LAPORAN COURSE FINAL EXAM

KEAMANAN SISTEM INFORMASI

Oleh :

Rizqi Hendra Ardiansyah

2141762145

SIB-4C

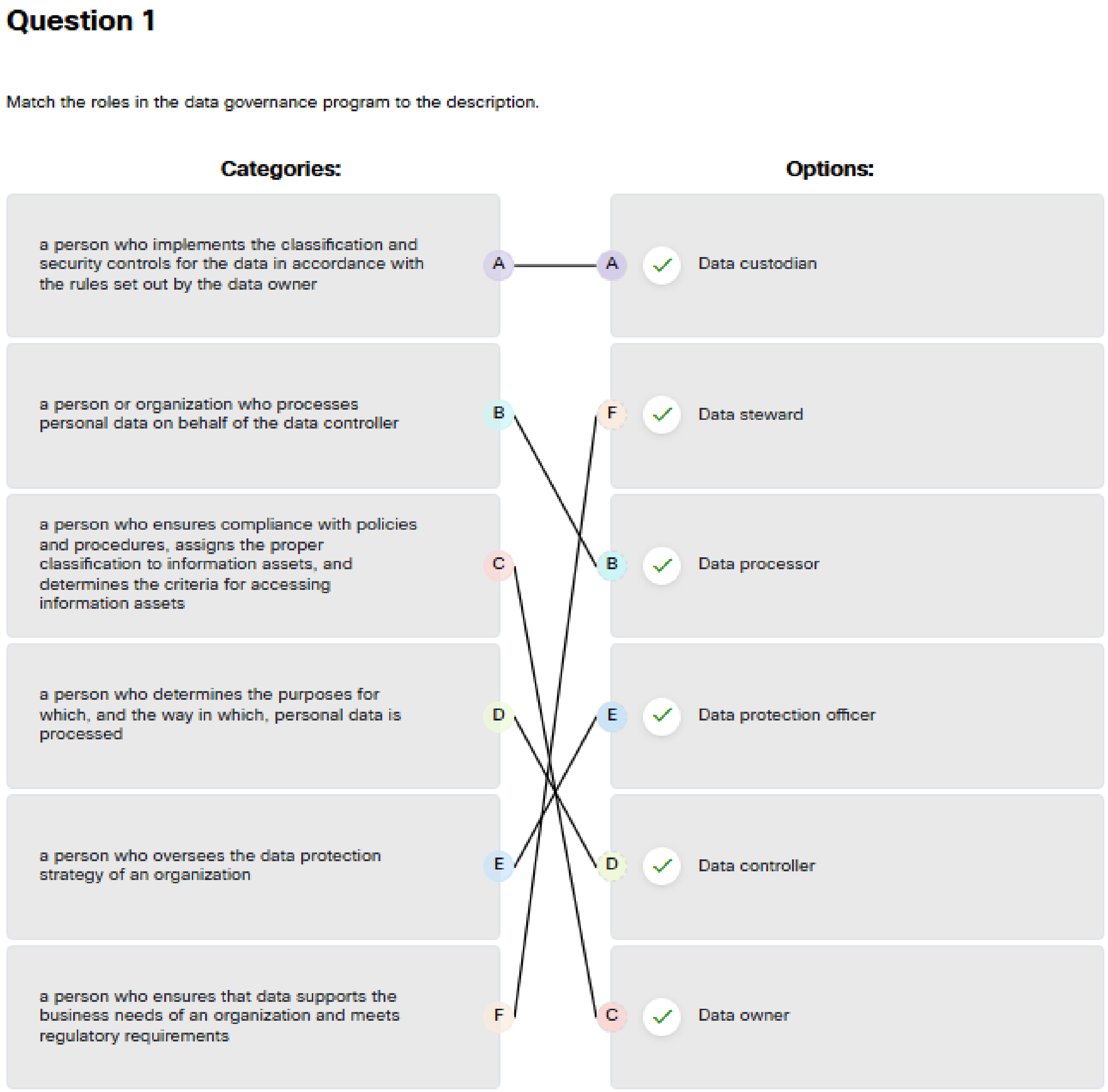
PROGAM STUDI D-IV SISTEM INFORMASI BISNIS

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

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

Course Final Exam



Question 1

Match the roles in the data governance program to the description.

Categories:			Options:
a person who implements the classification and security controls for the data in accordance with the rules set out by the data owner	A	A	✓ Data custodian
a person or organization who processes personal data on behalf of the data controller	B	F	✓ Data steward
a person who ensures compliance with policies and procedures, assigns the proper classification to information assets, and determines the criteria for accessing information assets	C	B	✓ Data processor
a person who determines the purposes for which, and the way in which, personal data is processed	D	E	✓ Data protection officer
a person who oversees the data protection strategy of an organization	E	D	✓ Data controller
a person who ensures that data supports the business needs of an organization and meets regulatory requirements	F	C	✓ Data owner

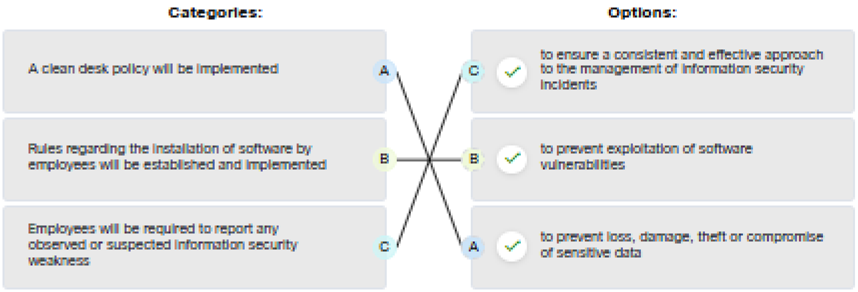
Question 2

If a person knowingly accesses a government computer without permission, what federal act laws would the person be subject to?

- GLBA
- ECPA
- SOX
- [✓ CFAA]

Question 3

A company is preparing for an ISMS audit. Match the right control for each control objective.

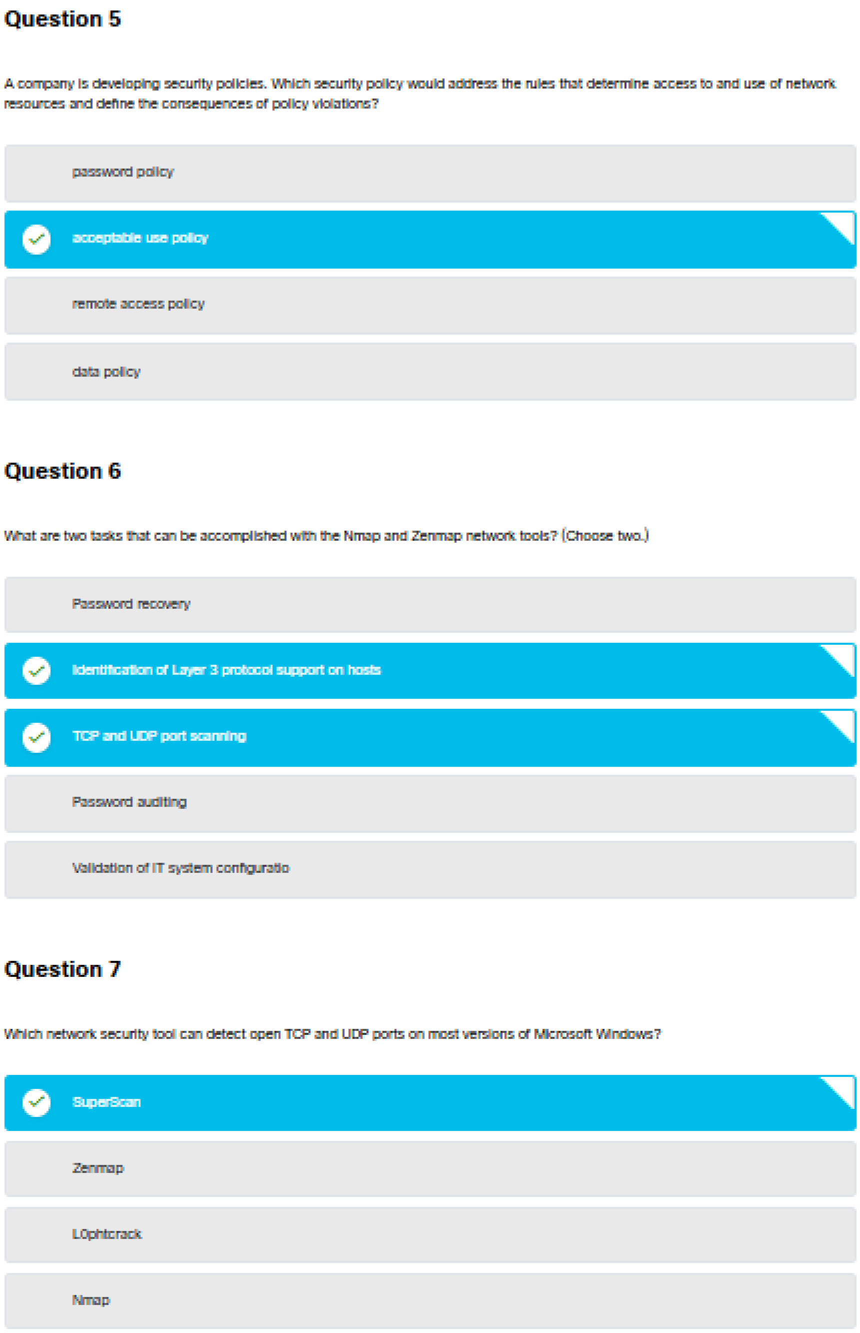


Categories:		Options:
A clean desk policy will be implemented	A	C ✓ to ensure a consistent and effective approach to the management of information security incidents
Rules regarding the installation of software by employees will be established and implemented	B	B ✓ to prevent exploitation of software vulnerabilities
Employees will be required to report any observed or suspected information security weakness	C	A ✓ to prevent loss, damage, theft or compromise of sensitive data

Question 4

What three tasks are accomplished by a comprehensive security policy? (Choose three.)

- [✓ defines legal consequences of violations]
- useful for management
- [✓ sets rules for expected behavior]
- is not legally binding
- [✓ gives security staff the backing of management]
- vagueness



Question 5

A company is developing security policies. Which security policy would address the rules that determine access to and use of network resources and define the consequences of policy violations?

- password policy
- ✓ acceptable use policy
- remote access policy
- data policy

Question 6

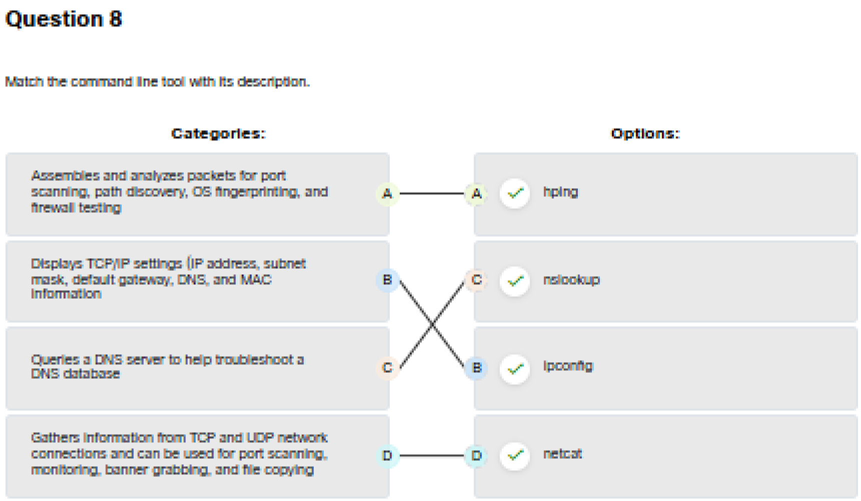
What are two tasks that can be accomplished with the Nmap and Zenmap network tools? (Choose two.)

- Password recovery
- ✓ Identification of Layer 3 protocol support on hosts
- ✓ TCP and UDP port scanning
- Password auditing
- Validation of IT system configuratio

Question 7

Which network security tool can detect open TCP and UDP ports on most versions of Microsoft Windows?

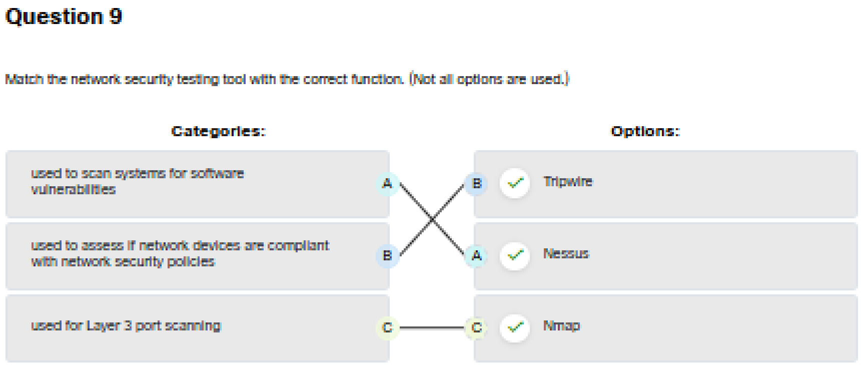
- ✓ SuperScan
- Zenmap
- L0phtcrack
- Nmap



Question 8

Match the command line tool with its description.

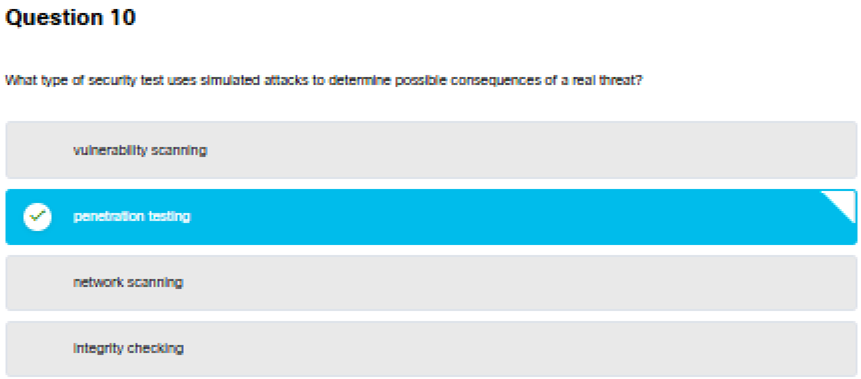
Categories:			Options:
Assembles and analyzes packets for port scanning, path discovery, OS fingerprinting, and firewall testing	A	A	✓ hping
Displays TCP/IP settings (IP address, subnet mask, default gateway, DNS, and MAC information	B	C	✓ nslookup
Queries a DNS server to help troubleshoot a DNS database	C	B	✓ ipconfig
Gathers information from TCP and UDP network connections and can be used for port scanning, monitoring, banner grabbing, and file copying	D	D	✓ netcat



Question 9

Match the network security testing tool with the correct function. (Not all options are used.)

Categories:			Options:
used to scan systems for software vulnerabilities	A	B	✓ Tripwire
used to assess if network devices are compliant with network security policies	B	A	✓ Nessus
used for Layer 3 port scanning	C	C	✓ Nmap



Question 10

What type of security test uses simulated attacks to determine possible consequences of a real threat?

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

Question 11

Which type of controls help uncover new potential threats?

- Preventive controls
- [✓ Detective controls]
- Corrective controls

Question 12

Which security organization maintains a list of common vulnerabilities and exposures (CVE) and is used by prominent security organizations?

- SANDS
- [✓ MITRE]
- SecurityNewsWire
- CIS

Question 13

As a Cybersecurity Analyst, it is very important to keep current. It was suggested by some colleagues that NewsBites contains many good current articles to read. What network security organization maintains this weekly digest?

- MITRE
- (ISC)^2
- CIS
- [✓ SANDS]

Question 14

What three services are offered by FireEye? (Choose three.)

- ✓ blocks attacks across the web
- creates firewall rules dynamically
- ✓ identifies and stops latent malware on files
- ✓ identifies and stops email threat vectors
- subjects all traffic to deep packet inspection analysis
- deploys incident detection rule sets to network security tools

Question 15

What is a characteristic of CybOX?

- It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.
- ✓ It is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations.
- It enables the real-time exchange of cyberthreat indicators between the U.S. Federal Government and the private sector.
- It is a set of specifications for exchanging cyberthreat information between organizations.

Question 16

A network administrator is creating a network profile to generate a network baseline. What is included in the critical asset address space element?

- the time between the establishment of a data flow and its termination
- the TCP and UDP daemons and ports that are allowed to be open on the server
- the list of TCP or UDP processes that are available to accept data
- ✓ the IP addresses or the logical location of essential systems or data

Question 17

In what order are the steps in the vulnerability management life cycle conducted?

- discover, assess, prioritize assets, report, remediate, verify
- discover, prioritize assets, assess, remediate, report, verify
- discover, prioritize assets, assess, remediate, verify, report
- ✓ discover, prioritize assets, assess, report, remediate, verify

Question 18

When a server profile for an organization is being established, which element describes the TCP and UDP daemons and ports that are allowed to be open on the server?

- software environment
- ✓ listening ports
- service accounts
- critical asset address space

Question 19

Which two classes of metrics are included in the CVSS Base Metric Group? (Choose two.)

- Confidentiality Requirement
- ✓ Impact metrics
- Modified Base
- Exploit Code Maturity
- ✓ Exploitability

Question 20

Which step in the Vulnerability Management Life Cycle performs inventory of all assets across the network and identifies host details, including operating system and open services?

assess

remediate

[✓ discover]

prioritize assets

Question 21

Match the stages in the risk management process to the description.

Categories:			Options:
Develop an action plan to reduce overall organization risk exposure. Management should rank and prioritize threats and a team determines how to respond to each threat	A	A	✓ Respond to the risk
Continuously review risk reductions due to elimination, mitigation and transfer actions	B	D	✓ Assess the risk
Identify the threats throughout the organization that increase risk	C	B	✓ Monitor the risk
Once a risk has been identified, it is assessed and analyzed to determine the severity that the threat poses	D	C	✓ Frame the risk

Question 22

Your risk manager just distributed a chart that uses three colors to identify the level of threat to key assets in the information security systems. Red represents high level of risk, yellow represents average level of threat and green represents low level of threat. What type of risk analysis does this chart represent?

loss analysis

exposure factor analysis

quantitative analysis

[✓ qualitative analysis]

Question 23

What is the first step taken in risk assessment?

- Perform audits to verify threats are eliminated.
- ✓ Identify threats and vulnerabilities and the matching of threats with vulnerabilities.
- Compare to any ongoing risk assessment as a means of evaluating risk management effectiveness.
- Establish a baseline to indicate risk before security controls are implemented.

Question 24

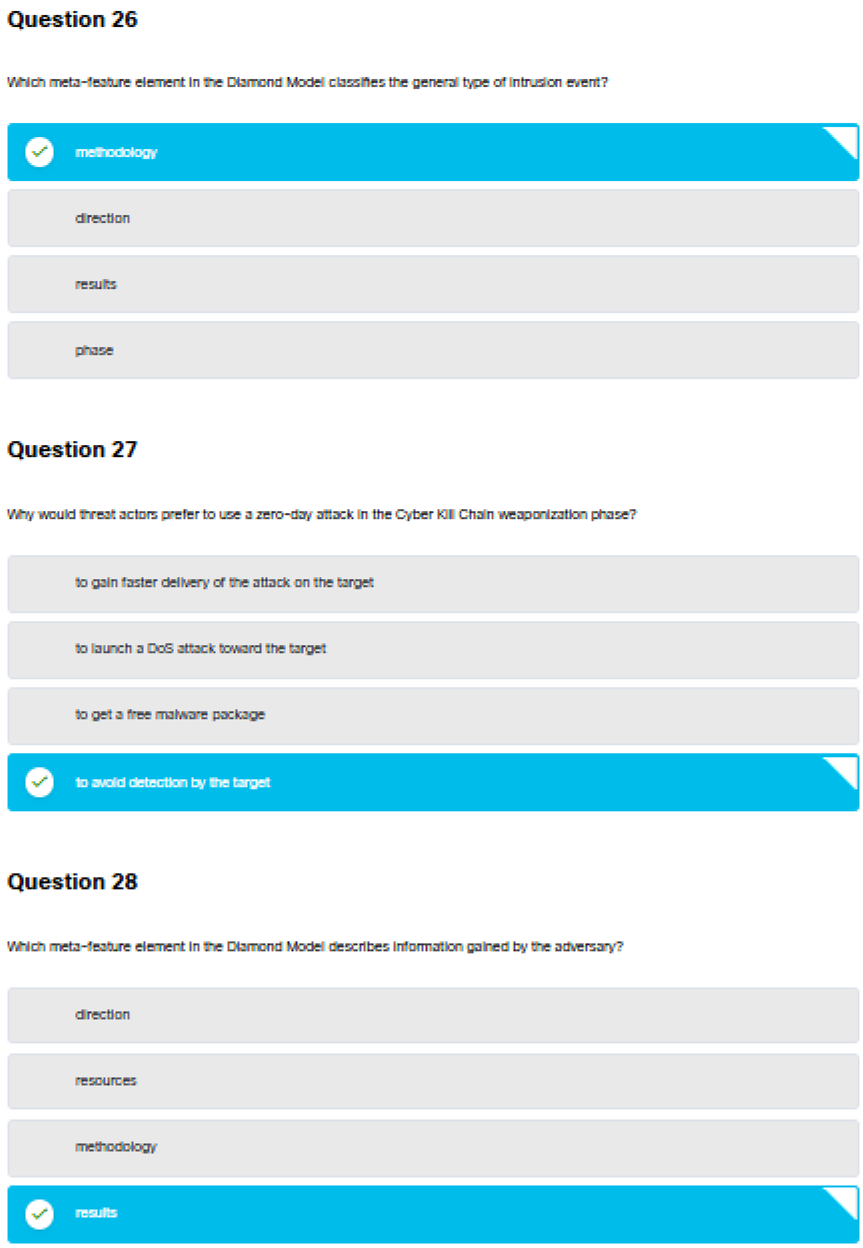
A company manages sensitive customer data for multiple clients. The current authentication mechanism to access the database is username and passphrase. The company is reviewing the risk of employee credential compromise that may lead to a data breach and decides to take action to mitigate the risk before further actions can be taken to eliminate the risk. Which action should the company take for now?

- Purchase an insurance policy.
- Install fingerprint or retinal scanners.
- Enhance data encryption with an advanced algorithm.
- ✓ Implement multi-factor authentication.

Question 25

An organization has implemented antivirus software. What type of security control did the company implement?

- compensative control
- ✓ recovery control
- detective control
- deterrent control



Question 26

Which meta-feature element in the Diamond Model classifies the general type of intrusion event?

- ✓ methodology
- direction
- results
- phase

Question 27

Why would threat actors prefer to use a zero-day attack in the Cyber Kill Chain weaponization phase?

- to gain faster delivery of the attack on the target
- to launch a DoS attack toward the target
- to get a free malware package
- ✓ to avoid detection by the target

Question 28

Which meta-feature element in the Diamond Model describes information gained by the adversary?

- direction
- resources
- methodology
- ✓ results

Question 29

A threat actor has identified the potential vulnerability of the web server of an organization and is building an attack. What will the threat actor possibly do to build an attack weapon?

- Create a point of persistence by adding services.
- ✓ Obtain an automated tool in order to deliver the malware payload through the vulnerability.
- Install a webshell on the web server for persistent access.
- Collect credentials of the web server developers and administrators.

Question 30

To ensure that the chain of custody is maintained, what three items should be logged about evidence that is collected and analyzed after a security incident has occurred? (Choose three.)

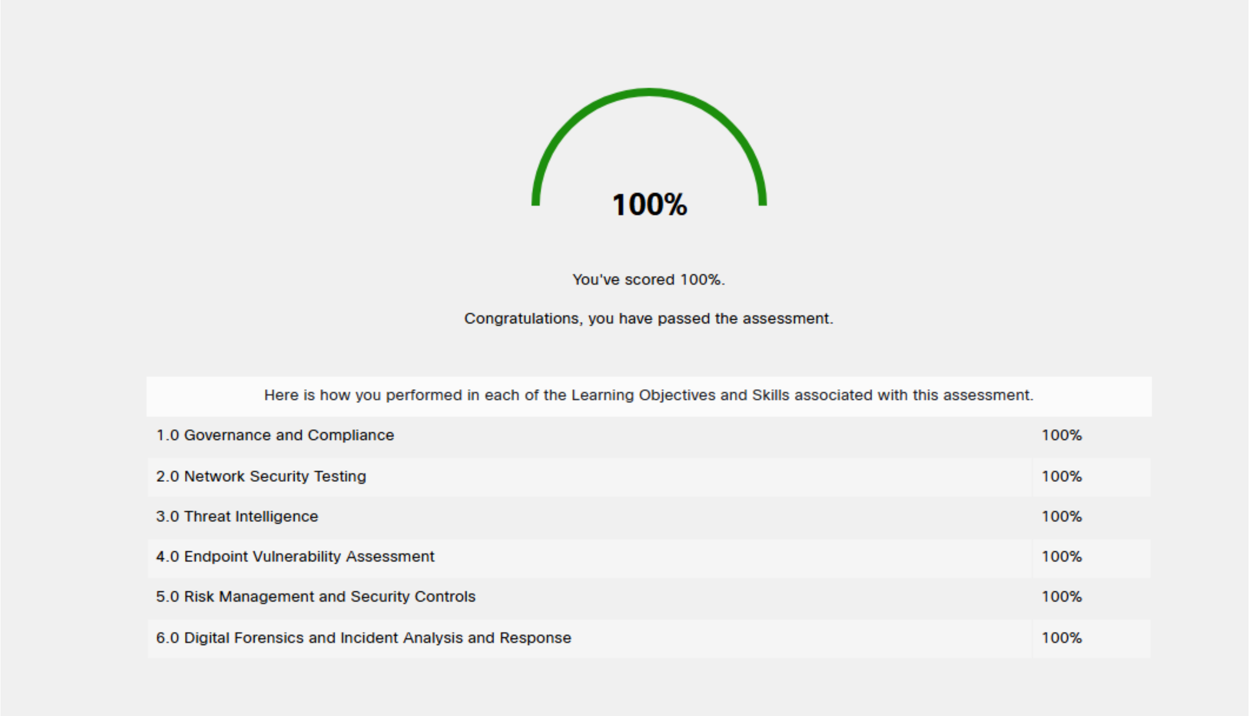
- ✓ location of all evidence
- vulnerabilities that were exploited in an attack
- measures used to prevent an incident
- extent of the damage to resources and assets
- ✓ time and date the evidence was collected
- ✓ serial numbers and hostnames of devices used as evidence

You've submitted your answers!

Reset ✓

Review Assessment

Hasil Course Final Exam



100%

You've scored 100%.

Congratulations, you have passed the assessment.

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

1.0 Governance and Compliance	100%
2.0 Network Security Testing	100%
3.0 Threat Intelligence	100%
4.0 Endpoint Vulnerability Assessment	100%
5.0 Risk Management and Security Controls	100%
6.0 Digital Forensics and Incident Analysis and Response	100%