Check Point Exam : Vulnerability Assesment And Risk Management

Nama : Mochammad Aldo Rizky

Kelas : SIB4C

Question 1

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.)

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

Question 2

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

- ECPA
- SOX
- GLBA
- ✓ PCI DSS

Question 3

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

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

Question 4

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?

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

Question 5

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?

- SOX
- ✓ GLBA
- PCI
- FIRPA

Question 6

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
- malware
- ✓ vulnerability scanner

Question 7

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

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

Question 8

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

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

Question 9

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

- Metasploit
- L0phtcrack
- Nessus
- ✓ Tripwire

Question 10

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?

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

Question 11

How does AIS address a newly discovered threat?

- by mitigating the attack with active response defense mechanisms
- by creating response strategies against the new threat
- 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 12

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

- 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.
- It is a signature-less engine utilizing stateful attack analysis to detect zero-day threats.

Question 13

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

- Cisco Talos
- FireEye
- DHS
- ✓ MITRE

Question 14

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?

- discover
- ✓ assess
- verify
- prioritize assets

Question 15

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

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

Question 16

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?

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

Question 17

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

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

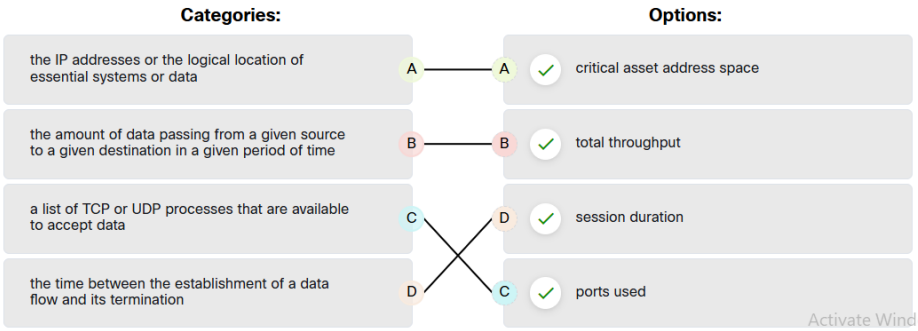
Question 18

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

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

Question 19

Match the network profile element to the description.



Question 20

Which risk mitigation strategies include outsourcing services and purchasing insurance?

- reduction
- ✓ transfer
- avoidance
- acceptance

Question 21

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
- loss analysis
- protection analysis
- ✓ quantitative analysis

Question 22

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

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

Question 23

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 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 management has documentation about the number of security attacks that have occurred within a particular time period

Question 24

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

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

Question 25

In quantitative risk analysis, what term is used to represent the degree of destruction that would occur if an event took place?

- annualized rate of occurrence
- ✓ exposure factor
- annualized loss expectancy
- single loss expectancy