Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Checkpoint Exam: Incident Response

Question 1

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

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

Question 2

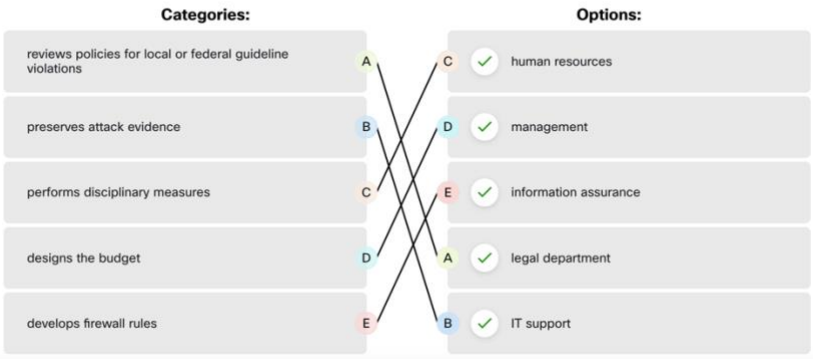
Which type of controls restore the system after a disaster or an event?

- Preventive controls
- Detective controls
- ✓ Corrective controls

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 3

Match the NIST incident response stakeholder with the role.



Question 4

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

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

Question 5

What is a chain of custody?

- 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
- the disciplinary measures an organization may perform if an incident is caused by an employee

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 6

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?

- ✓ exploitation
- weaponization
- installation
- action on objectives

Question 7

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 launch a buffer overflow attack
- to send user data stored on the target to the threat actor

Question 8

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

- ✓ preventive
- management
- corrective
- detective

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 9

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

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

Question 10

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
- detection
- ✓ scoping

Question 11

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

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 12

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

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

Question 13

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
- ✓ metrics for measuring the incident response capability and effectiveness
- incident handling based on the mission of the organization
- priority and severity ratings of incidents

Question 14

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

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 15

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

- analysis
- examination
- ✓ collection
- reporting

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

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?

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

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 18

Which task describes threat attribution?

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

Question 19

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

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

Question 20

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

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