to carry out his or her attack. This makes the malicious actor's moves highly visible to a first responder or security analyst and is valuable in the defense of assets.

Disaster recovery plans do not include an analysis of threats and victims.

While stakeholder management is important, it won't assist you in analyzing future threats.

REFERENCES

12.1.4 Incident Response Frameworks and Management Facts

q_incident_resp_fmwk_02_secp7.question.fex

Question 10: ✕ Incorrect

You are in charge of making sure the IT systems of your company survive in case of any type of disaster in any of your locations. Your document should include organizational charts, phone lists, and order of restore. Each business unit should write their own policies and procedures with guidelines from corporate management. Which of the following documents should you create for this purpose?

- Communication plan
- Disaster recovery plan
- Business continuity plan
- ~~Incident-response team charter~~

EXPLANATION

You would make a business continuity plan. More detailed and longer than a disaster recover plan, a business continuity plan has procedures and policies for each business unit. The policies and procedures are written by each business unit with guidelines from corporate management. This document includes organizational charts, phone lists, order of restore, and vendor contact information.

A disaster recovery plan is similar and is used for documenting a plan for policies and procedures that are executed in the event of a disruption of business. However, this type of plan is much less involved than the business continuity plan.

A communication plan is written to effectively communicate important company information in the case of an emergency.

An incident-response team charter simply describes the creation and function of a specialized team trained to identify malicious actions against a network.

REFERENCES

12.1.4 Incident Response Frameworks and Management Facts

13.2.6 Business Continuity Planning Facts

q_incident_resp_plan_01_secp7.question.fex