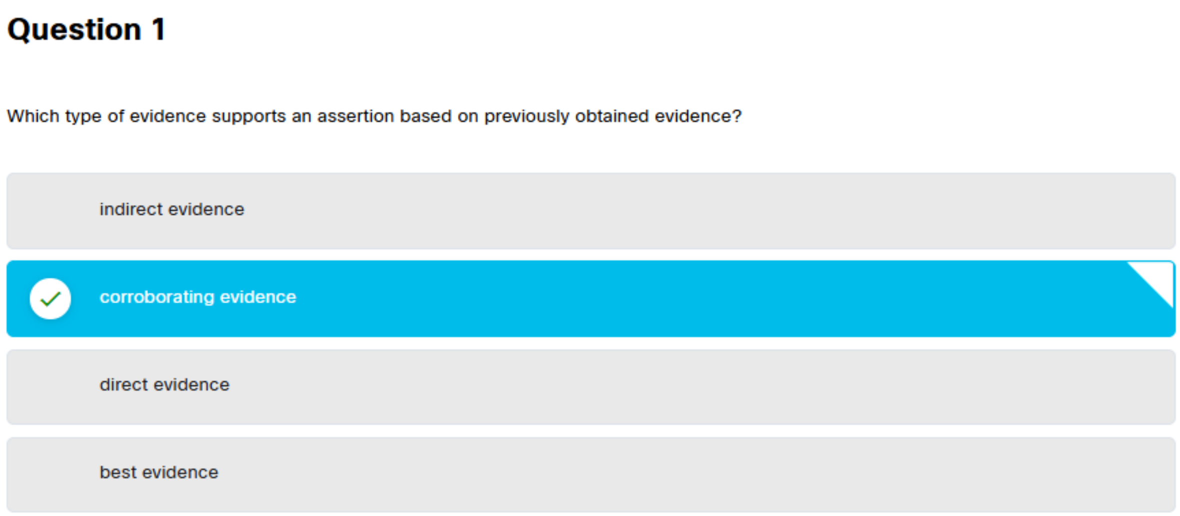
UJIAN TENGAH SEMESTER KEAMANAN SISTEM INFORMASI

Checkpoint Exam: Incident Response

Nama	: Anisatul Latifah
Nim	: 2141762008
Jurusan	: Teknologi Informasi
Prodi	: D-IV Sistem Informasi Bisnis

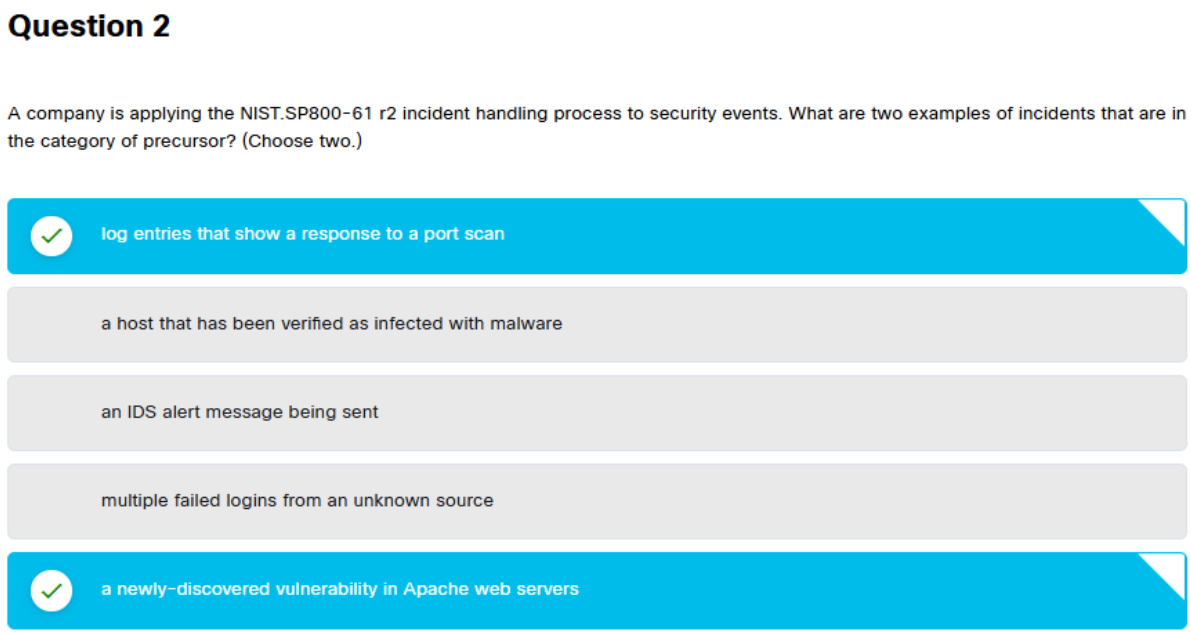
POLITEKNIK NEGERI MALANG



Question 1

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

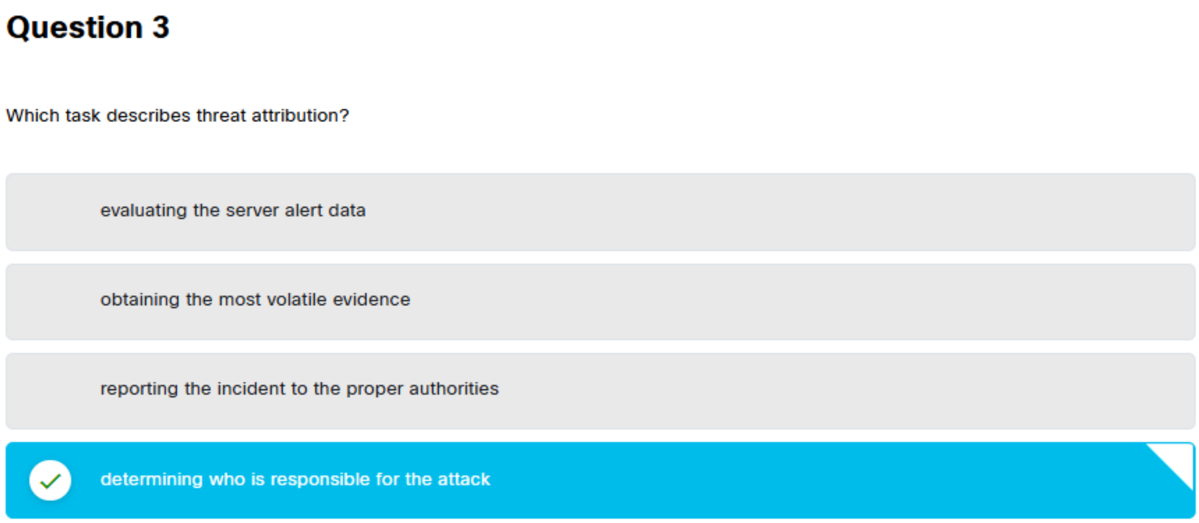
- indirect evidence
- ✓ corroborating evidence
- direct evidence
- best evidence



Question 2

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.)

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

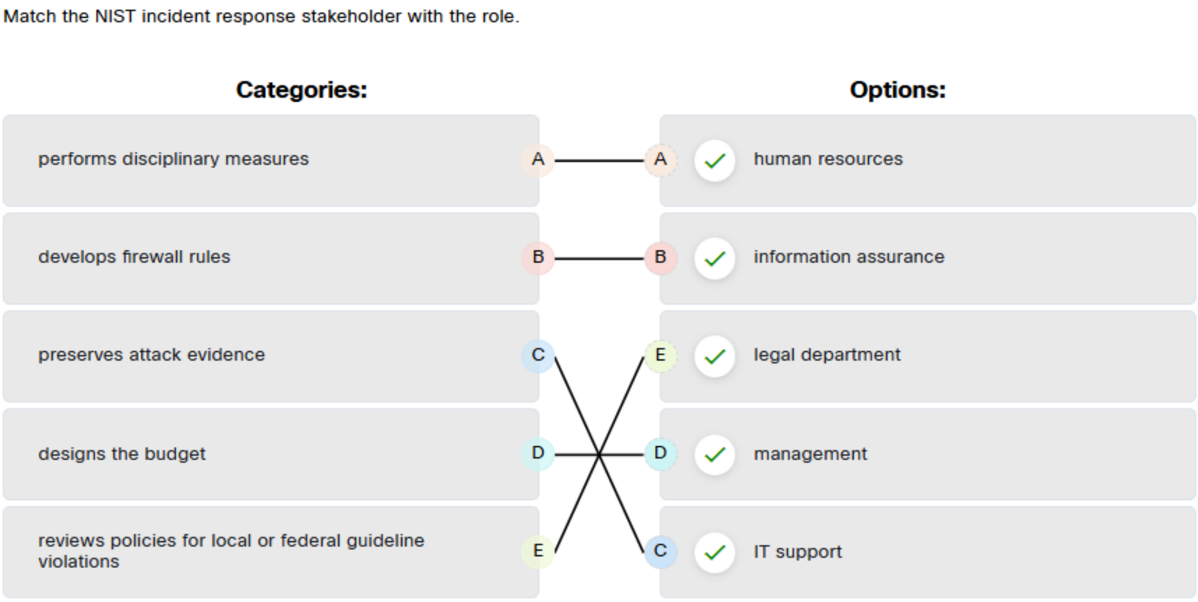


Question 3

Which task describes threat attribution?

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

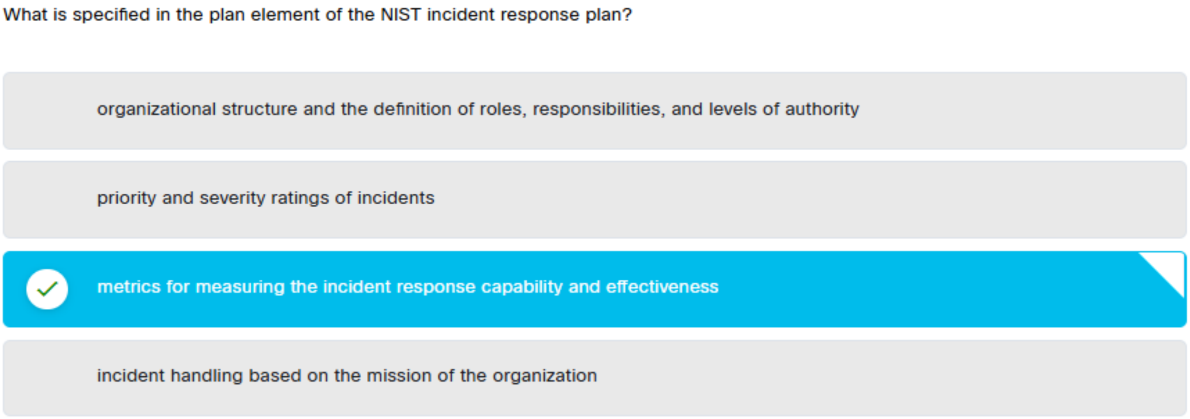
Question 4



Match the NIST incident response stakeholder with the role.

Categories:			Options:
performs disciplinary measures	A	A	✓ human resources
develops firewall rules	B	B	✓ information assurance
preserves attack evidence	C	E	✓ legal department
designs the budget	D	D	✓ management
reviews policies for local or federal guideline violations	E	C	✓ IT support

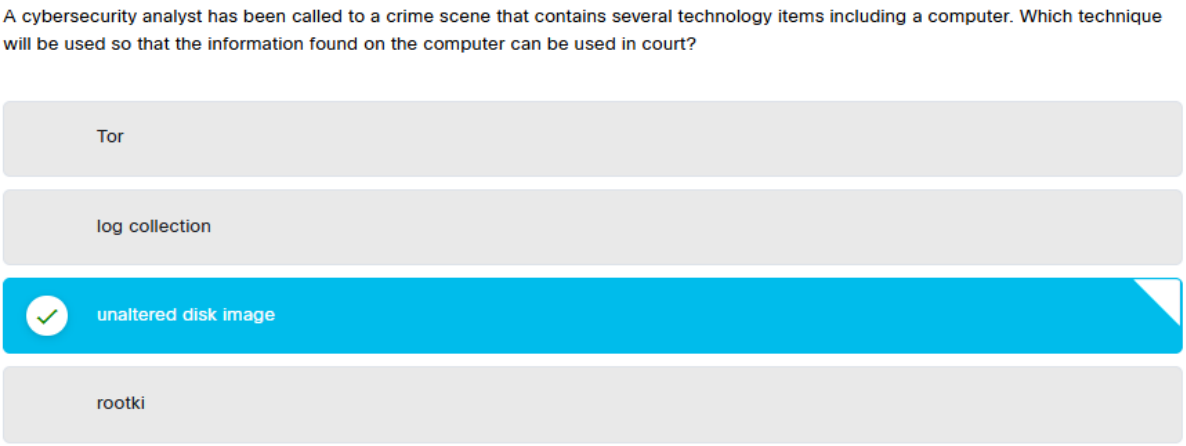
Question 5



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

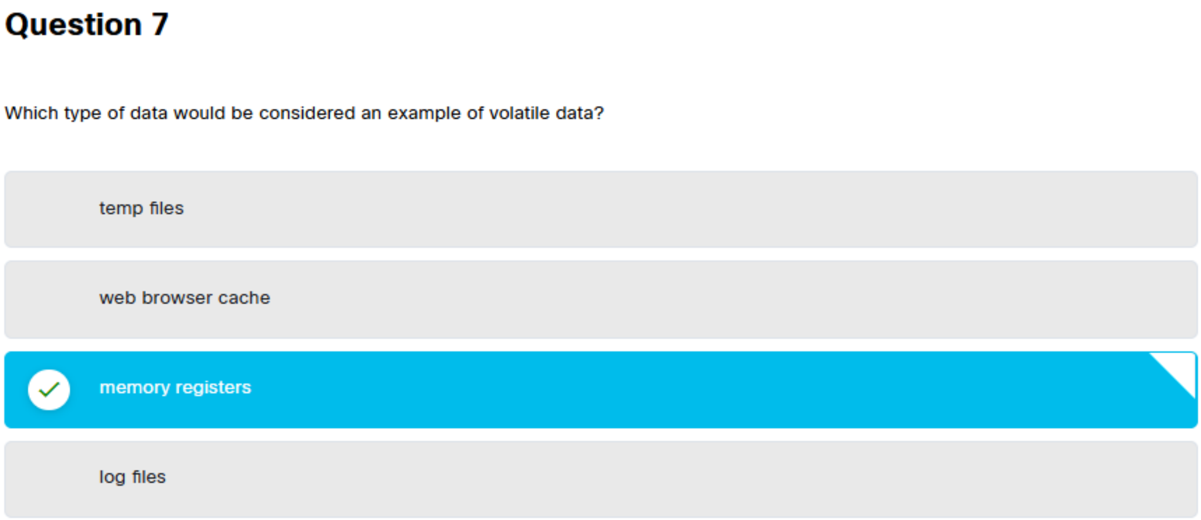
- organizational structure and the definition of roles, responsibilities, and levels of authority
- priority and severity ratings of incidents
- ✓ metrics for measuring the incident response capability and effectiveness
- incident handling based on the mission of the organization

Question 6



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?

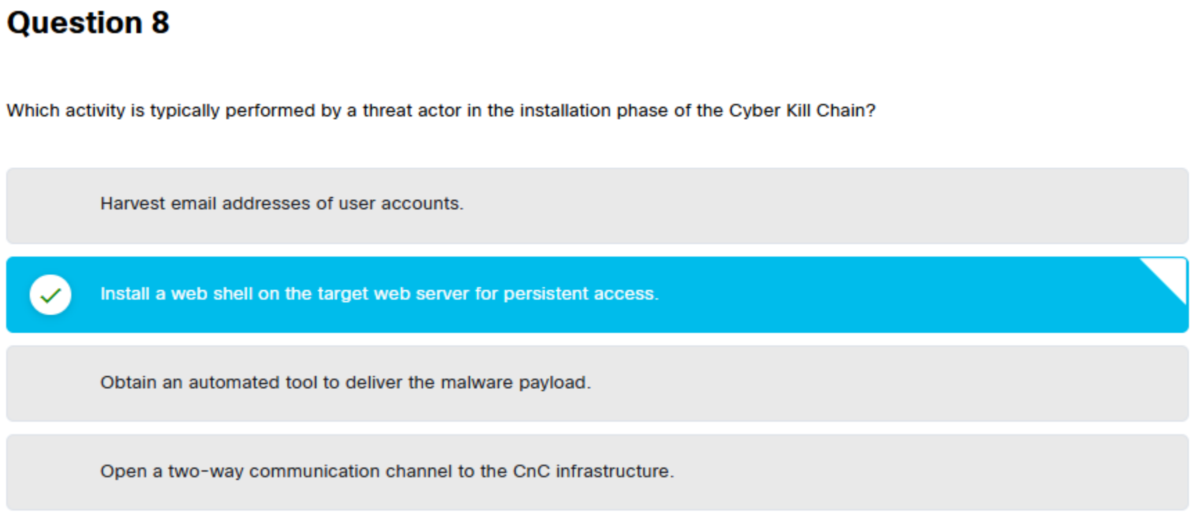
- Tor
- log collection
- ✓ unaltered disk image
- rootki



Question 7

Which type of data would be considered an example of volatile data?

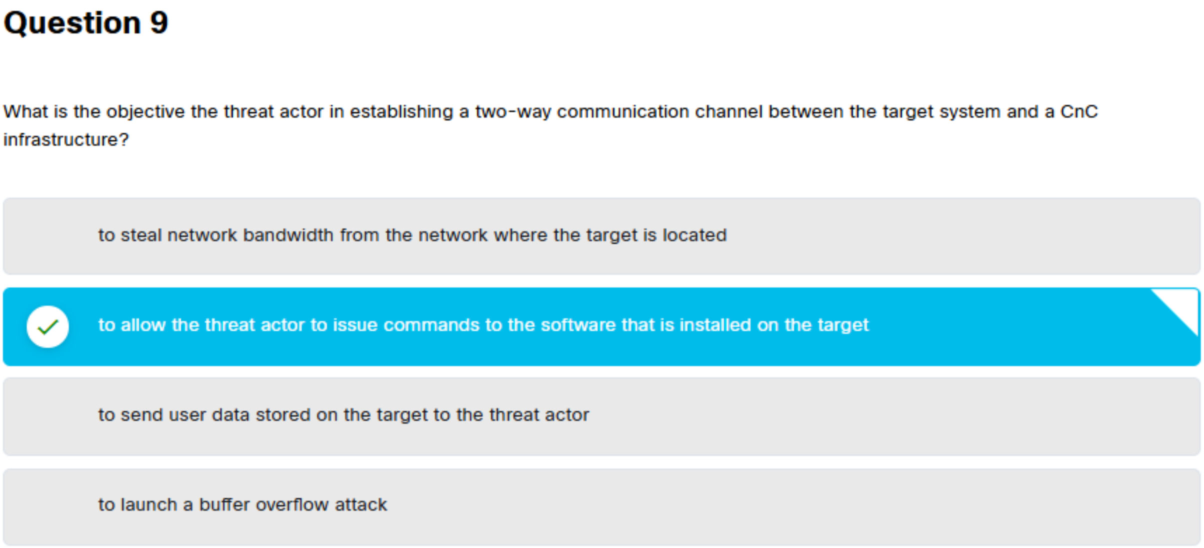
- temp files
- web browser cache
- ✓ memory registers
- log files



Question 8

Which activity is typically performed by a threat actor in the installation phase of the Cyber Kill Chain?

- Harvest email addresses of user accounts.
- ✓ Install a web shell on the target web server for persistent access.
- Obtain an automated tool to deliver the malware payload.
- Open a two-way communication channel to the CnC infrastructure.

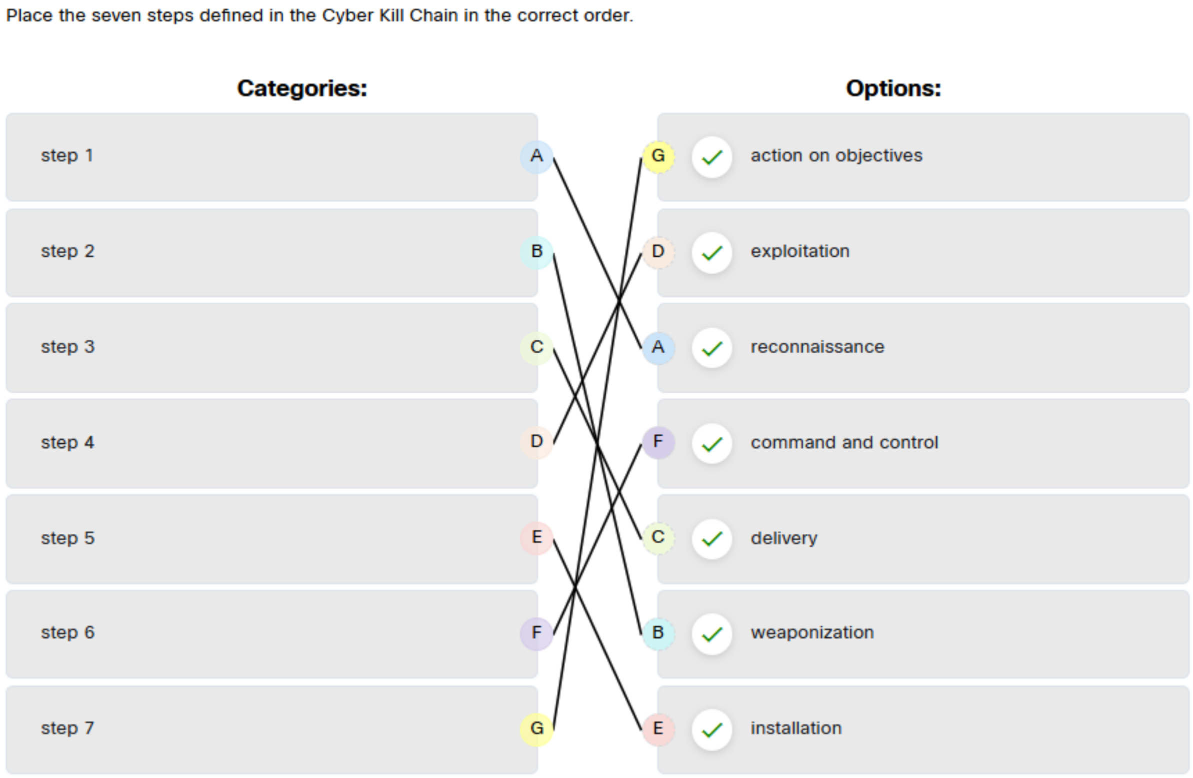


Question 9

What is the objective the threat actor in establishing a two-way communication channel between the target system and a CnC infrastructure?

- to steal network bandwidth from the network where the target is located
- ✓ to allow the threat actor to issue commands to the software that is installed on the target
- to send user data stored on the target to the threat actor
- to launch a buffer overflow attack

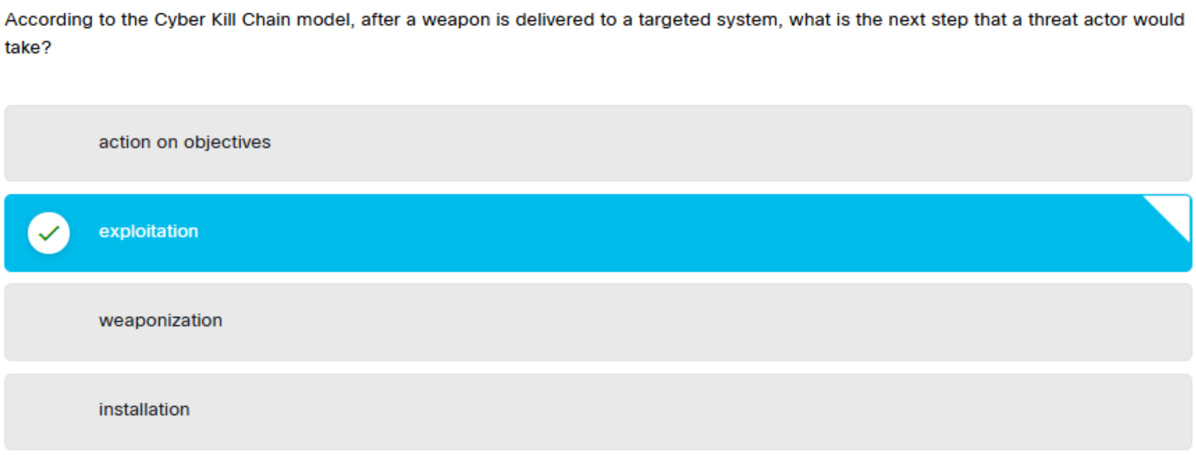
Question 10



Place the seven steps defined in the Cyber Kill Chain in the correct order.

Categories:			Options:
step 1	A	G	✓ action on objectives
step 2	B	D	✓ exploitation
step 3	C	A	✓ reconnaissance
step 4	D	F	✓ command and control
step 5	E	C	✓ delivery
step 6	F	B	✓ weaponization
step 7	G	E	✓ installation

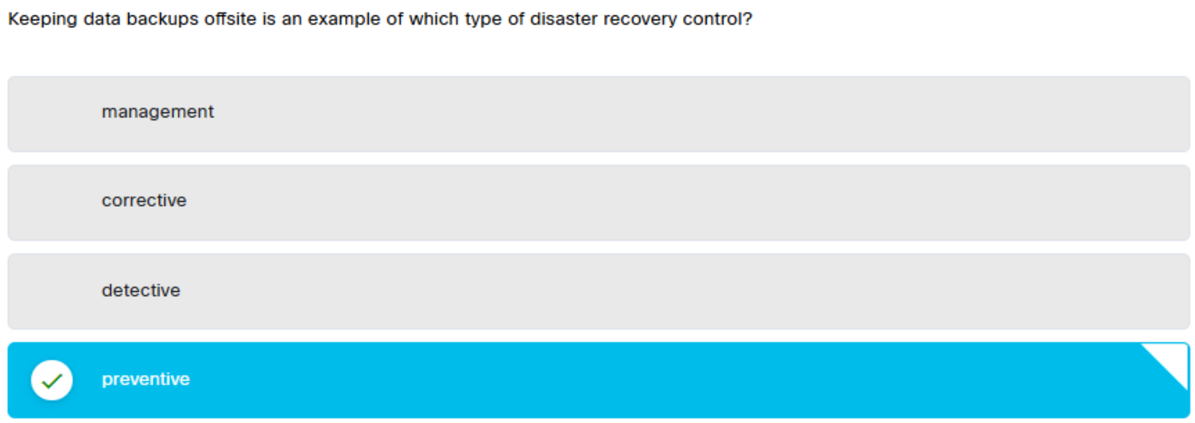
Question 11



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

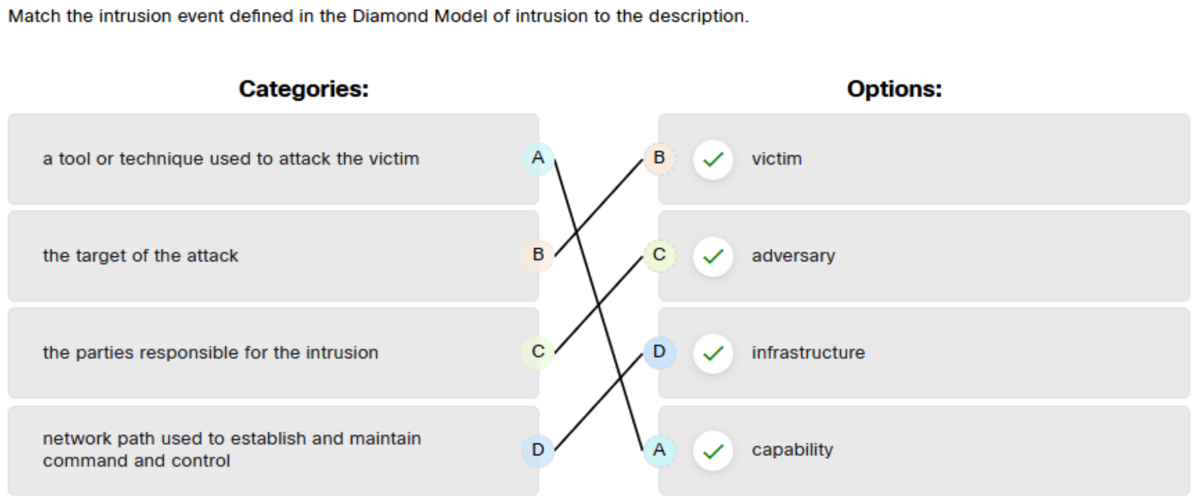
Question 12



Keeping data backups offsite is an example of which type of disaster recovery control?

- management
- corrective
- detective
- [✓ preventive]

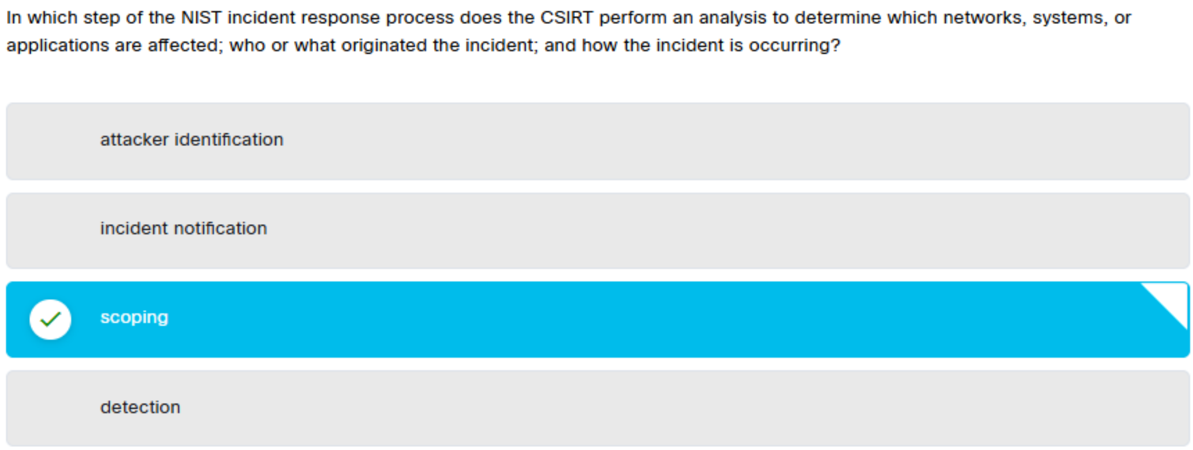
Question 13



Match the intrusion event defined in the Diamond Model of intrusion to the description.

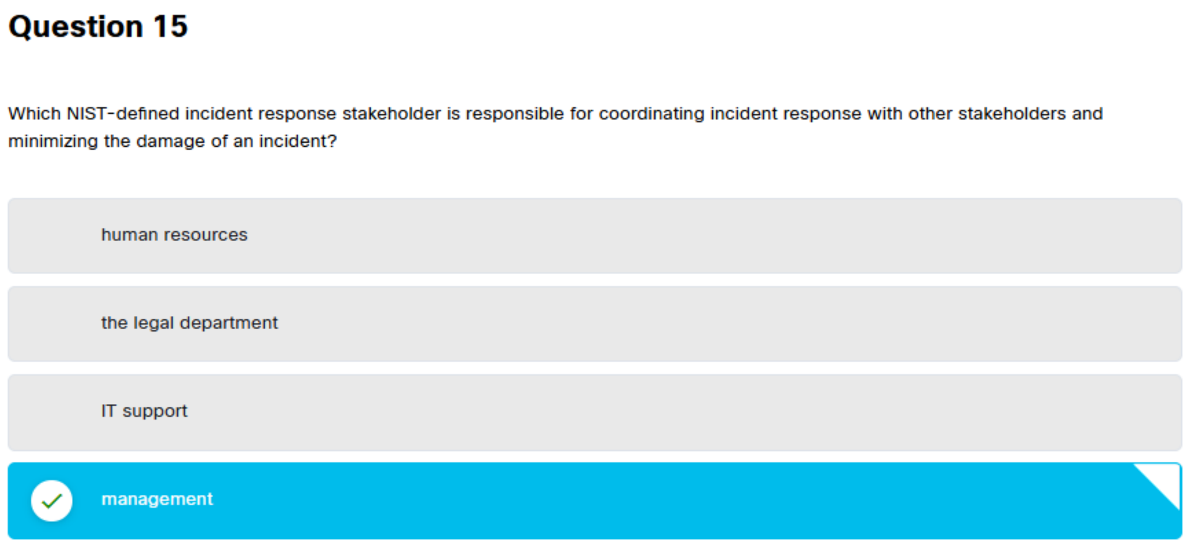
Categories:			Options:
a tool or technique used to attack the victim	A	B	✓ victim
the target of the attack	B	C	✓ adversary
the parties responsible for the intrusion	C	D	✓ infrastructure
network path used to establish and maintain command and control	D	A	✓ capability

Question 14



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?

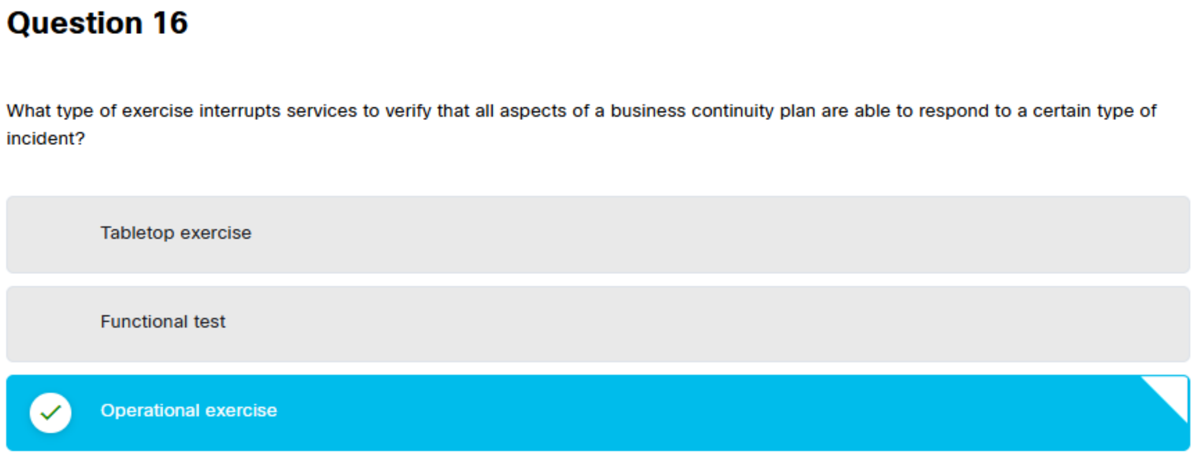
- attacker identification
- incident notification
- [✓ scoping]
- detection



Question 15

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

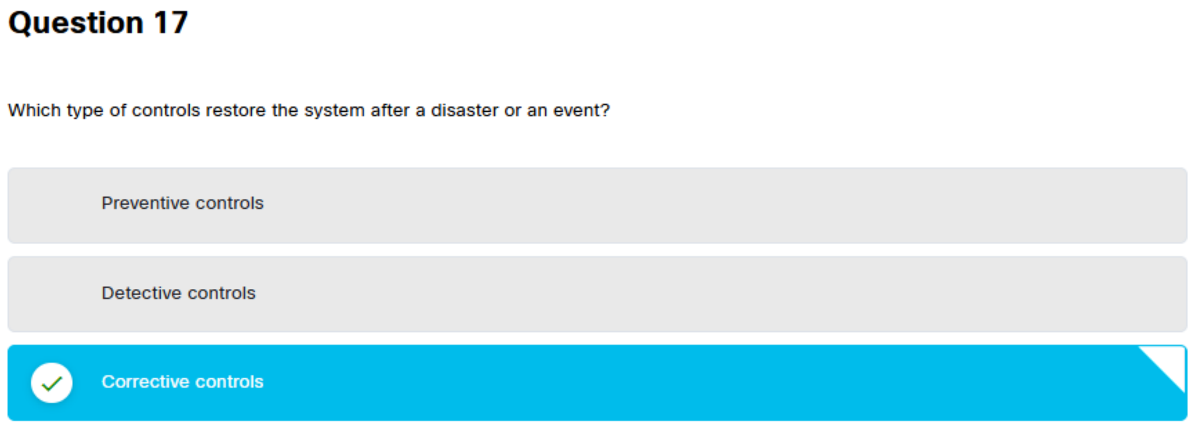
- human resources
- the legal department
- IT support
- ✓ management



Question 16

What type of exercise interrupts services to verify that all aspects of a business continuity plan are able to respond to a certain type of incident?

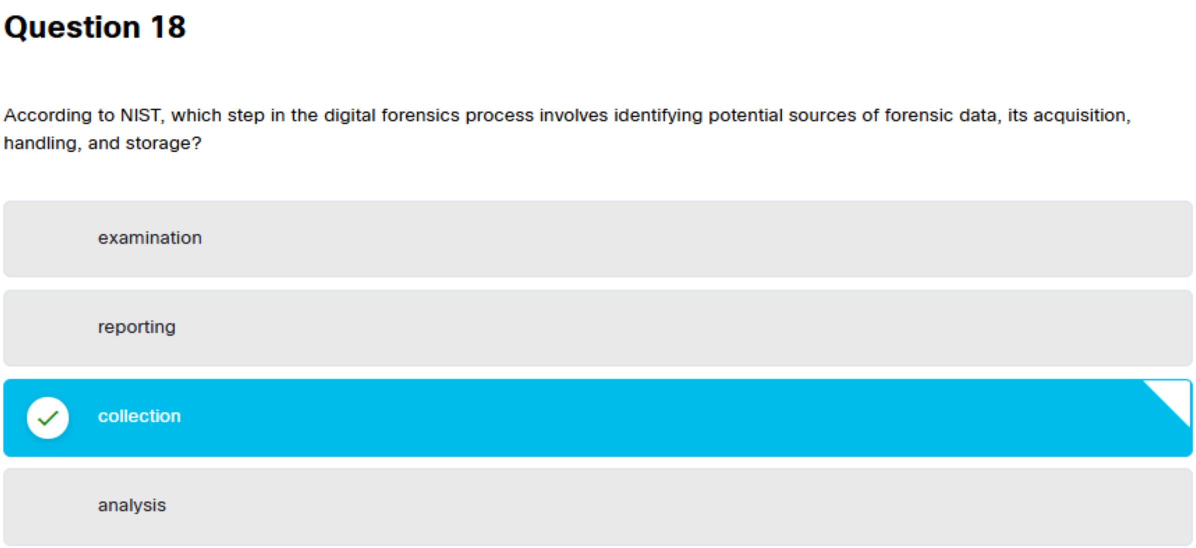
- Tabletop exercise
- Functional test
- ✓ Operational exercise



Question 17

Which type of controls restore the system after a disaster or an event?

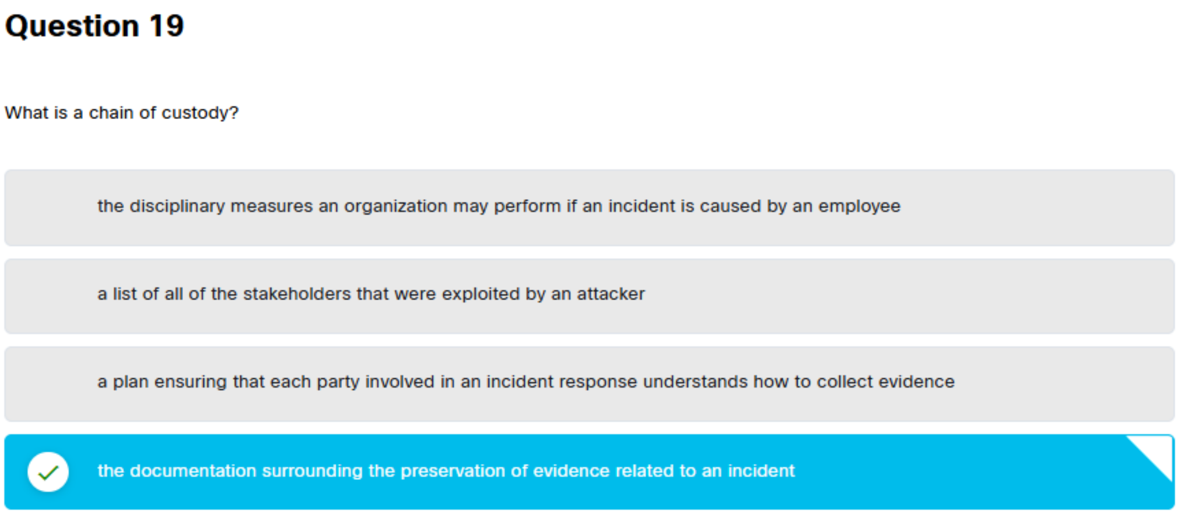
- Preventive controls
- Detective controls
- ✓ Corrective controls



Question 18

According to NIST, which step in the digital forensics process involves identifying potential sources of forensic data, its acquisition, handling, and storage?

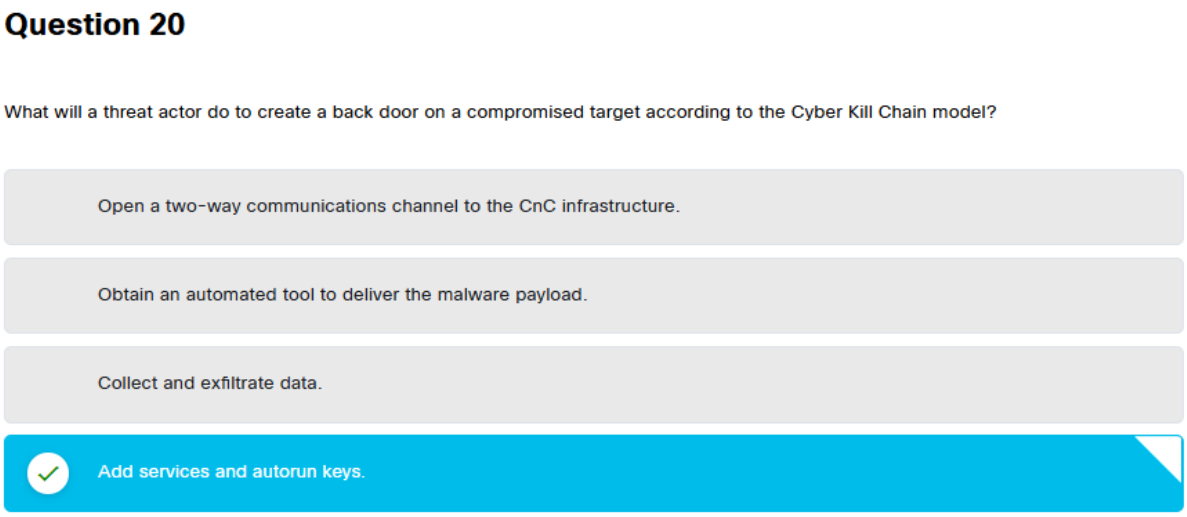
- examination
- reporting
- ✓ collection
- analysis



Question 19

What is a chain of custody?

- the disciplinary measures an organization may perform if an incident is caused by an employee
- a list of all of the stakeholders that were exploited by an attacker
- a plan ensuring that each party involved in an incident response understands how to collect evidence
- ✓ the documentation surrounding the preservation of evidence related to an incident

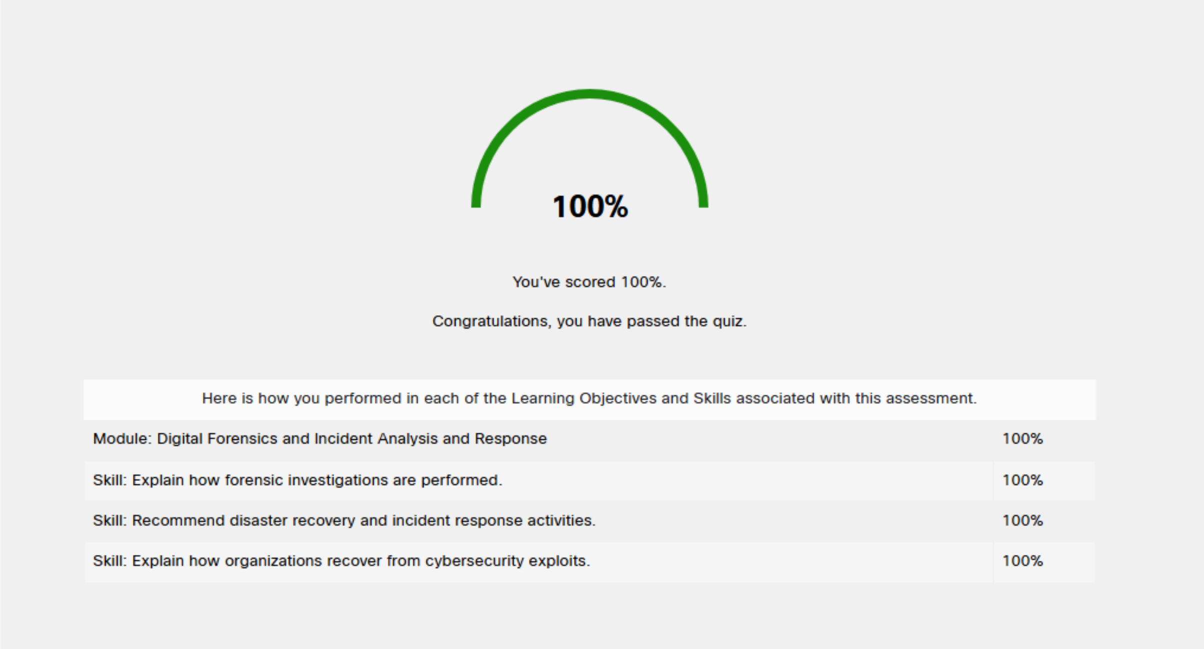


Question 20

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

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

Final Score :



100%

You've scored 100%.

Congratulations, you have passed the quiz.

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.	
Module: Digital Forensics and Incident Analysis and Response	100%
Skill: Explain how forensic investigations are performed.	100%
Skill: Recommend disaster recovery and incident response activities.	100%
Skill: Explain how organizations recover from cybersecurity exploits.	100%