LAPORAN KEAMANAN JARINGAN

OLEH :

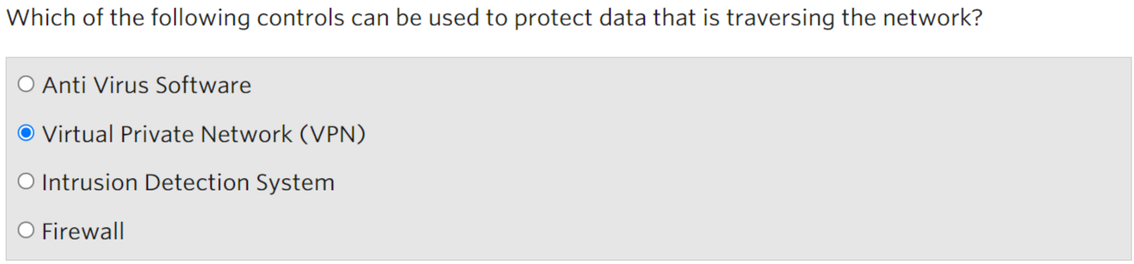
VEHA RAMADHAN DESENDAYA

3122640047

D4 LJ TEKNIK INFORMATIKA

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

Modul APNIC 3 Knowledge Check



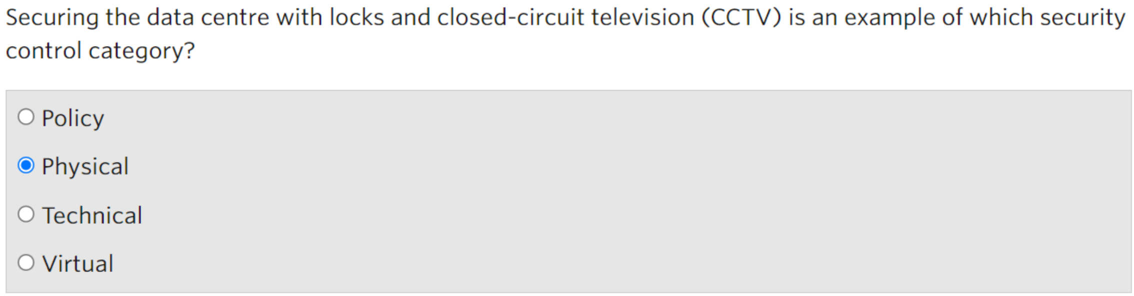
Which of the following controls can be used to protect data that is traversing the network?

○ Anti Virus Software

● Virtual Private Network (VPN)

○ Intrusion Detection System

○ Firewall



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

○ Policy

● Physical

○ Technical

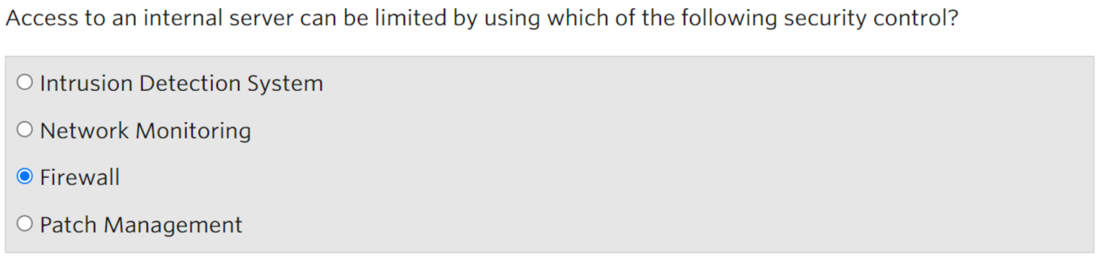
○ Virtual

Which Of the Following Controls can be used to protect data that is traversing the network?

Virtual Private Network (VPN) can be used to protect data that is traversing the network. When data is transmitted over a VPN, it is encrypted and protected from interception and eavesdropping, even if the data is transmitted over a public or insecure network. Anti virus Software, Intrusion Detection System, and Firewall is a type security network, but they cant protect data that is tranversing the network.

Securing the data centre with locks and closed – circuit Televisions (CCTV) is an example of which security Control Category?

That is type of acategory Physical. Because CCTV just can supervise by what it can see not the technical of network security or policy



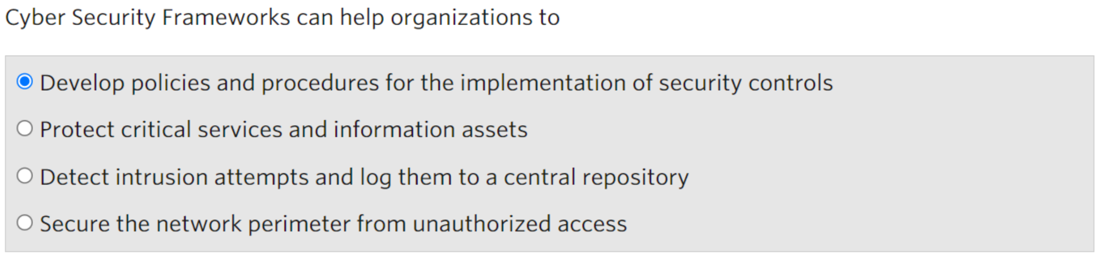
Access to an internal server can be limited by using which of the following security control?

○ Intrusion Detection System

○ Network Monitoring

● Firewall

○ Patch Management



Cyber Security Frameworks can help organizations to

● Develop policies and procedures for the implementation of security controls

○ Protect critical services and information assets

○ Detect intrusion attempts and log them to a central repository

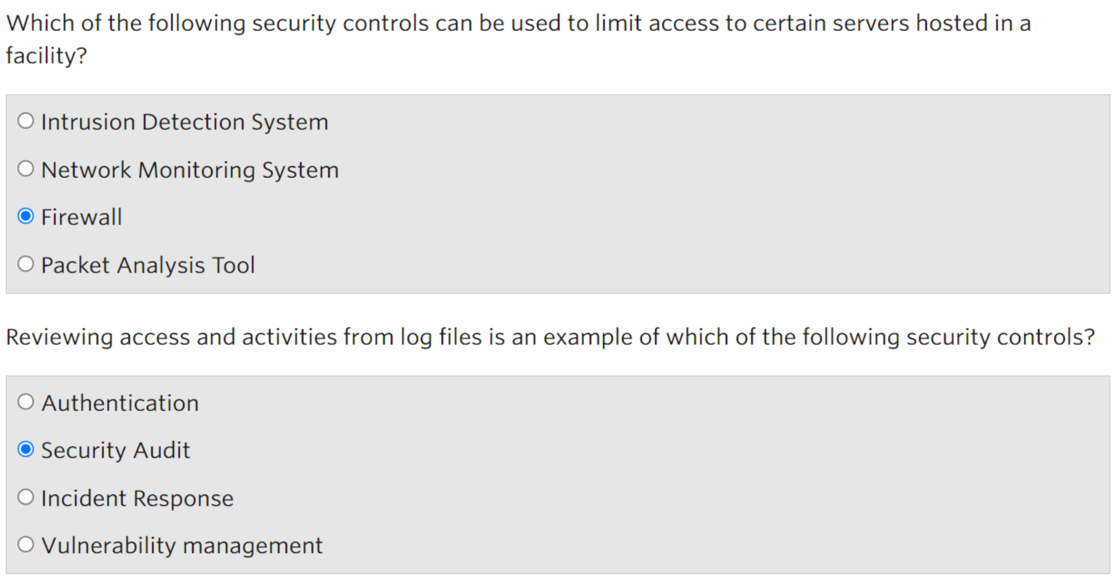
○ Secure the network perimeter from unauthorized access

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

Access to an internal server can be limited by using a firewall. By configuration limited using firewall, an organization can control network traffic which is allowed to reach the server and block any unauthorized or malicious traffic. Patch management is an application to detect vulnerabilities. Network monitoring and Intrusion Detection System are part of security Control but they cant do limit access.

Cyber Security Frameworks can help organizations to?

CSF can help organisations to Develop Policies and Procedure for the implementation of Security control.



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

○ Intrusion Detection System
○ Network Monitoring System
● Firewall
○ Packet Analysis Tool

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

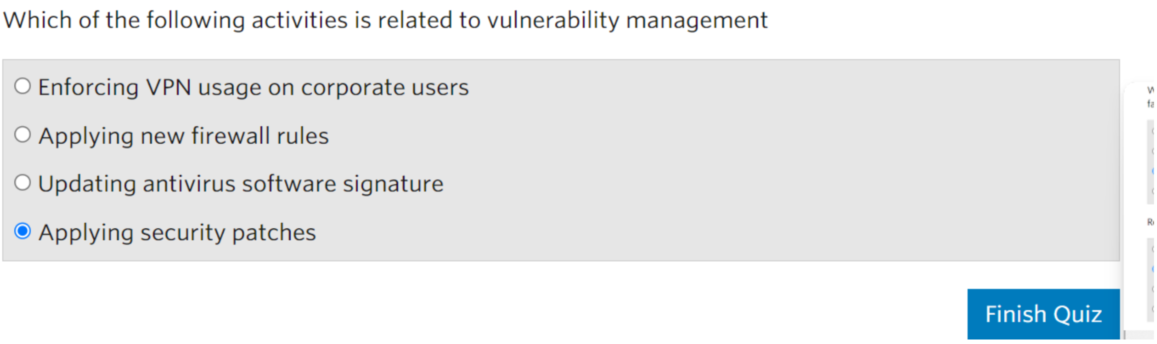
○ Authentication
● Security Audit
○ Incident Response
○ Vulnerability management

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

Firewall can limit acces to certain servers hosted

Reviewing Access and activities from log files is an example of which of the following Security Control?

Reviewing access and activities from log files is an example of a security audit. A security audit is a evaluation system of an organization's security policies, procedures and controls to detect potential security risks. An audit ca reviewing log files to control access and activity on systems.



Which of the following activities is related to vulnerability management

○ Enforcing VPN usage on corporate users

○ Applying new firewall rules

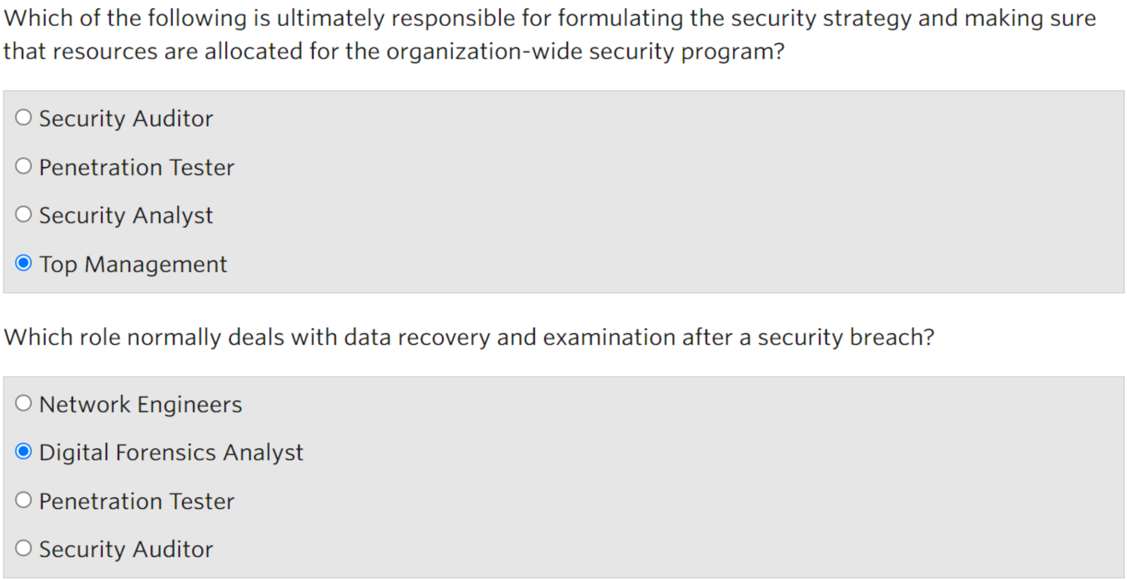
○ Updating antivirus software signature

● Applying security patches

Which of The following activities is related to vulnerability management

Applying security patches is related to vulnerability management. Applying security patches is a important component of vulnerability management because software vulnerabilities are discovered and publicly disclosed, and vendors typically release patches to discovered the vulnerabilities.

Modul 4 Knowledge Check



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

○ Penetration Tester

○ Security Analyst

● Top Management

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

○ Network Engineers

● Digital Forensics Analyst

○ Penetration Tester

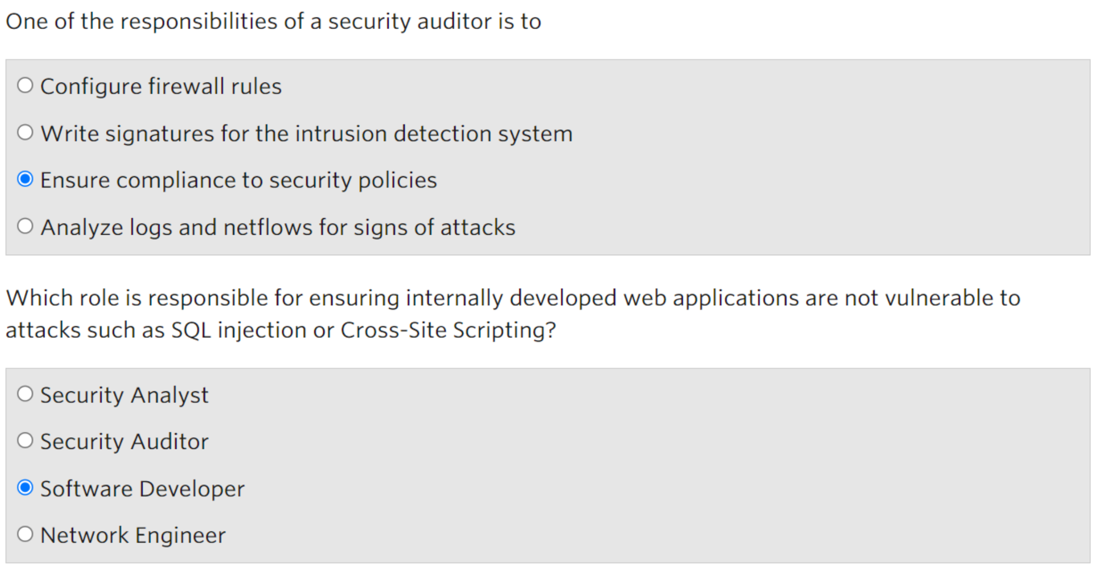
○ Security Auditor

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

The most responsible to dormulating the security strategy and making sure that resource are allocated for organisation security program is Top Management. Because top management have responsibility to ensure that security strategy, allowed resource to security, and have capability cyber defence in the organisation. Security analyse just planning and implementing the network security but doesn't have responsibility to take decision

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

Because everything whose include data recovery is Digital forensic’s task.



One of the responsibilities of a security auditor is to

○ Configure firewall rules

○ Write signatures for the intrusion detection system

● Ensure compliance to security policies

○ Analyze logs and netflows for signs of attacks

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

○ Security Analyst

○ Security Auditor

● Software Developer

○ Network Engineer

One of responsibility of a security auditor is to

Ensure compliance to security policies. A security auditor is responsible for evaluating an organization's security posture to identify potential risks and vulnerabilities, and to ensure that security policies and procedures are being followed.

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

Software Developer have responsible to protect from SQL injection and Cross Site Scripting. Because SQL injection and Cross-Site Scripting is part of software component attack. So, Software Developer have responsibility to ensure that application keep safe.