KEAMANAN SISTEM INFORMASI

UTS - Incident Response Checkpoint Exam

Disusun untuk Memenuhi UTS Mata Kuliah Manajemen Jaringan Komputer

Oleh:

Wiraswanti Rismanda Putri
NIM: 2141762021

PROGRAM STUDI D-IV SISTEM INFORMASI BISNIS

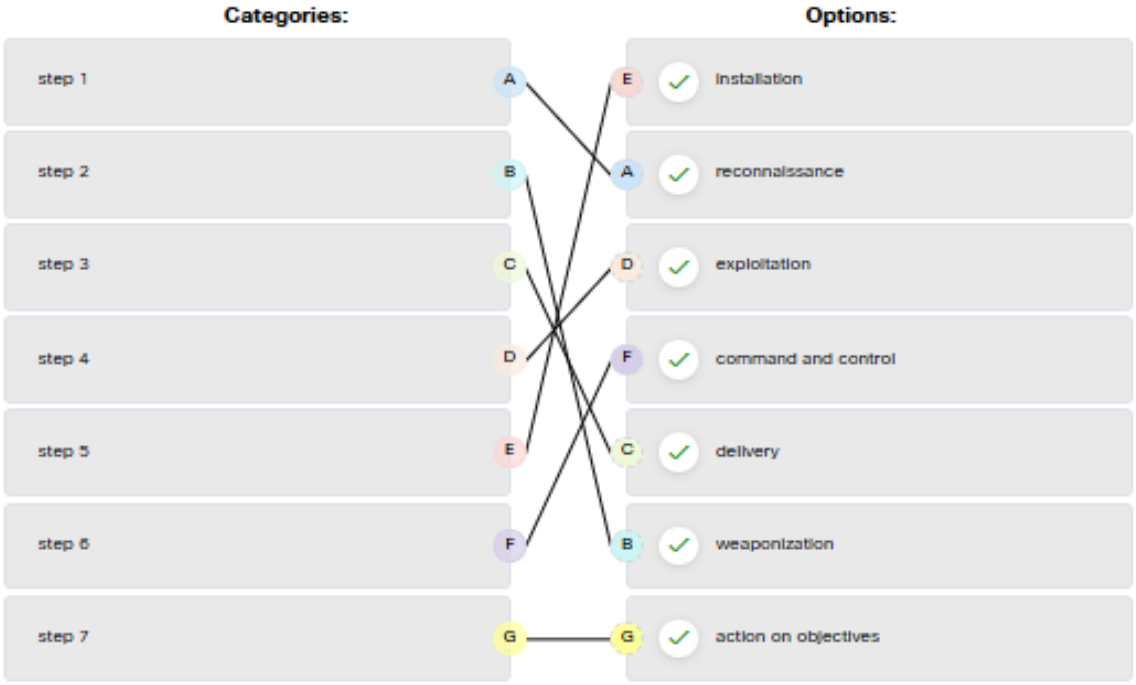
JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

2024

Question 1

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



Question 2

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

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

Question 3

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?

- incident notification
- attacker identification
- detection
- ✓ scoping

Question 4

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

- Preventive controls
- Detective controls
- ✓ Corrective controls

Question 5

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

- reporting
- analysis
- ✓ collection
- examination

Question 6

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

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

Question 7

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

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

Question 8

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

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

Question 9

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

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

Question 10

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

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

Question 11

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

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

Question 12

Which task describes threat attribution?

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

Question 13

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

- ✓ preventive
- corrective
- detective
- management

Question 14

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

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

Question 15

What is a chain of custody?

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

Question 16

Match the NIST incident response stakeholder with the role.

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

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
- ✓ 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
- ✓ a newly-discovered vulnerability in Apache web servers

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?

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

Question 19

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 20

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

Hasil Akhir