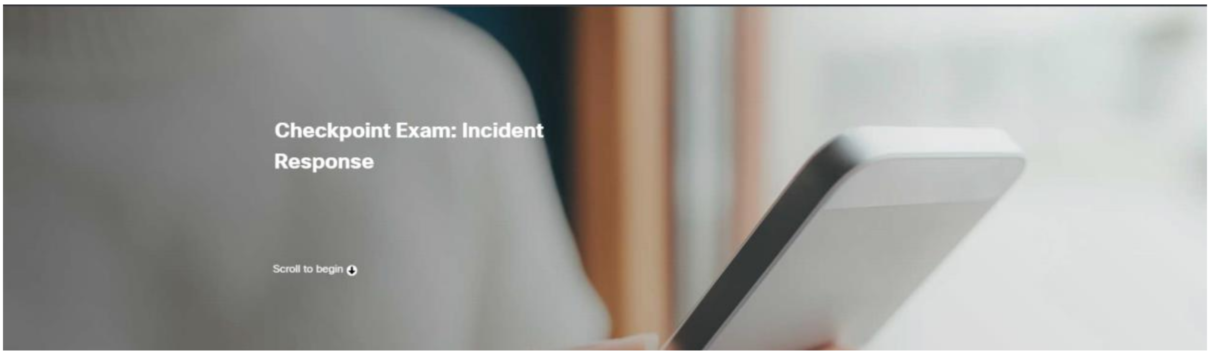
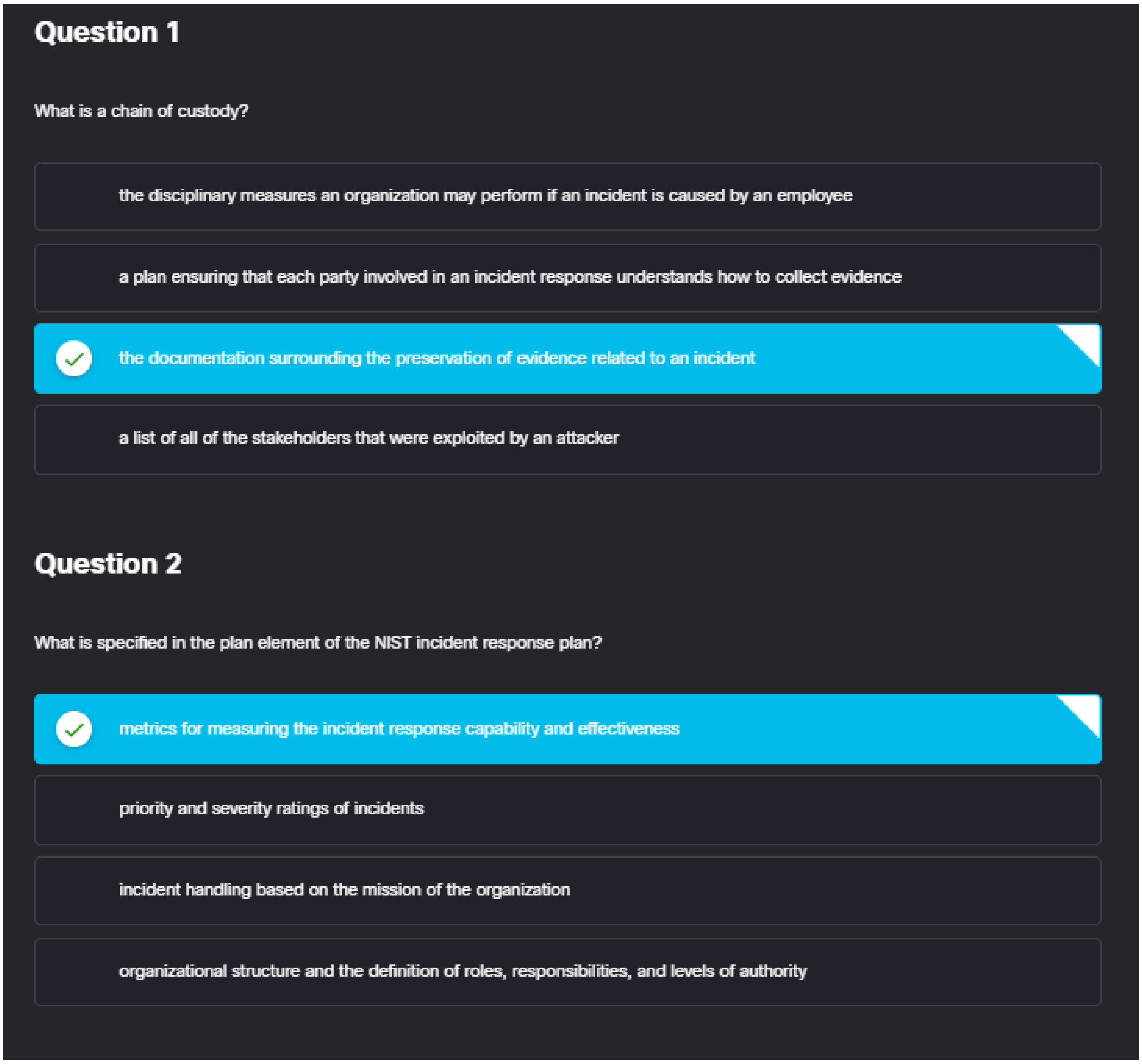
NAMA	: Sasmita Rachmawati
NIM	: 2141762141
Kelas	: SIB-4C
Matkul	: Keamanan Sistem Informasi



Checkpoint Exam: Incident Response



Question 1

What is a chain of custody?

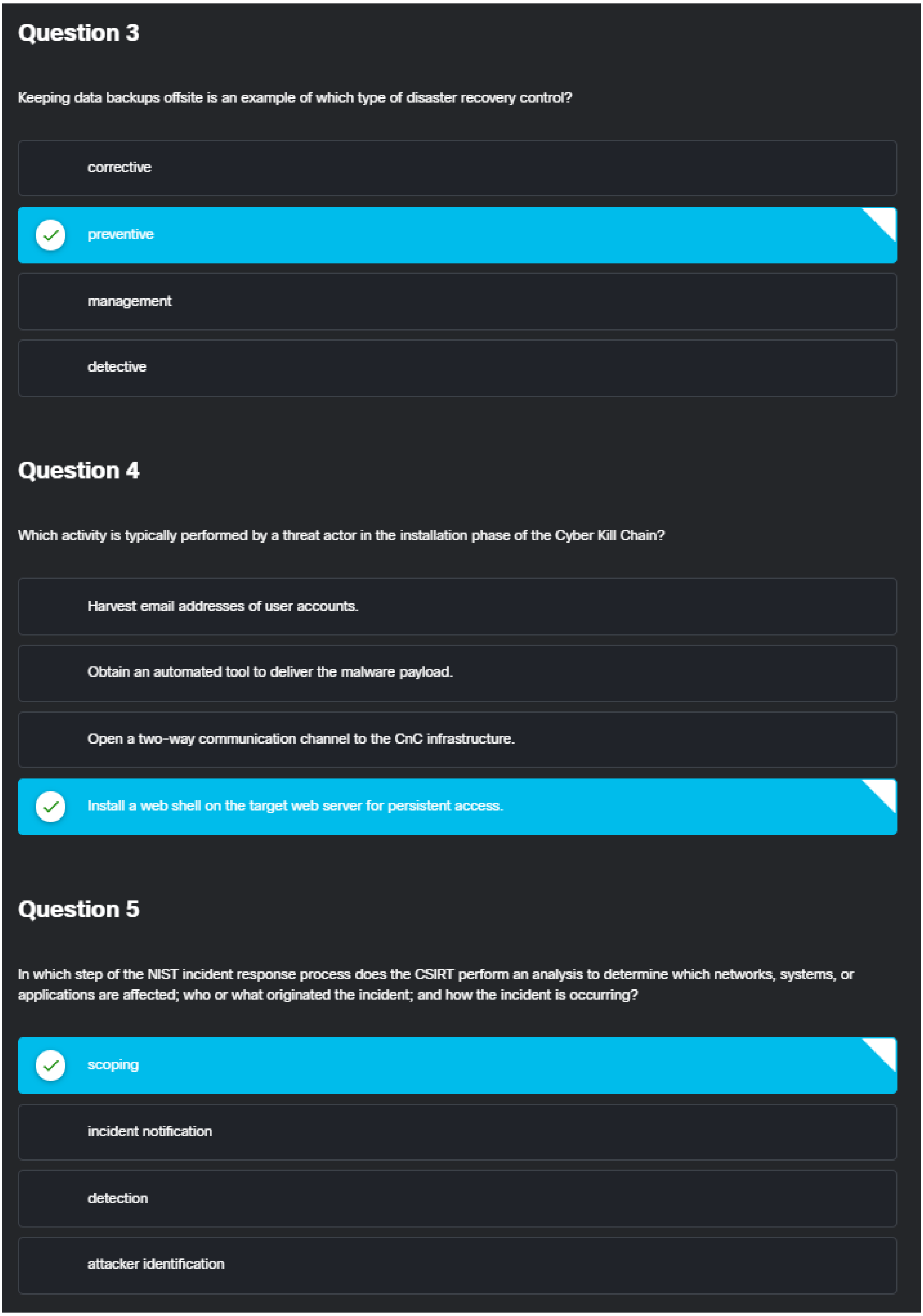
- the disciplinary measures an organization may perform if an incident is caused by an employee
- a plan ensuring that each party involved in an incident response understands how to collect evidence
- ✓ the documentation surrounding the preservation of evidence related to an incident
- a list of all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

Question 2

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

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

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 3

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

- corrective
- ✓ preventive
- management
- detective

Question 4

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

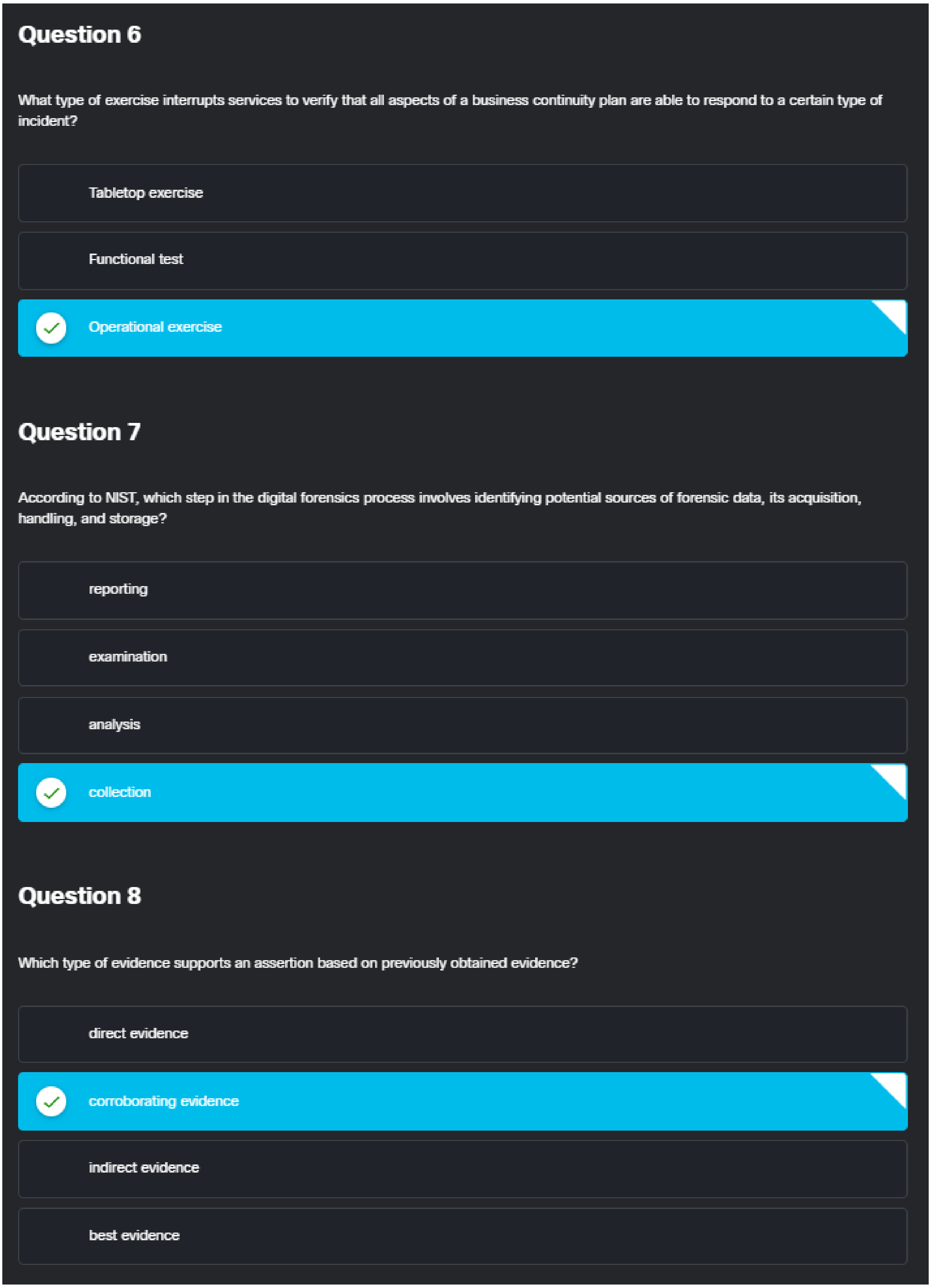
- Harvest email addresses of user accounts.
- Obtain an automated tool to deliver the malware payload.
- Open a two-way communication channel to the CnC infrastructure.
- ✓ Install a web shell on the target web server for persistent access.

Question 5

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?

- ✓ scoping
- incident notification
- detection
- attacker identification

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 6

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 7

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

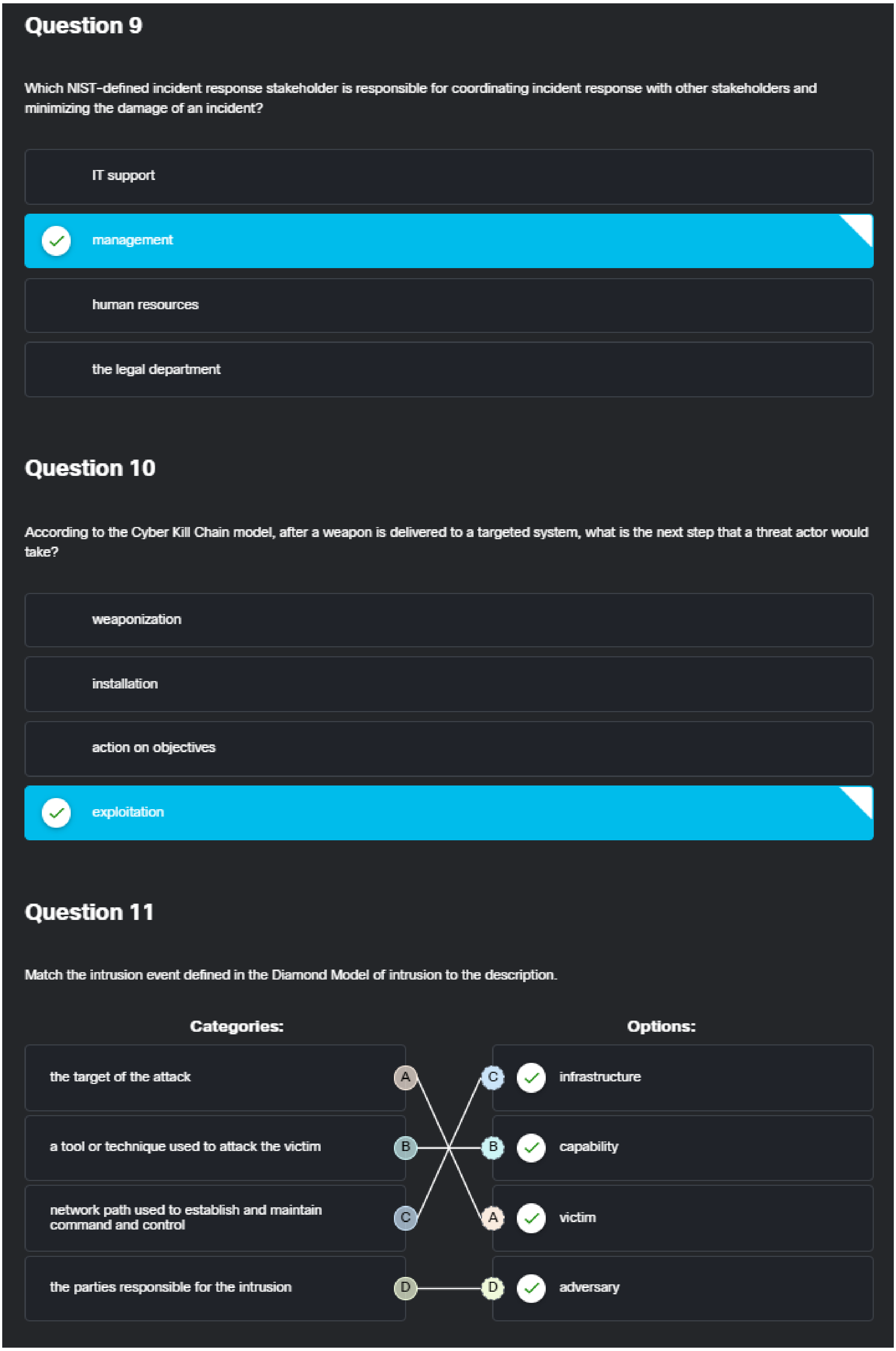
- reporting
- examination
- analysis
- ✓ collection

Question 8

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

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

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 9

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

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

Question 10

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?

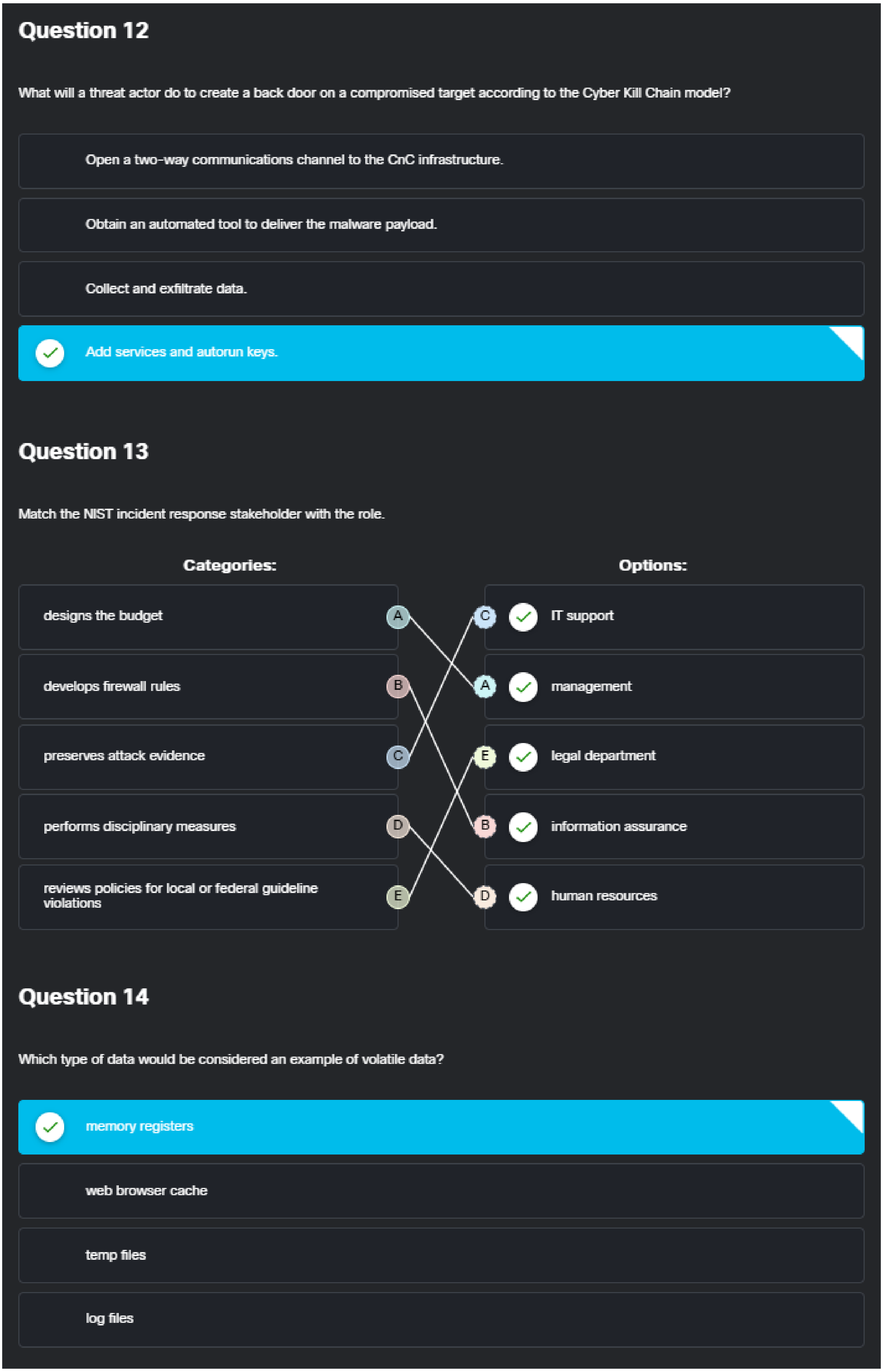
- weaponization
- installation
- action on objectives
- [✓ exploitation]

Question 11

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

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

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 12

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.

Question 13

Match the NIST incident response stakeholder with the role.

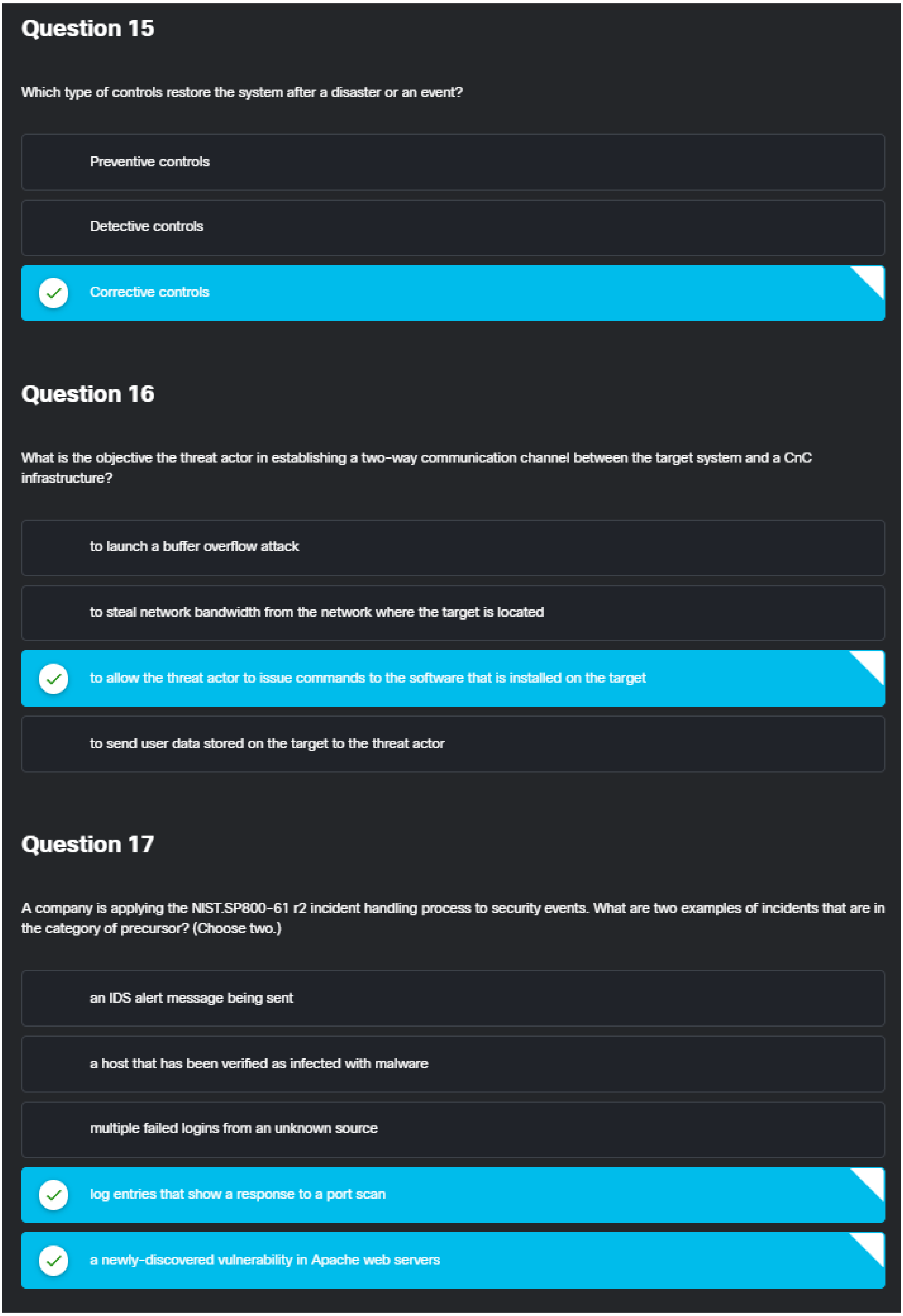
Categories:			Options:
designs the budget	A	C	✓ IT support
develops firewall rules	B	A	✓ management
preserves attack evidence	C	E	✓ legal department
performs disciplinary measures	D	B	✓ information assurance
reviews policies for local or federal guideline violations	E	D	✓ human resources

Question 14

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

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

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 15

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

- Preventive controls
- Detective controls
- ✓ Corrective controls

Question 16

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

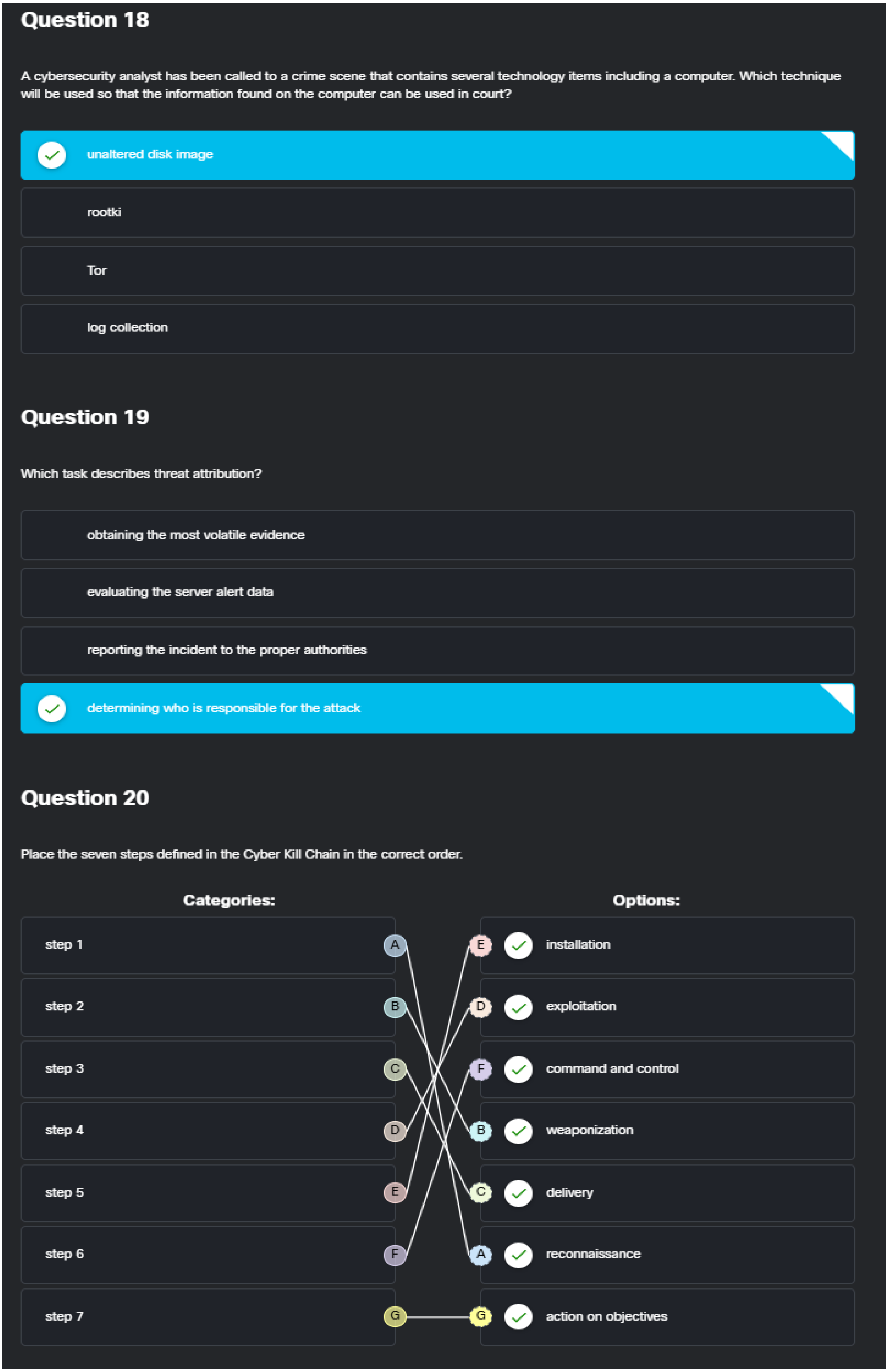
- to launch a buffer overflow attack
- to steal network bandwidth from the network where the target is located
- ✓ to allow the threat actor to issue commands to the software that is installed on the target
- to send user data stored on the target to the threat actor

Question 17

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.)

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

NAMA : Sasmita Rachmawati
NIM : 2141762141
Kelas : SIB-4C
Matkul : Keamanan Sistem Informasi



Question 18

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?

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

Question 19

Which task describes threat attribution?

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

Question 20

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

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