LAPORAN UTS

KEAMANAN SISTEM INFORMASI CHECKPOINT EXAM

Oleh :

Rizqi Hendra Ardiansyah

2141762145

SIB-4C

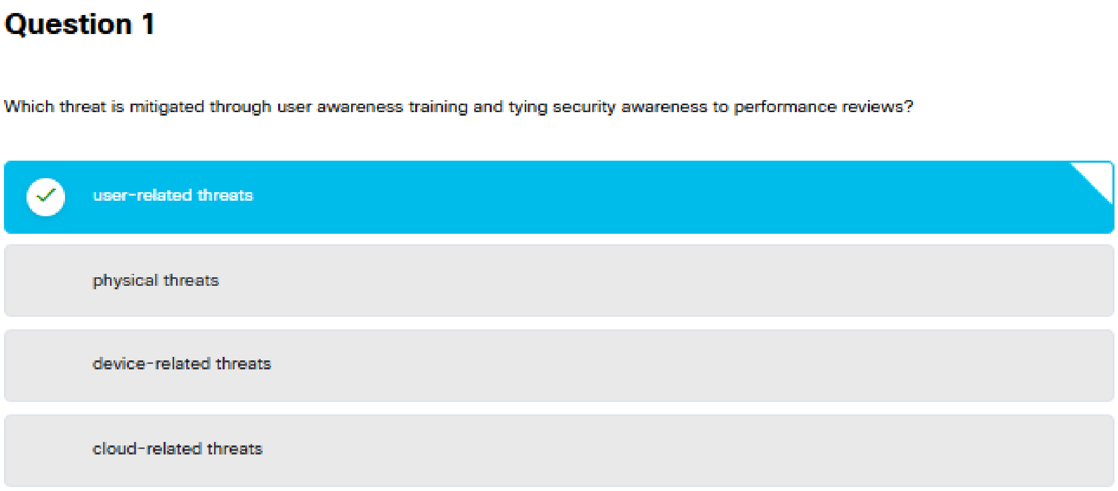
PROGAM STUDI D-IV SISTEM INFORMASI BISNIS

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

Jl. Soekarno Hatta No.9, Jatimulyo, Kec. Lowokwaru, Kota Malang,provinsi
Jawa Timur 65141

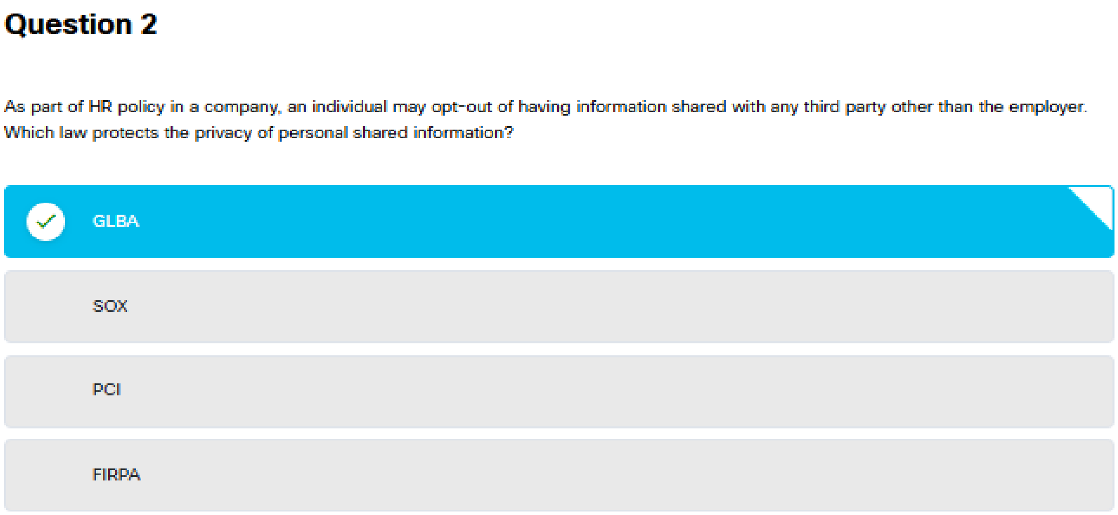
1. **Checkpoint Exam : Vulnerability Assessment and Risk Management**



Question 1

Which threat is mitigated through user awareness training and tying security awareness to performance reviews?

- ✓ user-related threats
- physical threats
- device-related threats
- cloud-related threats



Question 2

As part of HR policy in a company, an individual may opt-out of having information shared with any third party other than the employer. Which law protects the privacy of personal shared information?

- ✓ GLBA
- SOX
- PCI
- FIRPA

Question 3

A breach occurs in a company that processes credit card information. Which industry specific law governs credit card data protection?

- ✓ PCI DSS
- ECPA
- SOX
- GLBA

Question 4

A company has had several incidents involving users downloading unauthorized software, using unauthorized websites, and using personal USB devices. The CIO wants to put in place a scheme to manage the user threats. What three things might be put in place to manage the threats? (Choose three.)

- ✓ Disable CD and USB access.
- Change to thin clients.
- Implement disciplinary action.
- ✓ Use content filtering.
- Monitor all activity by the users.
- ✓ Provide security awareness training.

Question 5

What is the workforce framework category that includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence?

Securely Provision

Oversight and Development

[✓ Analyze]

Protect and Defend

Question 6

What type of network security test uses simulated attacks to determine the feasibility of an attack as well as the possible consequences if the attack occurs?

integrity checking

[✓ penetration testing]

network scanning

vulnerability scanning

Question 7

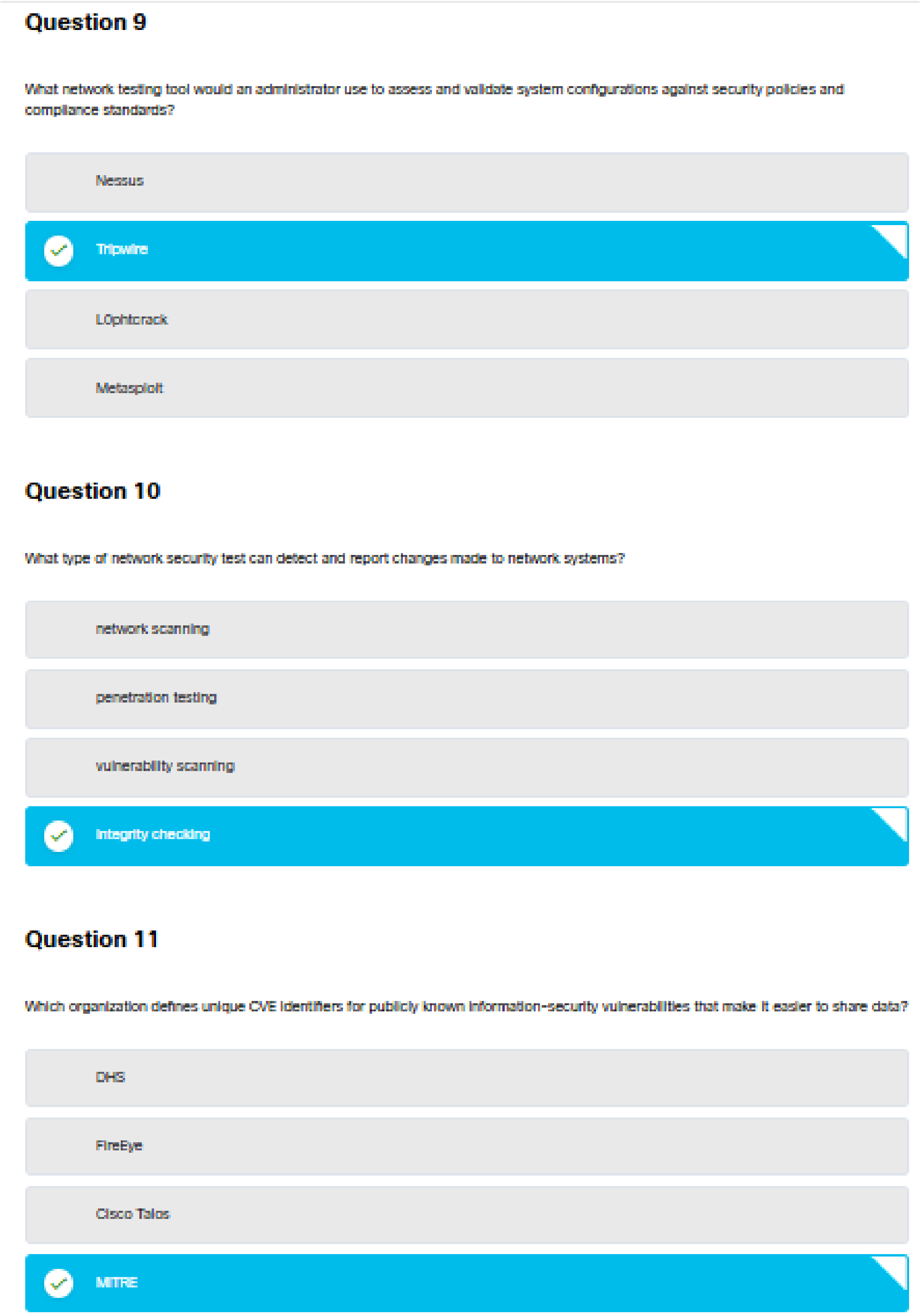
A security professional is asked to perform an analysis of the current state of a company network. What tool would the security professional use to scan the network only for security risks?

- pentest
- malware
- packet analyzer
- ✓ vulnerability scanner

Question 8

What information does the SIEM network security management tool provide to network administrators?

- a map of network systems and services
- ✓ real time reporting and analysis of security events
- assessment of system security configurations
- detection of open TCP and UDP ports



Question 9

What network testing tool would an administrator use to assess and validate system configurations against security policies and compliance standards?

- Nessus
- [✓ Tripwire]
- L0phtcrack
- Metasploit

Question 10

What type of network security test can detect and report changes made to network systems?

- network scanning
- penetration testing
- vulnerability scanning
- [✓ integrity checking]

Question 11

Which organization defines unique CVE Identifiers for publicly known information-security vulnerabilities that make it easier to share data?

- DHS
- FireEye
- Cisco Talos
- [✓ MITRE]

Question 12

Which statement describes Trusted Automated Exchange of Indicator Information (TAXII)?

- ✓ It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.
- It is a dynamic database of real-time vulnerabilities.
- It is a set of specifications for exchanging cyber threat information between organizations.
- It is a signature-less engine utilizing stateful attack analysis to detect zero-day threats.

Question 13

How does AIS address a newly discovered threat?

- ✓ by enabling real-time exchange of cyberthreat indicators with U.S. Federal Government and the private sector
- by advising the U.S. Federal Government to publish internal response strategies
- by mitigating the attack with active response defense mechanisms
- by creating response strategies against the new threat

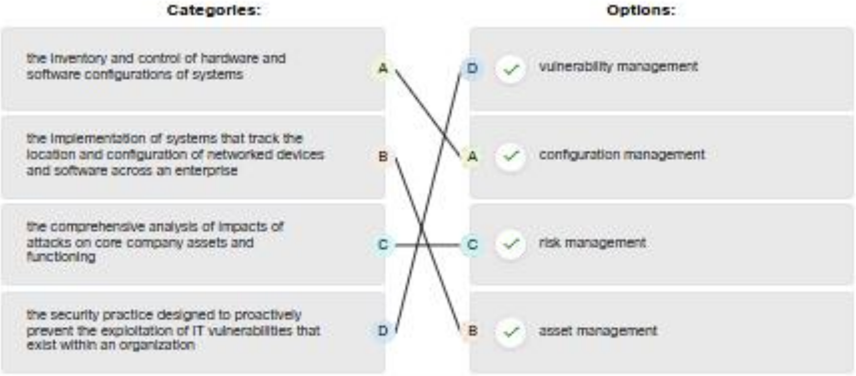
Question 14

What are the three impact metrics contained in the CVSS 3.0 Base Metric Group? (Choose three.)

- exploit
- ✓ confidentiality
- remediation level
- ✓ integrity
- ✓ availability
- attack vector

Question 15

Match the security management function with the description.



Categories:

- the inventory and control of hardware and software configurations of systems A
- the implementation of systems that track the location and configuration of networked devices and software across an enterprise B
- the comprehensive analysis of impacts of attacks on core company assets and functioning C
- the security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization D

Options:

- D ✓ vulnerability management
- A ✓ configuration management
- C ✓ risk management
- B ✓ asset management

Question 16

Which security management plan specifies a component that involves tracking the location and configuration of networked devices and software across an enterprise?

- ✓ asset management
- patch management
- risk management
- vulnerability management

Question 17

Which step in the Vulnerability Management Life Cycle determines a baseline risk profile to eliminate risks based on asset criticality, vulnerability threat, and asset classification?

- prioritize assets
- verify
- discover
- ✓ assess

Question 18

A security analyst is investigating a cyber attack that began by compromising one file system through a vulnerability in a custom software application. The attack now appears to be affecting additional file systems under the control of another security authority. Which CVSS v3.0 base exploitability metric score is increased by this attack characteristic?

- attack complexity
- privileges required
- ✓ scope
- user interaction

Question 19

What are the steps in the vulnerability management life cycle?

- identify, protect, detect, respond, recover
- plan, do, act, check
- ✓ discover, prioritize assets, assess, report, remediate, verify
- detect, analyze, recover, respond

Question 20

The team is in the process of performing a risk analysis on the database services. The information collected includes the initial value of these assets, the threats to the assets and the impact of the threats. What type of risk analysis is the team performing by calculating the annual loss expectancy?

- loss analysis
- protection analysis
- ✓ quantitative analysis
- qualitative analysis

Question 21

Which two values are required to calculate annual loss expectancy? (Choose two.)

- ✓ annual rate of occurrence
- quantitative loss value
- ✓ single loss expectancy
- asset value
- exposure factor
- frequency factor

Question 22

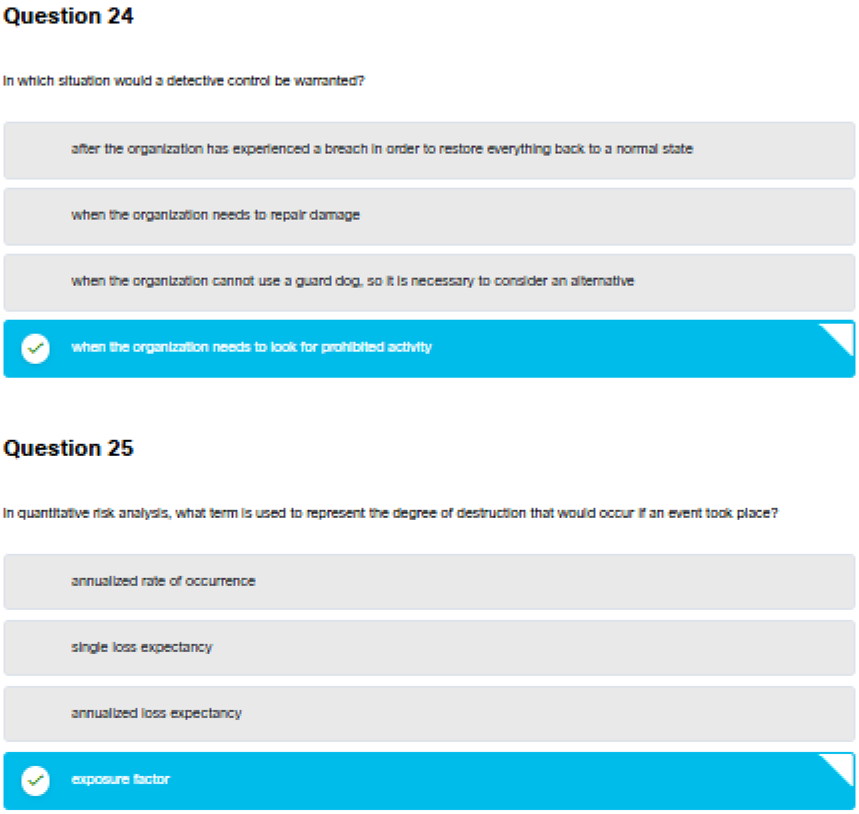
Which risk mitigation strategies include outsourcing services and purchasing insurance?

- reduction
- avoidance
- acceptance
- ✓ transfer

Question 23

Why would an organization perform a quantitative risk analysis for network security threats?

- so that the organization knows the top areas where network security holes exist
- so that management can determine the number of network devices needed to inspect, analyze, and protect the corporate resources
- so that management has documentation about the number of security attacks that have occurred within a particular time period
- ✓ so that the organization can focus resources where they are most needed



Question 24

In which situation would a detective control be warranted?

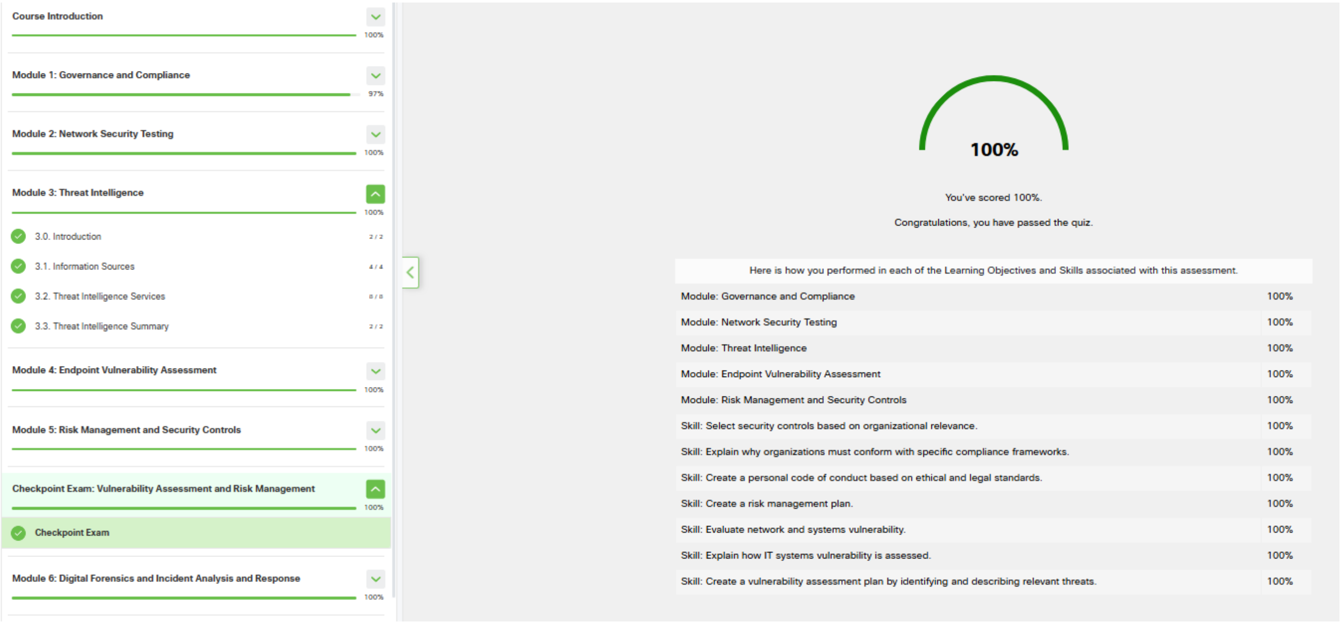
- after the organization has experienced a breach in order to restore everything back to a normal state
- when the organization needs to repair damage
- when the organization cannot use a guard dog, so it is necessary to consider an alternative
- ✓ when the organization needs to look for prohibited activity

Question 25

In quantitative risk analysis, what term is used to represent the degree of destruction that would occur if an event took place?

- annualized rate of occurrence
- single loss expectancy
- annualized loss expectancy
- ✓ exposure factor

Hasil CheckPoint Exam



Course Introduction 100%

Module 1: Governance and Compliance 97%

Module 2: Network Security Testing 100%

Module 3: Threat Intelligence 100%

- ✓ 3.0. Introduction 2 / 2
- ✓ 3.1. Information Sources 4 / 4
- ✓ 3.2. Threat Intelligence Services 8 / 8
- ✓ 3.3. Threat Intelligence Summary 2 / 2

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

- ✓ Checkpoint Exam

Module 6: Digital Forensics and Incident Analysis and Response 100%

100%

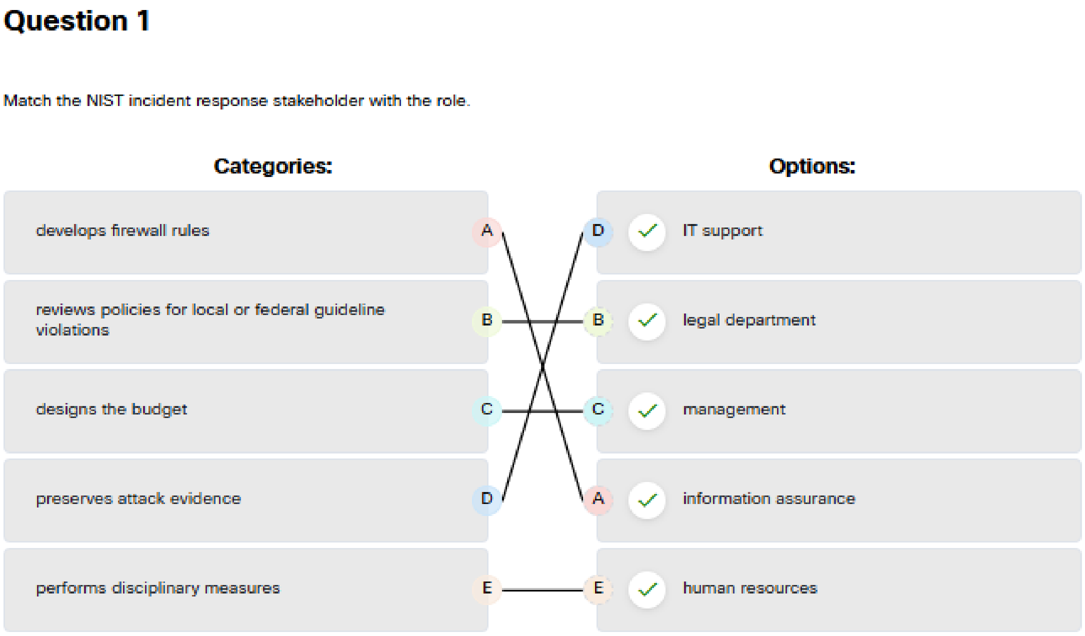
You've scored 100%.

Congratulations, you have passed the quiz.

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.

Module: Governance and Compliance	100%
Module: Network Security Testing	100%
Module: Threat Intelligence	100%
Module: Endpoint Vulnerability Assessment	100%
Module: Risk Management and Security Controls	100%
Skill: Select security controls based on organizational relevance.	100%
Skill: Explain why organizations must conform with specific compliance frameworks.	100%
Skill: Create a personal code of conduct based on ethical and legal standards.	100%
Skill: Create a risk management plan.	100%
Skill: Evaluate network and systems vulnerability.	100%
Skill: Explain how IT systems vulnerability is assessed.	100%
Skill: Create a vulnerability assessment plan by identifying and describing relevant threats.	100%

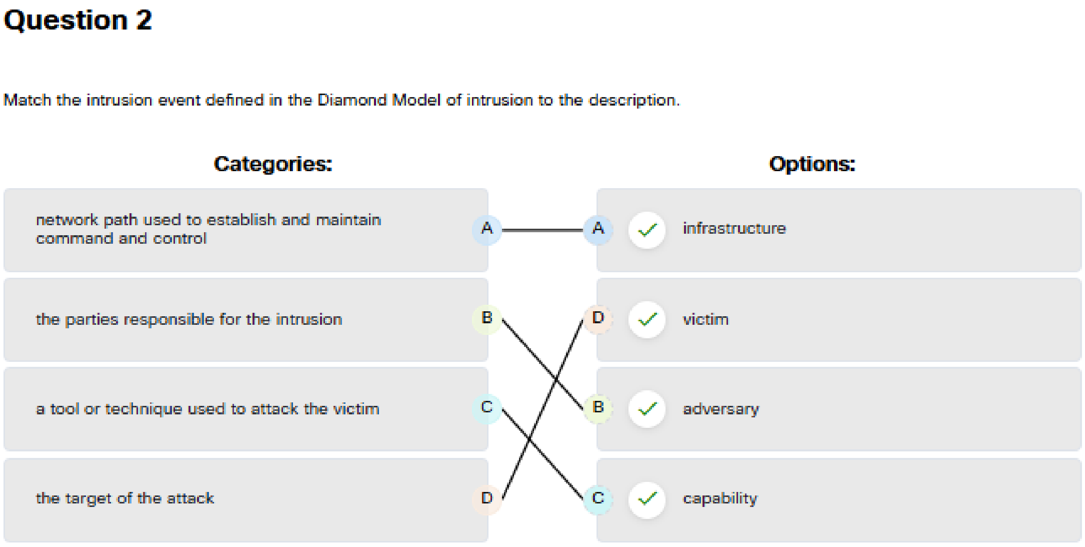
2. **Checkpoint Exam : Incident Response**



Question 1

Match the NIST incident response stakeholder with the role.

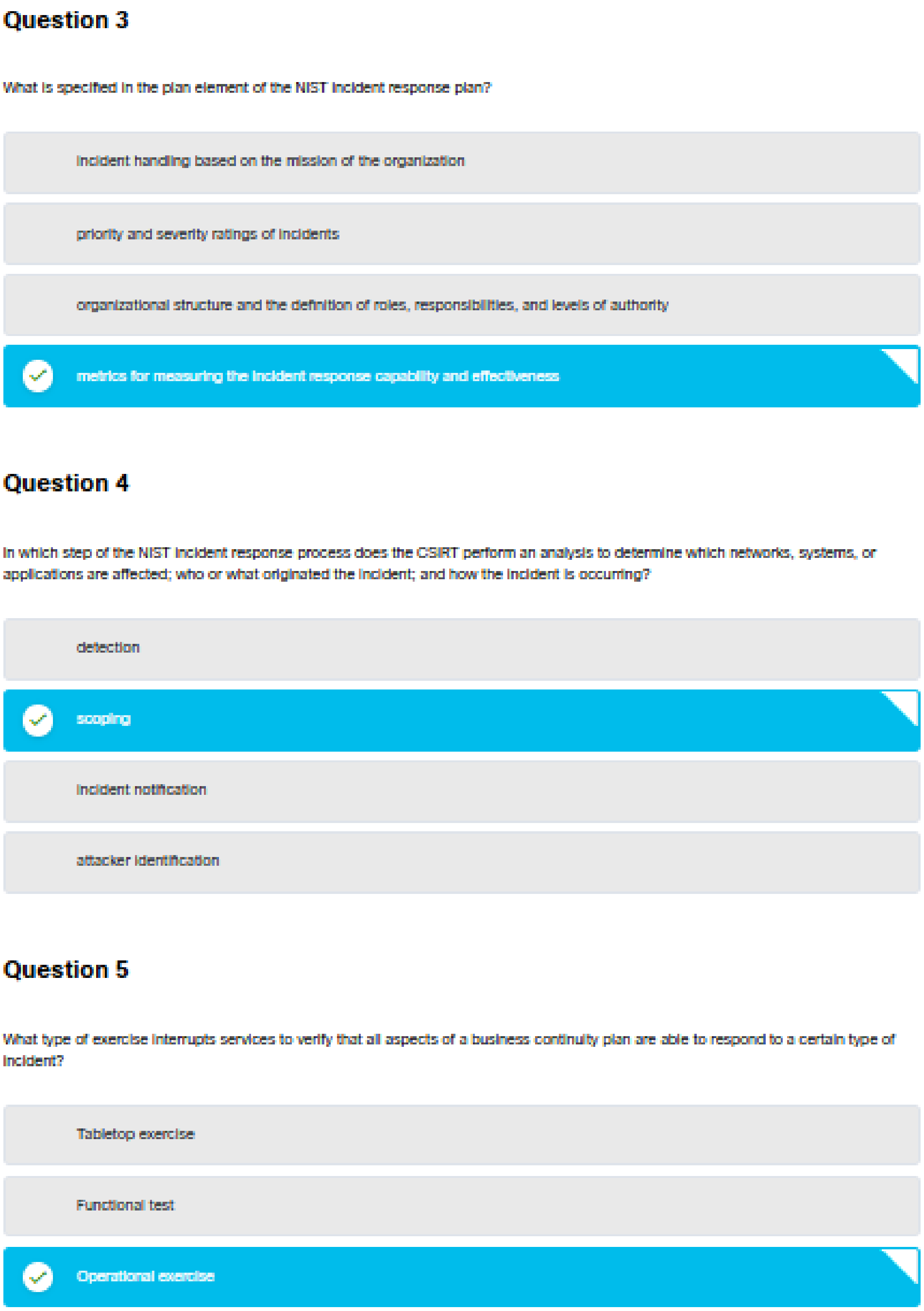
Categories:				Options:
develops firewall rules	A	D	✓	IT support
reviews policies for local or federal guideline violations	B	B	✓	legal department
designs the budget	C	C	✓	management
preserves attack evidence	D	A	✓	information assurance
performs disciplinary measures	E	E	✓	human resources



Question 2

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

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



Question 3

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

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

Question 4

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
- ✓ scoping
- incident notification
- attacker identification

Question 5

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 6

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

- ✓ collection
- reporting
- analysis
- examination

Question 7

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

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

Question 8

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
- action on objectives
- ✓ exploitation
- installation

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 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 steal network bandwidth from the network where the target is located
- to launch a buffer overflow attack

Question 10

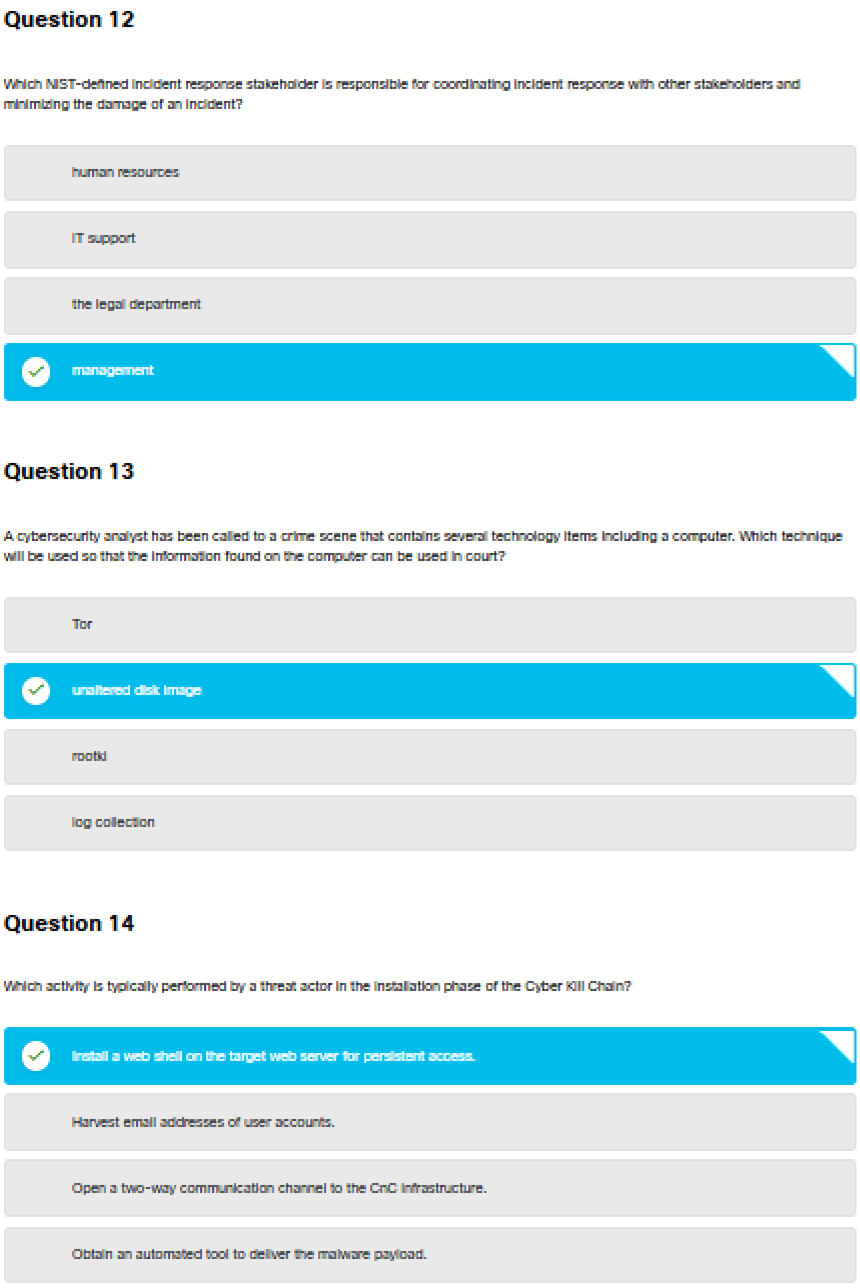
Which task describes threat attribution?

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

Question 11

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

- management
- ✓ preventive
- corrective
- detective



Question 12

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

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

Question 13

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
- ✓ unaltered disk image
- rootki
- log collection

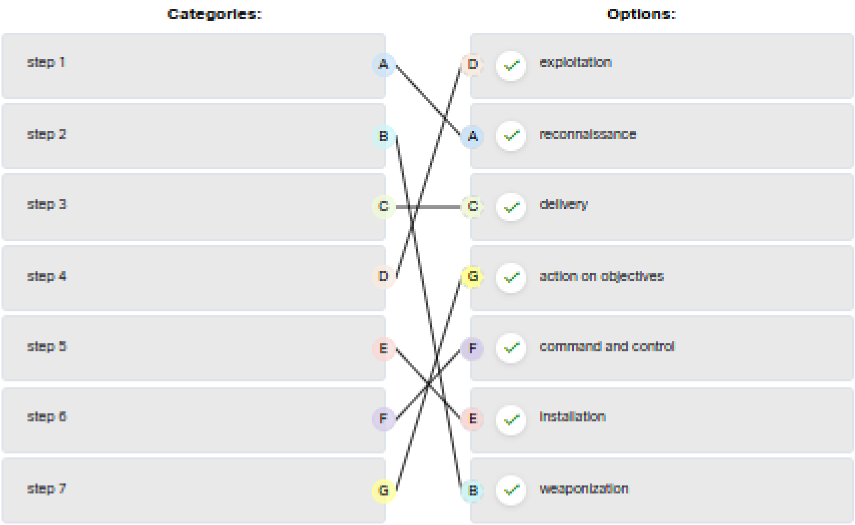
Question 14

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.
- Harvest email addresses of user accounts.
- Open a two-way communication channel to the CnC infrastructure.
- Obtain an automated tool to deliver the malware payload.

Question 15

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



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

Question 16

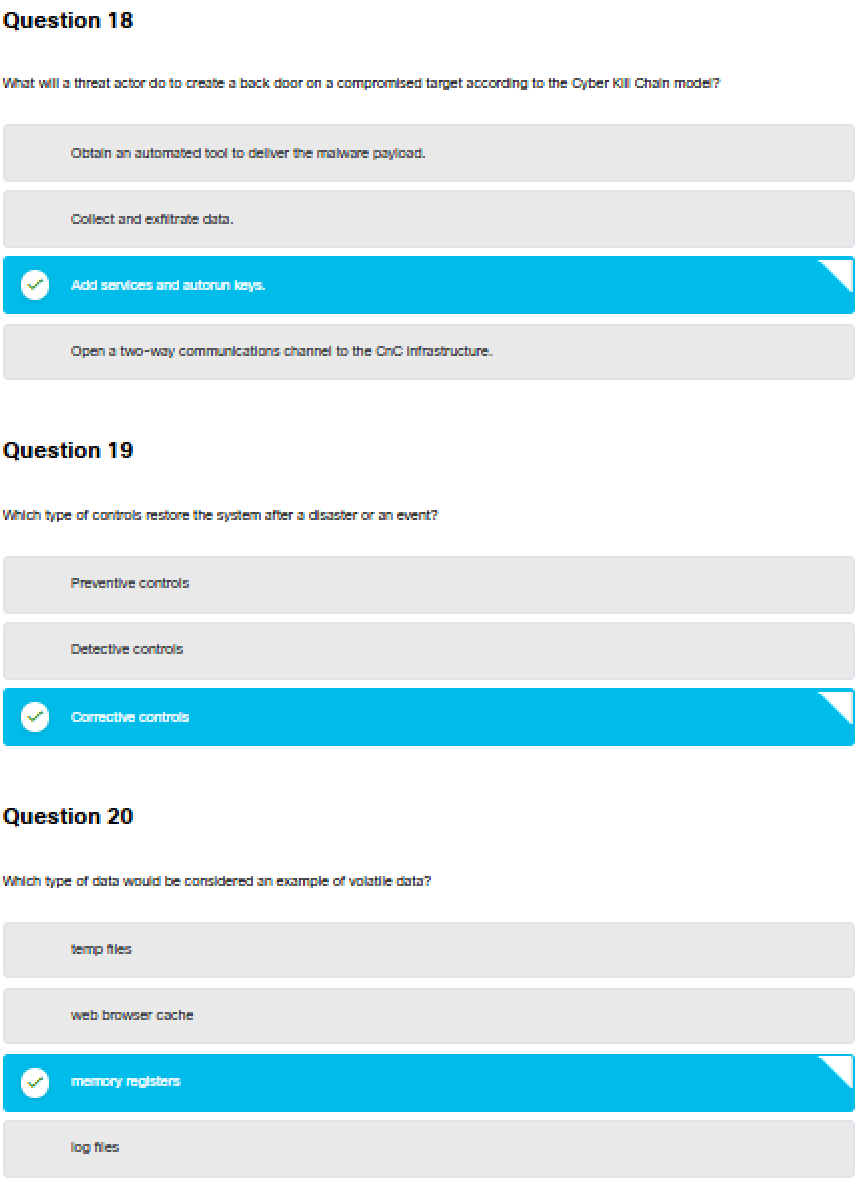
What is a chain of custody?

- 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

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.)

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



Question 18

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

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

Question 19

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

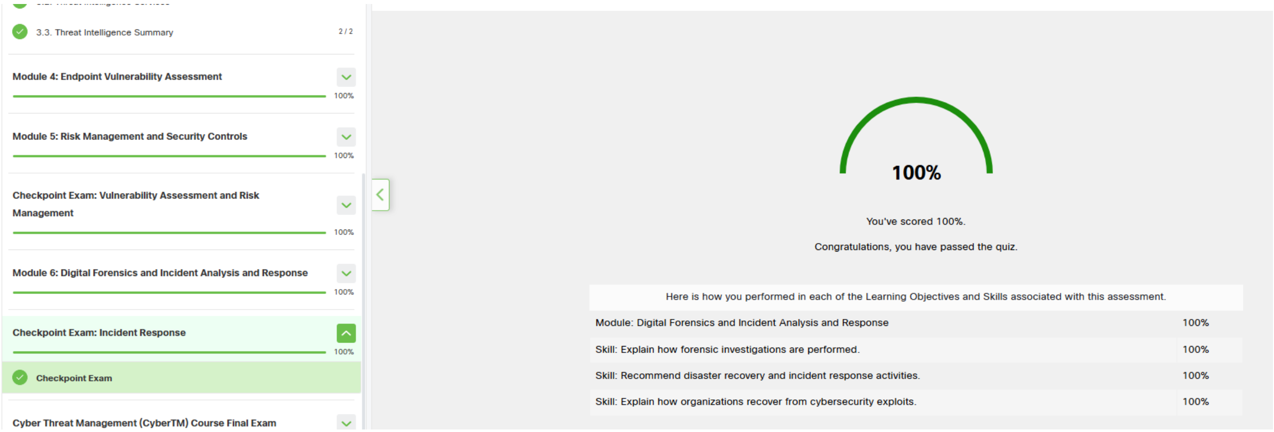
- Preventive controls
- Detective controls
- ✓ Corrective controls

Question 20

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

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

Hasil CheckPoint Exam



3.3. Threat Intelligence Summary 2 / 2

Module 4: Endpoint Vulnerability Assessment 100%

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Module 6: Digital Forensics and Incident Analysis and Response 100%

Checkpoint Exam: Incident Response 100%

✓ Checkpoint Exam

Cyber Threat Management (CyberTM) Course Final Exam

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%