Checkpoint Exam : Incident Response

Nama : Mochammad Aldo Rizky

Kelas : SIB : 4C

Question 1

Which task describes threat attribution?

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

Question 2

Match the NIST incident response stakeholder with the role.

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

Question 3

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

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

Question 4

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

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

Question 5

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

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

Question 6

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

- Preventive controls
- Detective controls
- ✓ Corrective controls

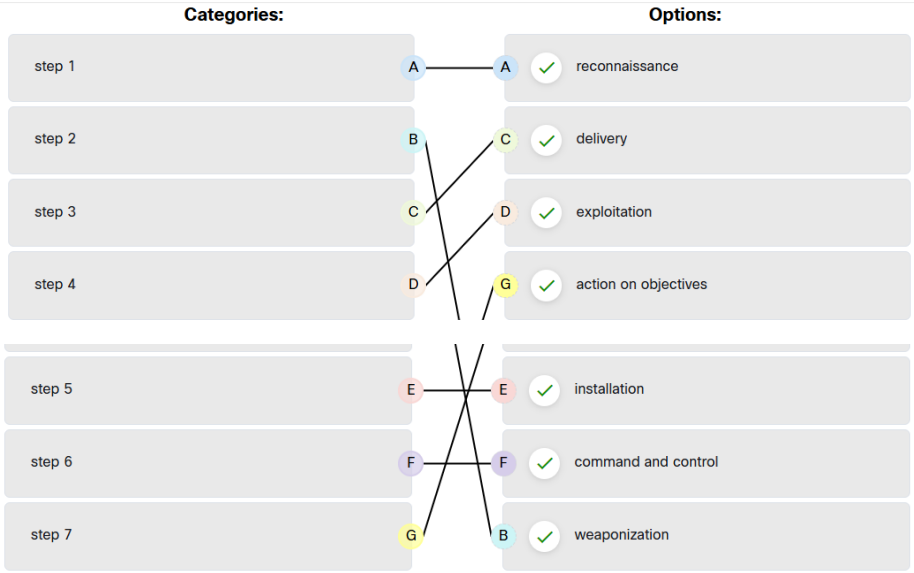
Question 7

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

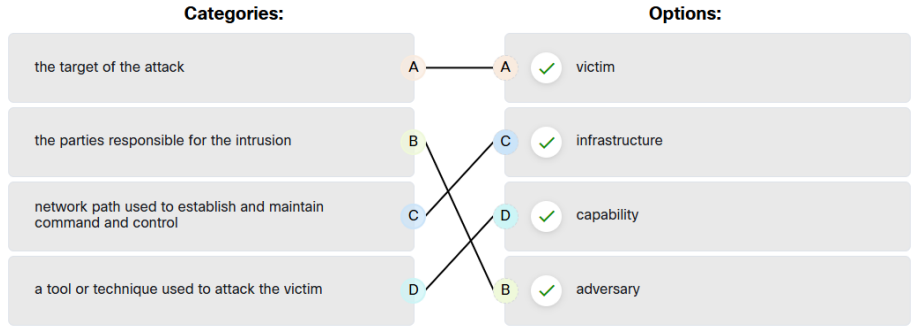
Question 8

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



Question 9

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



Question 10

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

- corrective
- management
- detective
- ✓ preventive

Question 11

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 12

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

- reporting
- ✓ collection
- examination
- analysis

Question 13

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 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?

- detection
- attacker identification
- ✓ scoping
- incident notification

Question 15

What is a chain of custody?

- a plan ensuring that each party involved in an incident response understands how to collect evidence
- the disciplinary measures an organization may perform if an incident is caused by an employee
- ✓ 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 16

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

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

Question 17

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?

- installation
- ✓ exploitation
- weaponization
- action on objectives

Question 18

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

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

Question 19

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.
- Collect and exfiltrate data.
- ✓ Add services and autorun keys.
- Obtain an automated tool to deliver the malware payload.

Question 20

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