Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Checkpoint Exam: Vulnerability Assessment and Risk Management

Question 1

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

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

Question 2

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

- SOX
- ✓ PCI DSS
- ECPA
- GLBA

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 3

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?

- Protect and Defend
- Oversight and Development
- Securely Provision
- ✓ Analyze

Question 4

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
- PCI
- FIRPA
- SOX

Question 5

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

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 6

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

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

Question 7

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?

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

Question 8

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?

- malware
- packet analyzer
- ✓ vulnerability scanner
- pentest

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 9

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

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

Question 10

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

- L0phtcrack
- ✓ Tripwire
- Nessus
- Metasploit

Question 11

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

- ✓ MITRE
- DHS
- Cisco Talos
- FireEye

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 12

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

- It is a signature-less engine utilizing stateful attack analysis to detect zero-day threats.
- ✓ 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 cyber threat information between organizations.
- It is a dynamic database of real-time vulnerabilities.

Question 13

How does AIS address a newly discovered threat?

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

Question 14

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

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

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 15

Match the network profile element to the description.

Categories:		Options:
a list of TCP or UDP processes that are available to accept data	A → A	ports used
the time between the establishment of a data flow and its termination	B → D	total throughput
the IP addresses or the logical location of essential systems or data	C → C	critical asset address space
the amount of data passing from a given source to a given destination in a given period of time	D → B	session duration

Question 16

When establishing a network profile for an organization, which element describes the time between the establishment of a data flow and its termination?

- routing protocol convergence
- bandwidth of the Internet connection
- ✓ session duration
- total throughput

Question 17

In addressing an identified risk, which strategy aims to decrease the risk by taking measures to reduce vulnerability?

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

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 18

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

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

Question 19

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?

- verify
- prioritize assets
- ✓ assess
- discover

Question 20

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

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

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 21

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

- so that management has documentation about the number of security attacks that have occurred within a particular time period
- 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 the organization can focus resources where they are most needed

Question 22

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?

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

Question 23

In which situation would a detective control be warranted?

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

Nama : Selly Amelia Putri
NIM : 2141762142
Kelas : SIB 4C
Mata Kuliah : Keamanan Sistem Informasi

Question 24

Based on the risk management process, what should the cybersecurity team do as the next step when a cybersecurity risk is identified?

- Respond to the risk.
- ✓ Assess the risk.
- Frame the risk.
- Monitor the risk.

Question 25

Which risk mitigation strategies include outsourcing services and purchasing insurance?

- reduction
- avoidance
- ✓ transfer
- acceptance