

**Keamanan Jaringan
(Knowledge Check 3&4)**



Dosen Pembimbing :
Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :
Fifin Nur Rahmawati (3122640040)

1 D4 – IT B LJ

**PROGRAM STUDI TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
2023/2024**

Knowledge Check 3

1. Answers : Security Audit

Reason : A security audit is a measurable technical assessment of a system or application. Analyzing physical access to the systems. Designed to ensure that system activity is logged, audited, and monitored in order to detect and respond to security incidents. By regularly reviewing access and activities from log files, organizations can detect any unauthorized access or suspicious activity and take appropriate actions to prevent or mitigate security incidents.

academy.apnic.net/en/course/introduction-to-cybersecurity/module/module-3-cyber-security-controls/quiz/knowledge-check-3

APNIC

Academy Courses ▾ Events ▾ Community Experts ▾

Knowledge Check 3

You will need to achieve a score of 80% or higher to pass the quiz. If you don't pass on your first attempt, you can retake the quiz as needed.

Reviewing access and activities from log files is an example of which of the following security controls?

- ☐ Authentication
- ☒ Security Audit
- ☐ Incident Response
- ☐ Vulnerability management

2. Answers : Applying security patches

Reason : Vulnerability management includes applying security fixes. The process of locating, evaluating, prioritizing, and addressing vulnerabilities in a company's network or information systems is known as vulnerability management. Applying security patches, which are updates to programs or operating systems that address known security flaws, is one of the most important approaches to reduce risks. When software or operating systems are produced, they may have vulnerabilities that can be exploited by attackers. Software providers release security patches to address these flaws and enhance the safety of their products. Organizations can lessen the likelihood that attackers will take advantage of known vulnerabilities by installing security fixes.

Which of the following activities is related to vulnerability management

- ☐ Updating antivirus software signature
- ☐ Applying new firewall rules
- ☐ Enforcing VPN usage on corporate users
- ☒ Applying security patches

3. Answers : Physical

Reason : Physical security is a type of security control that is concerned with preventing unauthorized access to physical assets, such as people, hardware, software, and data, as well as the theft, damage, or destruction of those assets. Physical security measures are employed to thwart physical threats and safeguard the availability, confidentiality, and integrity of data. CCTV cameras can be used to monitor and record activity in and around the data center, while locks can be used to restrict access to the data center and deter unlawful entry.

Securing the data centre with locks and closed-circuit television (CCTV) is an example of which security control category?

- ☒ Physical
- ☐ Technical
- ☐ Policy
- ☐ Virtual

4. Answers : Firewall

Reason : An access control measure known as a firewall can be used to restrict access to particular servers housed at a facility. Firewalls prevent unauthorized access to a computer or network. A firewall is a piece of network security equipment that keeps an eye on and manages incoming and outgoing network traffic in accordance with pre-established security rules.

Which of the following security controls can be used to limit access to certain servers hosted in a facility?

- ☐ Packet Analysis Tool
- ☐ Network Monitoring System
- ☒ Firewall
- ☐ Intrusion Detection System

5. Answers : Virtual Private Network (VPN)

Reason : Virtual Private Network (VPN) is a security control that can be used to protect data that is traversing the network. By encrypting data as it travels via the network, VPNs are frequently used to shield information from unauthorized access and interception by attackers.

Which of the following controls can be used to protect data that is traversing the network?

- ☐ Anti Virus Software
- ☐ Firewall
- ☐ Intrusion Detection System
- ☒ Virtual Private Network (VPN)

6. Answers : Develop policies and procedures for the implementation of security controls

Reason : Organizations can create policies and procedures for putting security controls in place with the use of cyber security frameworks. Cyber security frameworks give organizations a systematic and all-encompassing approach to security by outlining the security controls, rules, and practices required to safeguard their assets from online dangers. Organizations can create policies and processes for the deployment of security measures that are specific to their needs and risk profile by adhering to a cyber security framework.

Cyber Security Frameworks can help organizations to

- ☐ Protect critical services and information assets
- ☐ Detect intrusion attempts and log them to a central repository
- ☐ Secure the network perimeter from unauthorized access
- ☒ Develop policies and procedures for the implementation of security controls

7. Answers : Firewall

Reason : A firewall is a piece of network security equipment that keeps an eye on and manages incoming and outgoing network traffic in accordance with pre-established security rules. Organizations can restrict access to an internal server by implementing firewall rules, enabling only permitted traffic to reach the server.

Access to an internal server can be limited by using which of the following security control?

- ☐ Patch Management
- ☐ Network Monitoring
- ☐ Intrusion Detection System
- ☒ Firewall

Finish Quiz

Academy

[Courses](#) [Events](#) [Community Experts](#)

Knowledge Check 3

You will need to achieve a score of 80% or higher to pass the quiz. If you don't pass on your first attempt, you can retake the quiz as needed.

Results

7 of 7 Questions answered correctly

Your time: 00:19:57

You have reached 7 of 7 point(s), (100%)

[Click Here to Continue](#)

[Restart Quiz](#)

Knowledge Check 4

1. Answers : Ensure compliance to security policies

Reason : Making ensuring security policies are followed is one of a security auditor's major duties. An organization's security policies are a collection of norms, processes, and guidelines for safeguarding its assets, such as its data and information systems.

Knowledge Check 4

You will need to achieve a score of 80% or higher to pass the quiz. If you don't pass on your first attempt, you can retake the quiz as needed.

One of the responsibilities of a security auditor is to

- ☐ Analyze logs and netflows for signs of attacks
- ☒ Ensure compliance to security policies
- ☐ Write signatures for the intrusion detection system
- ☐ Configure firewall rules

2. Answers : Software Developer

Reason : Internally created web applications must be protected from threats like SQL injection and Cross-Site Scripting by software engineers (XSS). To make sure that their apps are not exposed to typical security risks, developers must design and apply safe coding techniques. Developers play a crucial role in the development process. This entails taking the necessary precautions to prevent Cross-Site Scripting (XSS) attacks as well as SQL injection and other forms of injection attacks by performing the necessary input validation.

Which role is responsible for ensuring internally developed web applications are not vulnerable to attacks such as SQL injection or Cross-Site Scripting?

- ☐ Network Engineer
- ☒ Software Developer
- ☐ Security Auditor
- ☐ Security Analyst

3. Answers : Digital Forensics Analyst

Reason : Data recovery and analysis following a security breach are often handled by a digital forensics analyst. The process of preserving, gathering, analyzing, and presenting electronic data in a form that is admissible in a court of law is known as digital forensics. A digital forensics analyst will be in charge of locating and examining the digital evidence connected to an occurrence in the context of a security breach with the aim of pinpointing the root cause and apprehending the culprits.

Which role normally deals with data recovery and examination after a security breach?

- ☒ Digital Forensics Analyst
- ☐ Penetration Tester
- ☐ Security Auditor
- ☐ Network Engineers

4. Answers : Top Management

Reason : The organization's security program's resources must be allocated, and management is ultimately in charge of developing the security plan. The overall responsibility for determining the direction and strategy of the business, including its security strategy.

Which of the following is ultimately responsible for formulating the security strategy and making sure that resources are allocated for the organization-wide security program?

- ☐ Security Auditor
- ☒ Top Management
- ☐ Penetration Tester
- ☐ Security Analyst

Finish Quiz

Knowledge Check 4

You will need to achieve a score of 80% or higher to pass the quiz. If you don't pass on your first attempt, you can retake the quiz as needed.

Results

4 of 4 Questions answered correctly

Your time: 00:19:30

You have reached 4 of 4 point(s), (100%)

Click Here to Continue

Restart Quiz