KEAMANAN
SISTEM INFORMASI
Cyber Threat Management
(CyberTM) Course Final Exam

Nama : Anisatul Latifah
Nim : 2141762008
Jurusan : Teknologi Informasi
Prodi : D-IV Sistem Informasi Bisnis

POLITEKNIK NEGERI MALANG
2024

Question 1

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

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

Question 2

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

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

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

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

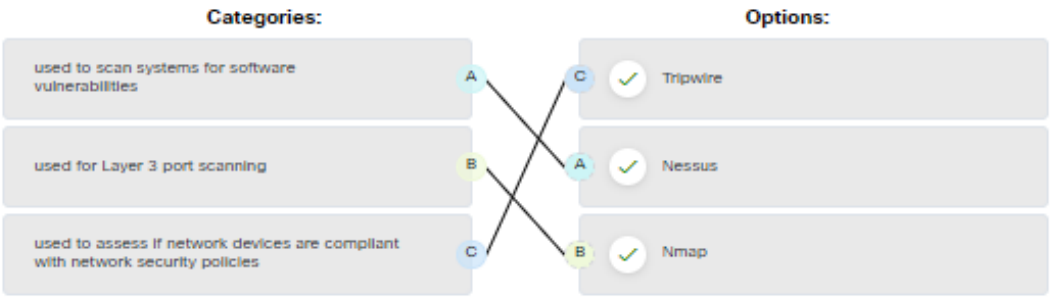
Question 5

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

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

Question 6

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



Question 7

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

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

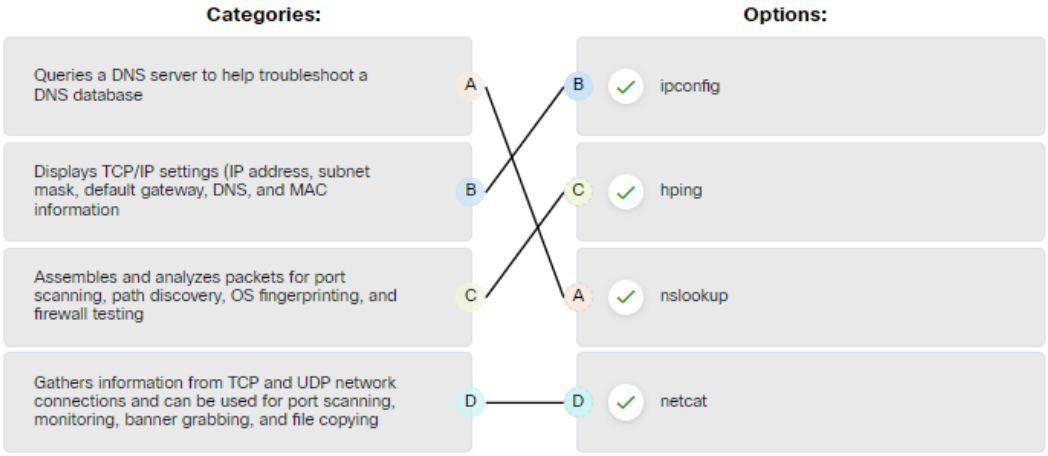
Question 8

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

- L0phtcrack
- ✓ SuperScan
- Nmap
- Zenmap

Question 9

Match the command line tool with its description.



Question 10

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

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

Question 11

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?

- CIS
- $(ISC)^2$
- ✓ SANDS
- MITRE

Question 12

Which type of controls help uncover new potential threats?

- Preventive controls
- ✓ Detective controls
- Corrective controls

Question 13

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 14

What is a characteristic of CybOX?

- 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 specifications for exchanging cyberthreat information between organizations.
- ✓ It is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations.

Question 15

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

- SANDS
- ✓ MITRE
- CIS
- SecurityNewsWire

Question 16

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
- critical asset address space
- software environment
- service accounts

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 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
- the time between the establishment of a data flow and its termination

Question 18

The IT security personnel of an organization notice that the web server deployed in the DMZ is frequently targeted by threat actors. The decision is made to implement a patch management system to manage the server. Which risk management strategy method is being used to respond to the identified risk?

- risk avoidance
- ✓ risk reduction
- risk retention
- risk sharing

Question 19

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

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

Question 20

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
- Modified Base
- ✓ Exploitability
- Impact

Question 21

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?

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

Question 22

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 ✓ Frame the risk
Continuously review risk reductions due to elimination, mitigation and transfer actions	B	C ✓ Respond to 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	C	A ✓ Assess the risk
Identify the threats throughout the organization that increase risk	D	B ✓ Monitor the risk

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?

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

Question 24

What is the first step taken in risk assessment?

- Establish a baseline to indicate risk before security controls are implemented.
- ✓ **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.
- Perform audits to verify threats are eliminated.

Question 25

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?

- ✓ preventive
- recovery
- corrective
- compensative

Question 26

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

- methodology
- ✓ results
- direction
- resources

Question 27

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

- results
- phase
- ✓ methodology
- direction

\

Question 28

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

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

Question 29

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

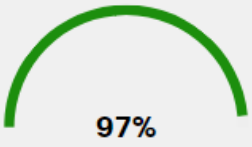
- best
- hearsay
- ✓ **indirect**
- corroborative

Question 30

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?

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

Final Score :



You've scored 97%.

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	92.9%