KNOWLEDGE CHECK MODUL 3 DAN 4

Cyber Security Control dan Cyber Security Professionals

DI SUSUN OLEH :

Nadya Indah Trisnawati (3122640034)

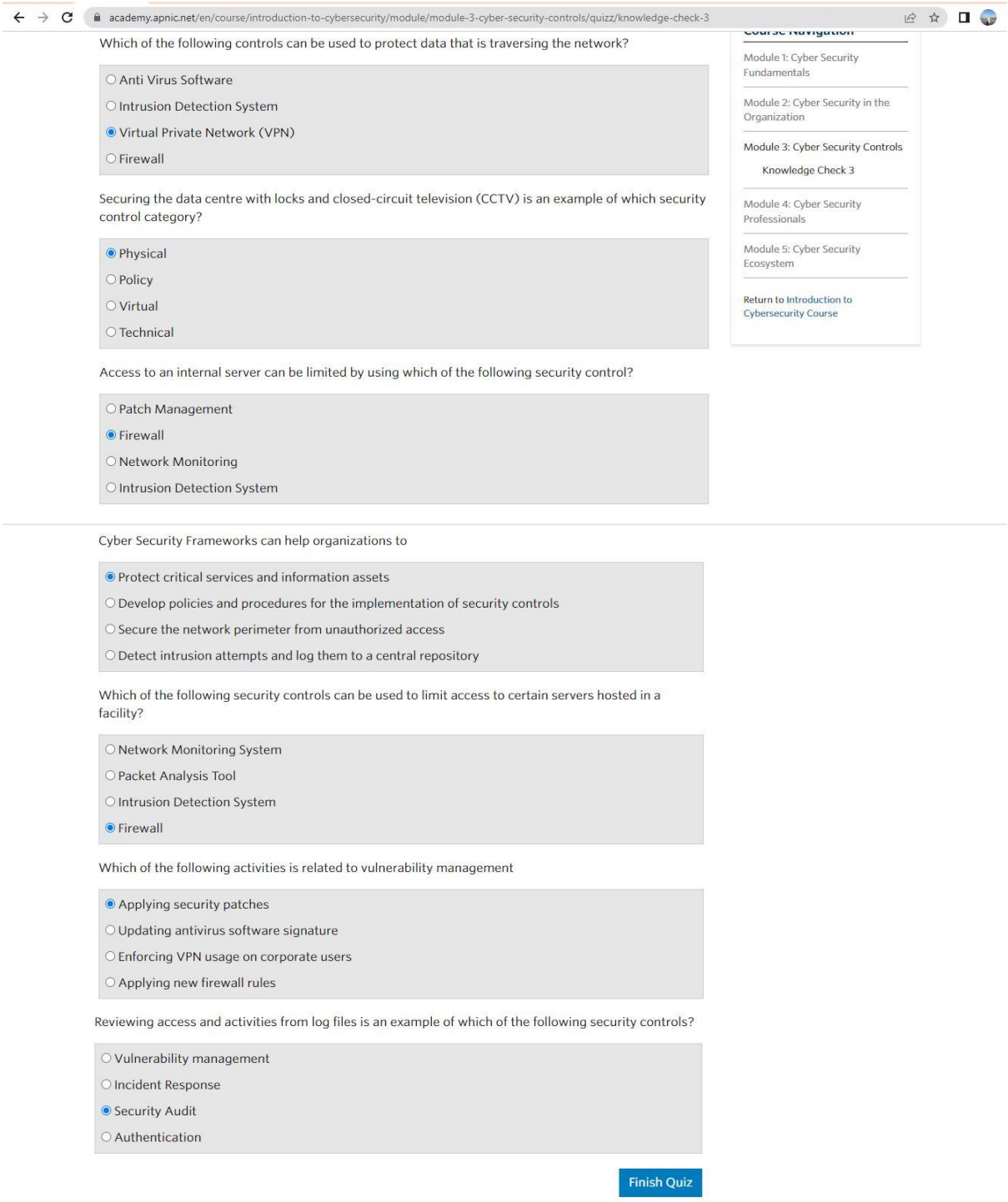
D4 LJ IT B

PROGRAM STUDI TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

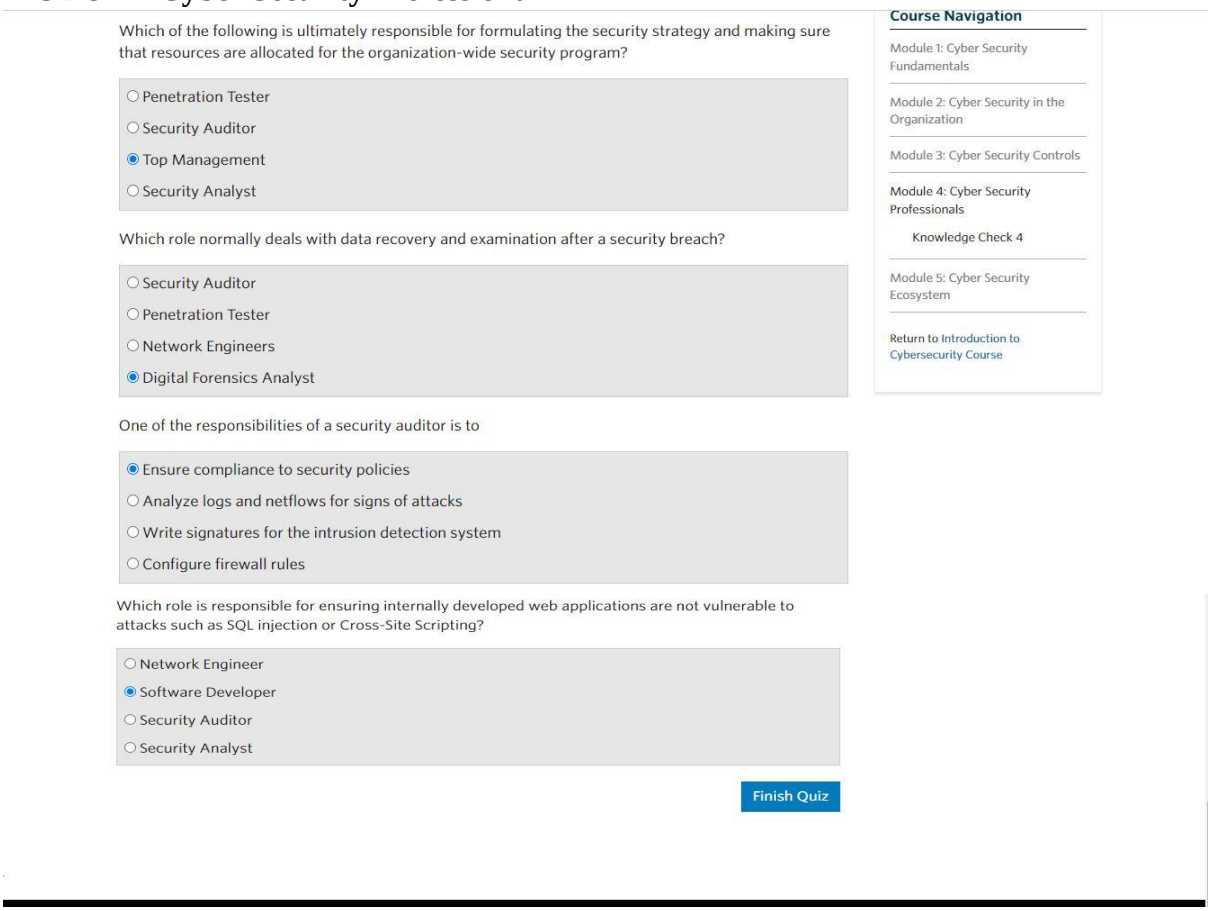
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

MODUL 3 Cyber Security Control



1. Virtual Private Network (VPN) can be used to protect data that is traversing the network. A VPN is a technology that provides a secure and encrypted connection between two devices over an unsecured network such as the internet. When data is transmitted over a VPN, it is encrypted at the sending end and decrypted at the receiving end, ensuring that the data remains confidential and secure.
2. Securing the data centre with locks and closed-circuit television (CCTV) is an example of a physical security control. Physical security controls are measures taken to protect physical assets, such as buildings, equipment, and people, from unauthorized access, theft, damage, or interference.
3. Access to an internal server can be limited by using a firewall security control. Firewalls are a security technology used to control and monitor traffic flowing into and out of a network or system. By configuring a firewall to restrict access to a server from outside the network, you can limit the number of people who can access the server and help to protect it from unauthorized access or attacks.
4. Cyber Security Frameworks can help organizations to establish a comprehensive and risk-based approach to cybersecurity that aligns with their business objectives and supports the protection of critical services and information assets.
5. Firewall can be used to limit access to certain servers hosted in a facility by blocking unauthorized traffic from reaching those servers.
6. Applying security patches is related to vulnerability management. Vulnerability management is the process of identifying, assessing, prioritizing, and mitigating vulnerabilities in software, hardware, and networks. Applying security patches is one way to mitigate vulnerabilities and reduce the risk of exploitation. Updating antivirus software signatures, enforcing VPN usage, and applying new firewall rules are also important security activities, but they are not directly related to vulnerability management.
7. Reviewing access and activities from log files is an example of the security control called Security Audit.

MODUL 4 Cyber Security Professional



1. Top Management is ultimately responsible for formulating the security strategy and ensuring that resources are allocated to the organization-wide security program. Top management has the responsibility to ensure that the organization has an effective and comprehensive security program that is in line with the overall goals and objectives of the organization.
2. Digital Forensics Analysts typically handle data recovery and review after a security breach. A Digital Forensics Analyst is an information security professional who specializes in collecting, analyzing, and recovering electronic data involved in computer crimes or security breaches. They can also assist in determining the source of attacks, recovering lost or deleted data, and providing electronic evidence for courts.
3. One of the responsibilities of a security auditor is to ensure compliance with security policies. Security auditors are professionals responsible for evaluating the security of information systems and the business processes associated with those systems. One of their tasks is to check compliance with the organization's security policies and evaluate the effectiveness of existing security controls.
4. The Software Developer role is responsible for ensuring internally developed web applications are not vulnerable to attacks such as SQL injection or Cross-Site Scripting. A software developer is responsible for designing, developing and maintaining web applications that meet the functional requirements of an organization. Part of this responsibility includes implementing safe coding practices to prevent common vulnerabilities such as SQL injection or Cross-Site Scripting, as well as conducting tests to ensure the application is secure.