KEAMANAN SISTEM INFORMASI

Final Exam : Cyber Threat Management

Oleh :

Moh. Samsul Hadi

2141762133

KELAS SIB – 4C

PROGRAM STUDI

D-IV SISTEM INFORMASI BISNIS

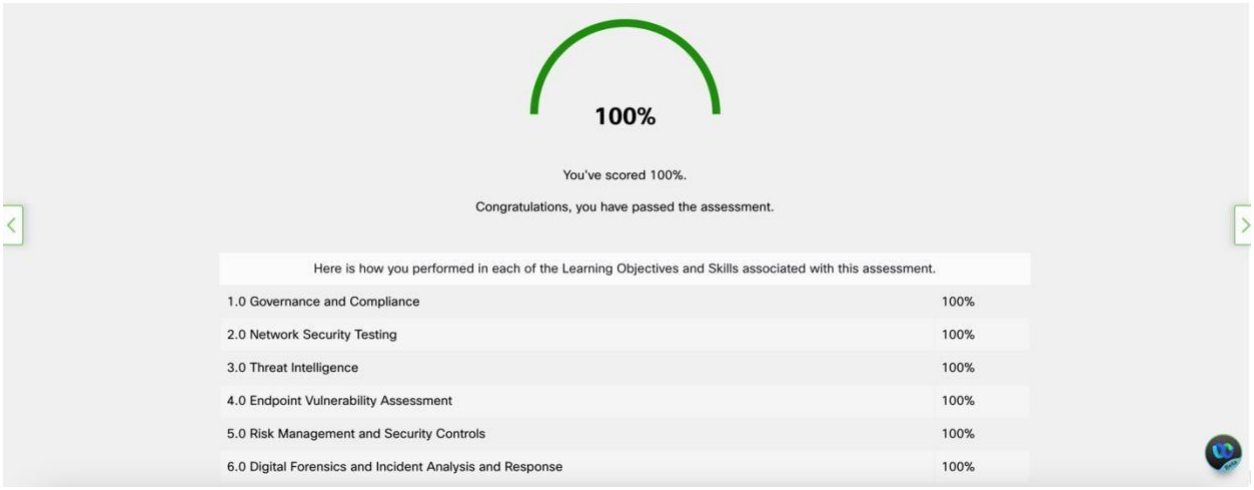
JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

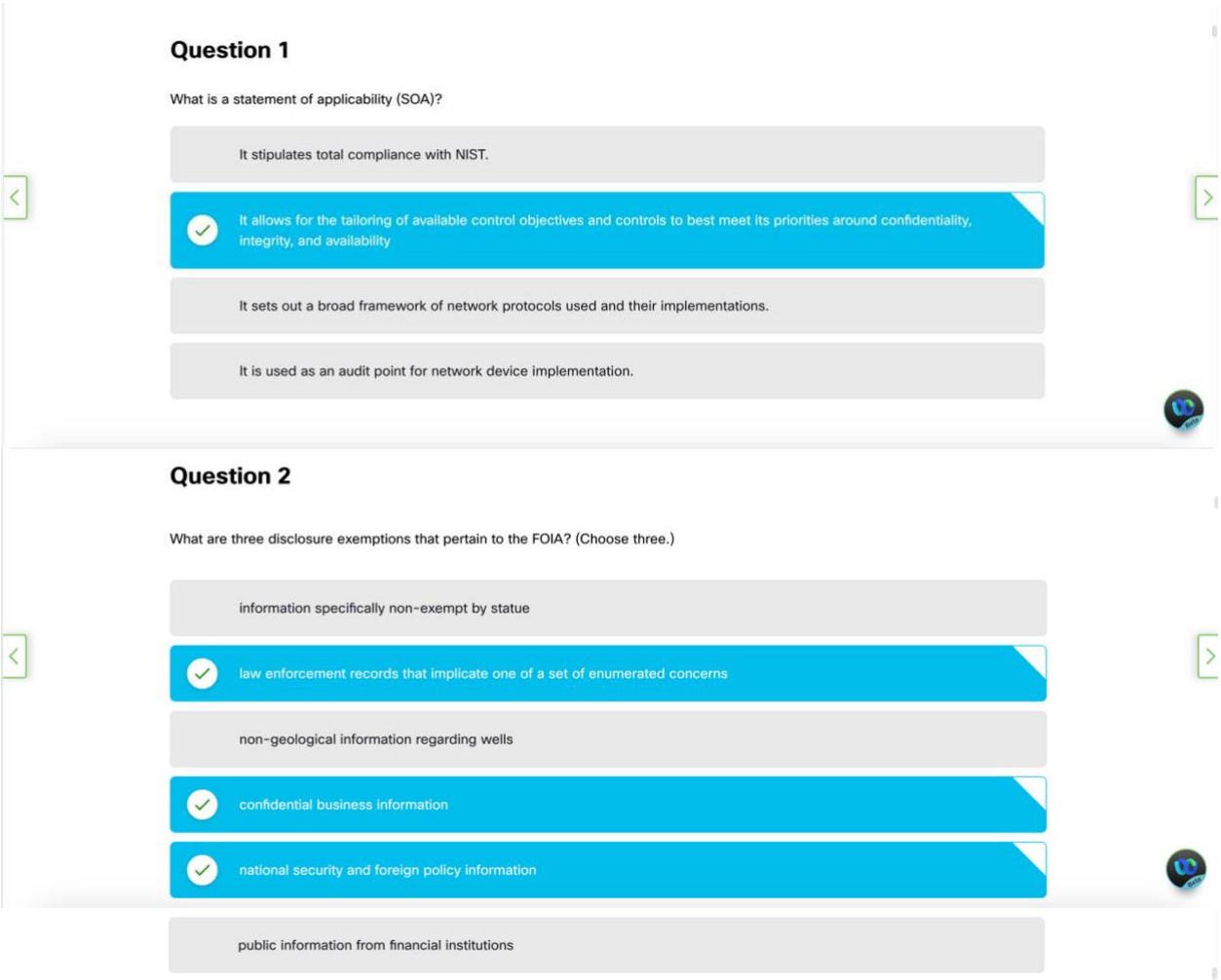
Jl. Soekarno Hatta No.9, Jatimulyo, Kec, Lowokwaru, Kota Malang, Jawa Timur

65141

Final Exam : Cyber Threat Management (Result)



Final Exam : Cyber Threat Management



Question 3

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

Categories:		Options:
Employees will be required to report any observed or suspected information security weakness	A — A	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
A clean desk policy will be implemented	C — C	to prevent loss, damage, theft or compromise of sensitive data

Question 4

An organization is developing a data governance program that follows regulations and policies. Which role in the program is responsible for ensuring compliance with policies and procedures, assigning the proper classification to information assets, and determining the criteria for accessing information assets?

- data controller
- data custodian
- ✓ data owner
- data protection officer

Question 5

Which framework should be recommended for establishing a comprehensive information security management system in an organization?

- ISO OSI model
- NIST/NICE framework
- CIA Triad
- ✓ ISO/IEC 27000

Question 6

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 → C	Tripwire
used for Layer 3 port scanning	B → A	Nessus
used to assess if network devices are compliant with network security policies	C → B	Nmap

Question 7

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

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

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 → B	ipconfig
Displays TCP/IP settings (IP address, subnet mask, default gateway, DNS, and MAC information	B → A	hping
Gathers information from TCP and UDP network connections and can be used for port scanning, monitoring, banner grabbing, and file copying	C → C	netcat
Queries a DNS server to help troubleshoot a DNS database	D → D	nslookup

Question 9

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

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

Question 10

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

- L0phtcrack
- Zenmap
- Nmap
- ✓ SuperScan

Question 11

What key considerations does a business impact analysis (BIA) examine?

Choose four correct answers

- ✓ Recovery time objectives (RTOs)
- ✓ Recovery point objectives (RPOs)
- Recovery point times (RPTs)
- Mean time between objectives (RBOs)
- ✓ Mean time between failures (MTBF)
- ✓ Mean time to repair (MTTR)

Question 12

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

- CIS
- ✓ MITRE
- SecurityNewsWire
- SANDS

Question 13

Which type of controls help uncover new potential threats?

- Preventive controls
- ✓ Detective controls
- Corrective controls

Question 14

What is a characteristic of CybOX?

- ✓ 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 the specification for an application layer protocol that allows the communication of CTI over HTTPS.
- It is a set of specifications for exchanging cyberthreat information between organizations.

Question 15

What three security tools does Cisco Talos maintain security incident detection rule sets for? (Choose three.)

- [x] ClamAV
- [ ] NetStumbler
- [x] SpamCop
- [ ] Socat
- [x] Snort

Question 16

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?

- [ ] prioritize assets
- [x] discover
- [ ] assess
- [ ] remediate

Question 17

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

- [ ] the list of TCP or UDP processes that are available to accept data
- [x] the IP addresses or the logical location of essential systems or data
- [ ] 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

Question 18

Which class of metric in the CVSS Base Metric Group defines the features of the exploit such as the vector, complexity, and user interaction required by the exploit?

- Exploit Code Maturity
- ✓ Exploitability
- Modified Base
- Impact

Question 19

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?

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

Question 20

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

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

Question 21

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.
- Establish a baseline to indicate risk before security controls are implemented.
- Compare to any ongoing risk assessment as a means of evaluating risk management effectiveness.

Question 22

The manager of a new data center requisitions magnetic door locks. The locks will require employees to swipe an ID card to open. Which type of security control is being implemented?

- compensative
- ✓ preventive
- recovery
- corrective

Question 23

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
- quantitative analysis
- ✓ qualitative analysis
- exposure factor analysis

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

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

Categories:		Options:
Identify the threats throughout the organization that increase risk	A	D ✓ Assess the risk
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	B	C ✓ Monitor the risk
Continuously review risk reductions due to elimination, mitigation and transfer actions	C	A ✓ Frame the risk
Once a risk has been identified, it is assessed and analyzed to determine the severity that the threat poses	D	B ✓ Respond to the risk

Question 26

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

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

Question 27

Which type of evidence cannot prove an IT security fact on its own?

- corroborative
- best
- hearsay
- ✓ indirect

Question 28

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.
- Collect credentials of the web server developers and administrators.
- Install a webshell on the web server for persistent access.

Question 29

According to NIST standards, which incident response stakeholder is responsible for coordinating an incident response with other stakeholders to minimize the damage of an incident?

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

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.)

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