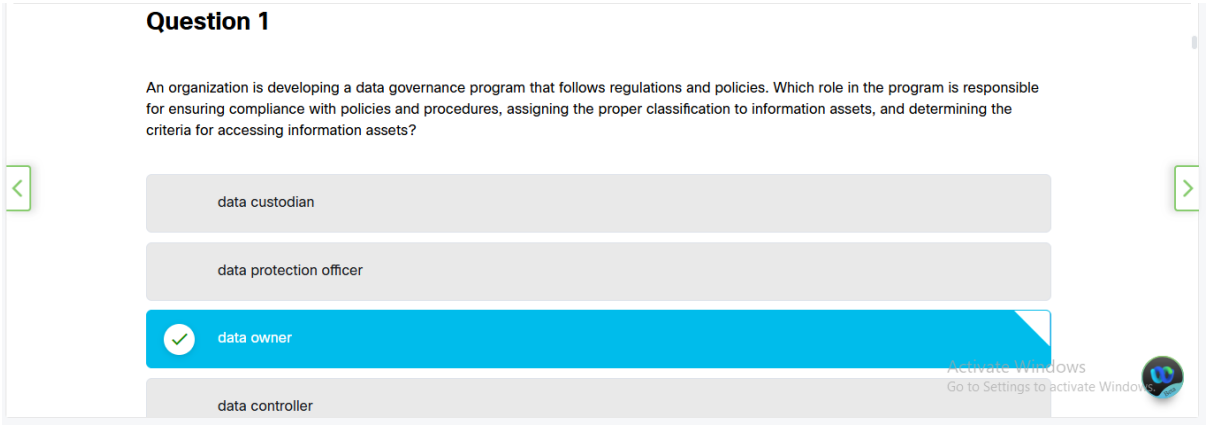
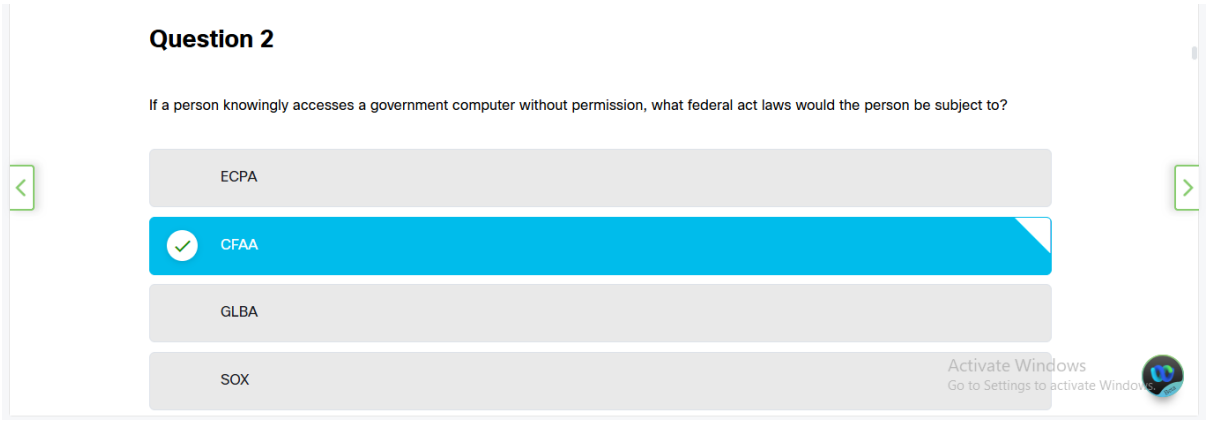
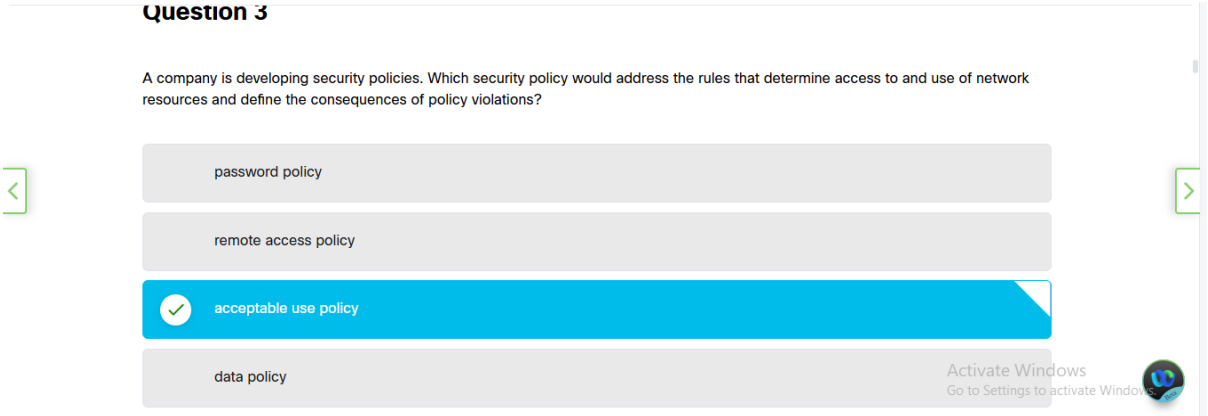
Cyber Threat Management (CyberTM) Course Final Exam

Nama : Mochammad Aldo Rizky

Kelas : SIB : 4C







Question 4

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

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

Question 5

What are three disclosure exemptions that pertain to the FOIA? (Choose three.)

- ✓ confidential business information
- ✓ law enforcement records that implicate one of a set of enumerated concerns
- information specifically non-exempt by statue
- non-geological information regarding wells
- ✓ national security and foreign policy information
- public information from financial institutions

Question 6

Match the command line tool with its description.

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

Question 7

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

- L0phtcrack
- ✓ SuperScan
- Zenmap
- Nmap

Question 8

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

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

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

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

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

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

What is a characteristic of CybOX?

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

Question 13

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

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

Question 14

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

- SecurityNewsWire
- ✓ MITRE
- SANDS
- CIS

Question 15

Which type of controls help uncover new potential threats?

- Preventive controls
- ✓ Detective controls
- Corrective controls

Question 16

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?

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

Question 17

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

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

Question 18

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?

- remediate
- prioritize assets
- ✓ discover
- assess

Question 19

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

Question 20

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?

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

Question 21

What is the first step taken in risk assessment?

- 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.
- Perform audits to verify threats are eliminated.
- ✓ Identify threats and vulnerabilities and the matching of threats with vulnerabilities.

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
- corrective
- recovery
- ✓ preventive

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?

- ✓ qualitative analysis
- exposure factor analysis
- loss analysis
- quantitative analysis

Question 24

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

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

Question 25

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.
- ✓ Implement multi-factor authentication.

Enhance data encryption with an advanced algorithm.

Install fingerprint or retinal scanners.

Question 26

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

legal department

✓ management

human resources

Question 27

Match the security incident stakeholder with the role.

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

Question 28

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

phase

✓ methodology

results

direction

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?

- Install a webshell on the web server for persistent access.
- 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.

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