KEAMANAN SISTEM INFORMASI

UTS - Vulnerability Assessment and Risk Management Checkpoint Exam

Disusun untuk Memenuhi UTS Mata Kuliah Manajemen Jaringan Komputer

Oleh:

Wiraswanti Rismanda Putri
NIM: 2141762021

PROGRAM STUDI D-IV SISTEM INFORMASI BISNIS

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

2024

Question 1

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

- ✓ PCI DSS
- GLBA
- SOX
- ECPA

Question 2

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?

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

Question 3

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

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

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
- FIRPA
- SOX
- PCI

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

Question 6

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

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

Question 7

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

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

Question 8

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

- Tripwire
- ✗ Nessus
- L0phtcrack
- Metasploit

Question 9

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?

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

Question 10

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?

- packet analyzer
- pentest
- ✓ vulnerability scanner
- malware

Question 11

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 a set of specifications for exchanging cyber threat information between organizations.
- ✓ It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.
- It is a dynamic database of real-time vulnerabilities.

Question 12

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

- FireEye
- ✓ MITRE
- DHS
- Cisco Talos

Question 13

How does AIS address a newly discovered threat?

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

Question 14

What are the steps in the vulnerability management life cycle?

- detect, analyze, recover, respond
- ✓ discover, prioritize assets, assess, report, remediate, verify
- plan, do, act, check
- identify, protect, detect, respond, recover

Question 15

Match the security management function with the description.

Categories:		Options:
the inventory and control of hardware and software configurations of systems	A	D ✓ vulnerability management
the comprehensive analysis of impacts of attacks on core company assets and functioning	B	C ✓ asset management
the implementation of systems that track the location and configuration of networked devices and software across an enterprise	C	A ✓ configuration management
the security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization	D	B ✓ risk management

Question 16

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

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

Question 17

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

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

Question 18

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

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

Question 19

A security analyst is investigating a cyber attack that began by compromising one file system through a vulnerability in a custom software application. The attack now appears to be affecting additional file systems under the control of another security authority. Which CVSS v3.0 base exploitability metric score is increased by this attack characteristic?

- attack complexity
- user interaction
- ✓ scope
- privileges required

Question 20

Which risk mitigation strategies include outsourcing services and purchasing insurance?

- avoidance
- ✓ transfer
- acceptance
- reduction

Question 21

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

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

Question 22

In which situation would a detective control be warranted?

- ✓ when the organization needs to look for prohibited activity
- 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
- when the organization needs to repair damage

Question 23

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?

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

Question 24

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

- ✓ so that the organization can focus resources where they are most needed
- 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

Question 25

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.
- Monitor the risk.
- Frame the risk.

Hasil Akhir