Course Module Test Module APNIC
Keamanan Jaringan

Dosen Pembimbing :

Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :

Lula Rania Salsabilla (3122640045)

1 D4 – IT B LJ

D4 TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2023

Course Module Test Bab 3

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

   A. Security Audit

   B. Incident Response

   C. Authentication

   D. Vulnerability management

   Analyses

   - A network security audit is a systematic and measurable technical assessment or evaluation of computer security and its applications. This network security audit consists of two parts, namely automatic assessment and non-automated assessment.
   - Automatic assessment is related to making an audit report that is run by a software on changes in the status of files on the computer: create, modify, delete, etc.
   - Non-automated assessments relate to interviewing staff who handle computers, evaluating computer vulnerabilities and security, observing all access to operating systems and application software, and analyzing all physical access to computer systems as a whole.

2. Cyber Security Frameworks can help organizations to

   A. Detect intrusion attempts and log them to a central repository

   B. Protect critical services and information assets

   C. Secure the network perimeter from unauthorized access

   D. Develop policies and procedures for the implementation of security controls

   Analyses

   Cyber security frameworks help teams address cyber security challenges, providing a strategic, well-thought plan to protect its data, infrastructure, and information systems. The frameworks offer guidance, helping IT security leaders manage their organization's cyber risks more intelligently.

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

   A. Firewall

   B. Intrusion Detection System

   C. Anti Virus Software

D. Virtual Private Network (VPN)

Analyses

Virtual Private Network or VPN is a virtual network service that protects your privacy while online on the Internet. The way it works is by masking your IP address and encrypting your traffic so you can go online safely and open content that is blocked in your country or region.

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

   A. Virtual

   B. Physical

   C. Technical

   D. Policy

   Analyses

   Physical security controls include such things as data center perimeter fencing, locks, guards, access control cards, biometric access control systems, surveillance cameras, and intrusion detection sensors.

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

   A. Network Monitoring System

   B. Firewall

   C. Intrusion Detection System

   D. Packet Analysis Tool

   Analyses

   Firewalls prevent unauthorized access to a computer or network, usually installed at the boundary between two networks. Firewalls can be hardware or software running on a computer that acts as a gateway.

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

   A. Patch Management

   B. Network Monitoring

   C. Firewall

D. Intrusion Detection System

Analyses

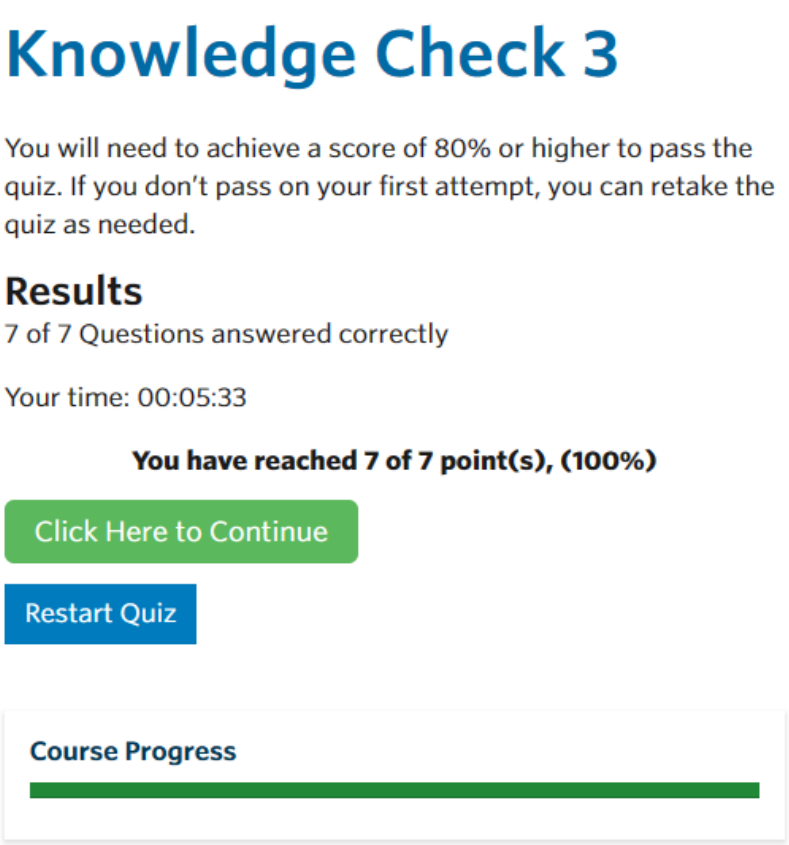
Firewalls prevent unauthorized access to a computer or network, usually installed at the boundary between two networks. Firewalls can be hardware or software running on a computer that acts as a gateway.

7. Which of the following activities is related to vulnerability management
   A. Updating antivirus software signature
   B. Applying security patches
   C. Applying new firewall rules
   D. Enforcing VPN usage on corporate users

Analyses

In the module it is explained that an example of vulnerability management is applying patches or updates in a timely manner is an example of the result of this process.

Result Test



Course Module Test Bab 4

1. One of the responsibilities of a security auditor is to
   A. Analyze logs and netflows for signs of attacks
   B. Ensure compliance to security policies
   C. Write signatures for the intrusion detection system
   D. Configure firewall rules

   Analyses

   Security Auditors are responsible for ensuring that security plans and controls are properly implemented. They assist in identifying practices that do not comply with existing policies or standards. In addition, they will discuss improvement opportunities with relevant stakeholders. The skills required by Security Auditors are familiarity with security standards, a strong technical understanding of the environment being audited, and attention to detail.

2. Which role is responsible for ensuring internally developed web applications are not vulnerable to attacks such as SQL injection or Cross-Site Scripting?
   A. Network Engineer
   B. Security Auditor
   C. Security Analyst
   D. Software Developer

   Analyses

   Software developers are responsible for writing and coding individual programs or providing entirely new software resources based on requirements.

   From a security perspective, there is a need to understand or have an appreciation of the following areas

   - various types of security threats
   - security coding practices so that programs are secure including integrating libraries and security framework
   - address found vulnerabilities and provide patches
   - perform code audits or security testing of programs or applications

3. 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?
    A. Security Analyst
    B. Security Auditor
    C. Top Management
    D. Penetration Tester

    Analyses

    Executive Level → The CEO and Executive level of the organization have a big role in the overall security implementation. Executive level role :

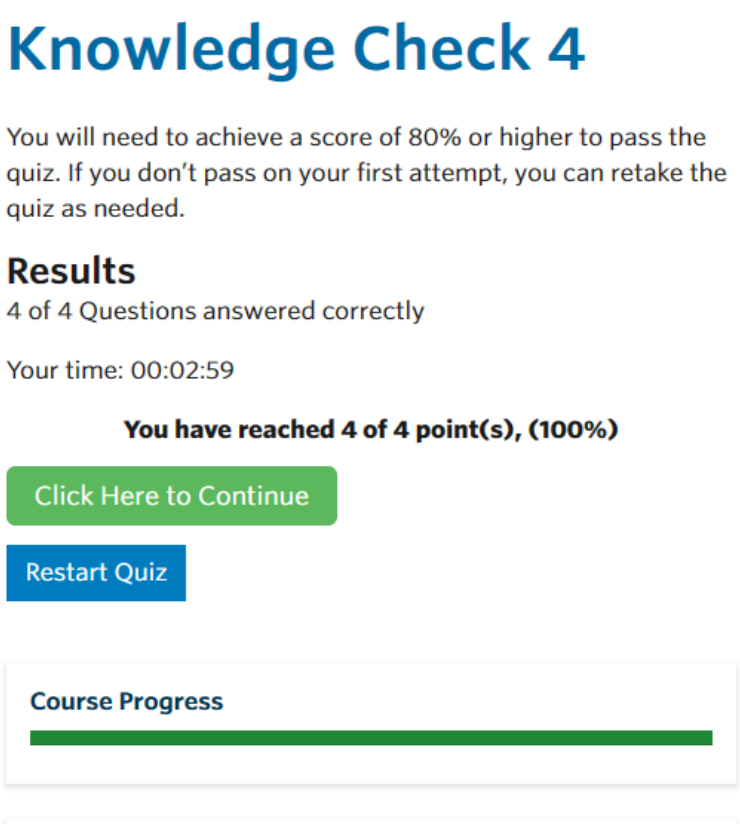
    - Demonstrate leadership by example. cybersecurity is one of the top priorities and critical success factors for organizations
    - Ensure that there is a security strategy, sufficient resources are allocated for security and understand the network defense capabilities of an organization

4. Which role normally deals with data recovery and examination after a security breach?
    A. Network Engineers
    B. Digital Forensics Analyst
    C. Penetration Tester
    D. Security Auditor

    Analyses

    Digital Forensic Analysts have a role to recover and examine data from computers and electronic storage for use as evidence in investigations.

Result Test


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: 00:02:59
You have reached 4 of 4 point(s), (100%)
Click Here to Continue
Restart Quiz
Course Progress