****

**DEPARTMENT: ICT**

**PROGRAM: INFORMATION TECHNOLOGY**

**MODULE CODE: ITLCS801**

**TITLE: CYBER SECURITY**

**RQF LEVEL: 8 B-Tech**

**Examination**

**Submitted By:** NIYIGABA CLAUDE

On 4st April, 2025

RP-MUSANZE College is a medium-sized technology institution that specializes in high training programs. They store sensitive customer data, including personal information and payment details, on their servers. They have a headquarter and six branches, where the network, which is interconnecting them, is composed of different network devices such as (routers, switches, and servers,). The company implemented various cybersecurity measures to protect their data. However, the company is facing different challenges as follows:

1. Recently, some employees have been experiencing difficulties with their login credentials. They suspect that their accounts might have been compromised.

Using social engineering attack in kali

Email spoofing is a social engineering attack where an attacker forges the sender’s email address to make it appear as if it comes from a trusted source. At RP-MUSANZE College, employees may have received fraudulent emails impersonating IT support or management, asking them to reset passwords, verify accounts, or click on malicious links. This attack likely succeeded due to the lack of email authentication mechanisms such as SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance), which help verify legitimate email senders. Additionally, employee unawareness of phishing tactics, weak password policies, and the absence of Multi-Factor Authentication (MFA) made it easier for attackers to gain access to employee accounts.

To mitigate this issue, RP-MUSANZE College should implement SPF, DKIM, and DMARC on their email servers to authenticate email senders and block spoofed messages. Enabling MFA for employee accounts will provide an extra layer of security, ensuring that even if credentials are compromised, unauthorized access is prevented. Additionally, conducting cybersecurity awareness training will help employees recognize and avoid phishing emails. Deploying email filtering and monitoring tools can detect and block suspicious emails before they reach users. Furthermore, enforcing strong password policies, encouraging the use of password managers, and establishing an incident response plan will strengthen the institution’s overall cybersecurity posture, reducing the risk of future email spoofing attacks.

1. The company's firewall logs show an unusual increase in incoming traffic from a specific IP address located in a foreign country. This traffic is attempting to access the company's internal network.

Cause of the Attack

The unusual increase in incoming traffic from a foreign IP address attempting to access RP-MUSANZE College’s internal network suggests a possible cyberattack, such as a port scanning attack, brute force attack, or Distributed Denial-of-Service (DDoS) attack. Attackers might be trying to exploit open ports, weak authentication methods, or unpatched vulnerabilities to gain unauthorized access to the institution’s network. This could be due to a lack of strict firewall rules, absence of Intrusion Detection Systems (IDS), or weak access controls, allowing malicious traffic to reach the network. If left unchecked, this could lead to a data breach, service disruption, or unauthorized control over network resources.

Solution to the Attack

To mitigate this issue, RP-MUSANZE College should first analyze firewall logs to identify the source and pattern of the attack. Configuring Intrusion Detection and Prevention Systems (IDS/IPS), such as Snort, will help detect and block malicious IP addresses automatically. Additionally, the institution should implement geo-blocking rules on the firewall to restrict traffic from suspicious foreign countries and enforce rate-limiting policies to prevent brute-force login attempts. Updating firewall rules to allow only legitimate traffic, patching network vulnerabilities, and enabling Multi-Factor Authentication (MFA) for remote access will further enhance security.

**Evidence Using Snort to Detect & Block Malicious IPs**

To detect and block malicious IP traffic using Snort, the following rule can be implemented:

alert tcp any any -> $HOME\_NET any (msg:"Suspicious foreign IP detected";

sid:1000001; rev:1; content:"malicious\_payload";

flow:established; detection\_filter:track by\_src, count 10, seconds 30;

classtype:attempted-recon; threshold:type threshold, track by\_src, count 5, seconds 60;)

**To block the IP, an IPS rule can be applied:**

drop ip [192.168.10.100] any -> $HOME\_NET any (msg:"Blocking Malicious IP"; sid:1000002; rev:1;)

These Snort rules help detect unusual traffic patterns and automatically block repeated access attempts from the attacker’s IP. Additionally, firewall rules should be updated to block the specific foreign IP address and monitor future suspicious activity. By implementing these measures, RP-MUSANZE College can protect its network from unauthorized access and potential cyber threats.

1. The company is concerned about the security of data transmitted between their offices and data center. They suspect that data might be intercepted during transmission.

Cause of the Attack

RP-MUSANZE College’s concern about the security of data transmitted between their offices and data center suggests a potential Man-in-the-Middle (MitM) attack or packet sniffing. In such an attack, a hacker intercepts and possibly alters data as it travels between locations. This could be due to unencrypted data transmission, weak VPN configurations, or vulnerable network devices (e.g., compromised routers or switches). If data is transmitted over the internet without encryption, attackers can eavesdrop using packet sniffers like Wireshark to capture sensitive information, including login credentials and payment details. Additionally, if the company’s network lacks secure tunneling protocols, hackers could exploit vulnerabilities to gain unauthorized access.

Solution to the Attack

To prevent data interception, RP-MUSANZE College should implement end-to-end encryption using protocols such as SSL/TLS for web traffic and IPsec or Open VPN for secure communication between offices and the data center. Deploying a Virtual Private Network (VPN) with strong encryption algorithms (e.g., AES-256) will create a secure tunnel for data transmission, preventing unauthorized access. Additionally, enforcing network segmentation and updating firmware on network devices (routers, switches) will help mitigate vulnerabilities. Enabling Intrusion Detection Systems (IDS) to monitor suspicious activities and implementing firewall rules to restrict unauthorized access will further enhance security

1. The IT security team notices an increase in phishing emails targeting employees. Some employees have fallen victim to these attacks, compromising their credentials.

Cause of the Attack

The increase in phishing emails targeting RP-MUSANZE College’s employees suggests that attackers are attempting to steal login credentials and sensitive information through social engineering tactics. These emails may appear to be from trusted sources, such as IT support, management, or financial institutions, and trick employees into clicking malicious links or downloading harmful attachments. The primary causes of this attack include lack of email authentication mechanisms (SPF, DKIM, and DMARC), low employee awareness of phishing threats, and insufficient email filtering security. If employees unknowingly enter their credentials on fake login pages, attackers can gain unauthorized access to internal systems, potentially leading to data breaches or financial loss.

Solution to the Attack

To mitigate phishing attacks, RP-MUSANZE College should implement SPF, DKIM, and DMARC on their email servers to verify email senders and block spoofed messages. Enabling Multi-Factor Authentication (MFA) for employee logins will prevent attackers from accessing accounts, even if credentials are compromised. Conducting regular cybersecurity awareness training will help employees recognize and report phishing attempts. Additionally, email filtering and anti-phishing tools should be deployed to detect and block suspicious emails before they reach users. The security team should also establish an incident response plan to quickly reset compromised accounts, analyze attack patterns, and strengthen security policies.

Tools for Gathering Evidence

To collect evidence of phishing attacks, the IT security team can use the following tools:

* Wireshark – To analyze network traffic and detect suspicious email activity.
* PhishTank – To check and report known phishing URLs.
* Microsoft Defender for Office 365 / Google Workspace Security – To scan and filter phishing emails.
* Gophish – To conduct phishing simulation tests and assess employee awareness.

1. The IT security team detects a suspicious login attempt on their core server. This login attempt was made by a user who should not have access to the server.

Cause of the Attack

The suspicious login attempt on RP-MUSANZE College’s core server indicates a potential unauthorized access attempt, which could result from stolen credentials, brute-force attacks, insider threats, or malware infections. If an attacker has obtained employee login details through phishing or credential leaks, they might try to access restricted systems. Additionally, weak password policies, the lack of Multi-Factor Authentication (MFA), or misconfigured access control may have made the system vulnerable. If this attempt is successful, it could lead to data breaches, system compromise, or unauthorized modifications to critical files.

Solution to the Attack

To mitigate this risk, RP-MUSANZE College should enforce MFA for all privileged accounts, ensuring that even if credentials are stolen, unauthorized access is blocked. The institution should implement strict access controls, following the Principle of Least Privilege (PoLP), allowing only necessary users to access critical servers. Additionally, enabling intrusion detection and prevention systems (IDS/IPS) will help identify and block suspicious login attempts in real time. The IT team should also configure account lockout policies to prevent brute-force attacks, regularly review audit logs, and deploy automated monitoring tools to flag abnormal login behaviors. If unauthorized activity is detected, immediate action should be taken to reset credentials, block suspicious IP addresses, and investigate possible security breaches.

**Using server event logs**

1. Further, the main company network security admin realized that the routers configurations are being modified by their co-admins without consulting him/her.

Cause of the Issue

The unauthorized modification of router configurations by co-admins at RP-MUSANZE College suggests a lack of proper access control, role-based privileges, and change management policies. Without proper logging and approval mechanisms, multiple administrators may have the ability to alter critical network configurations, leading to potential misconfigurations, security vulnerabilities, or service disruptions. This issue can also arise due to insider threats, poor documentation of network changes, or the absence of an audit trail, making it difficult to track who made the changes and why.

Solution to the Issue

To prevent unauthorized modifications, the company should implement Role-Based Access Control (RBAC), ensuring that only authorized personnel can make configuration changes based on their roles. Implementing a Change Management Policy will require all network changes to be reviewed, approved, and documented before implementation. Additionally, enabling Configuration Change Logging and Auditing on routers will help track modifications, identifying who made the changes and when. The security team should also deploy Network Configuration Management (NCM) tools, such as RANCID, SolarWinds NCM, or Cisco Prime Infrastructure, to monitor, log, and alert administrators about unauthorized changes. Finally, implementing backup and rollback mechanisms will ensure that previous configurations can be restored in case of unintended or malicious modifications.

Evidence :hashing, winmerge, hash checker

1. The system administrator was alerted by some system logs about unauthorized public IPs which are accessing systems devices and data.

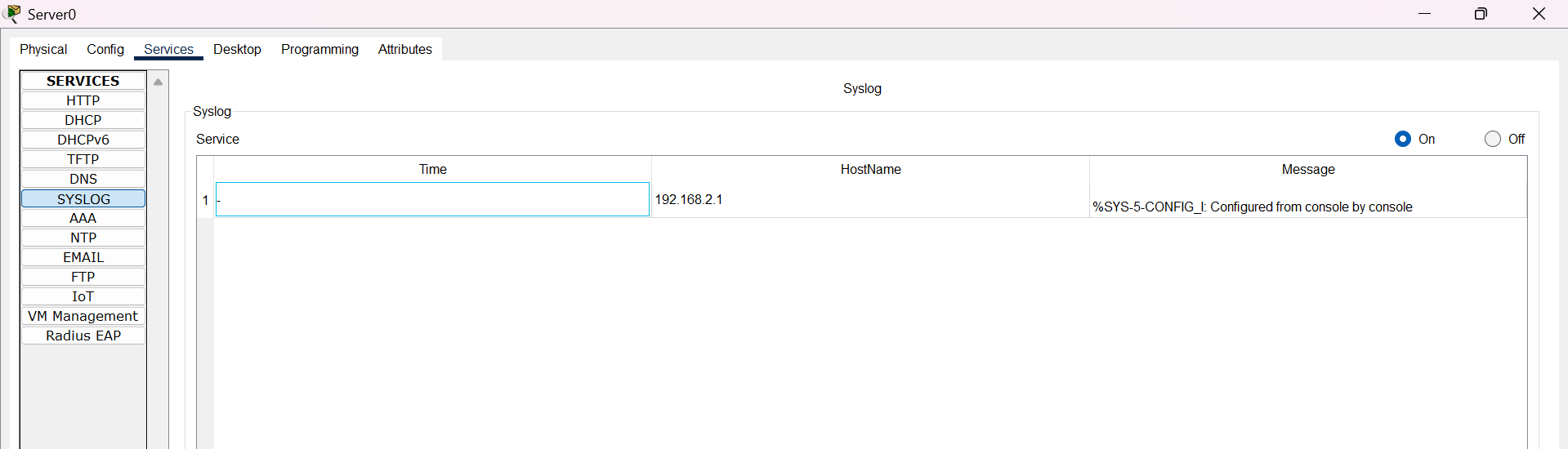
Cause of the Issue

The detection of unauthorized public IPs accessing system devices and data at RP-MUSANZE College suggests a potential security breach, where external attackers or unauthorized users are attempting to gain access to internal systems. This could be caused by misconfigured firewall rules, open ports exposed to the internet, weak authentication mechanisms, or compromised credentials obtained through phishing or brute-force attacks. If public IPs can access critical systems without proper restrictions, it increases the risk of data breaches, system compromise, and malware infections.

Solution to the Issue

To mitigate this threat, the IT security team should immediately review firewall rules and block all unnecessary public IP access, only allowing traffic from trusted sources. Network Access Control (NAC) should be implemented to restrict system access based on predefined security policies. Enforcing Multi-Factor Authentication (MFA) and strong password policies will prevent unauthorized logins, even if credentials are leaked. The security team should deploy Intrusion Detection and Prevention Systems (IDS/IPS) to monitor and automatically block suspicious IPs. Additionally, implementing Geo-IP restrictions can prevent access from foreign or suspicious regions. Continuous log monitoring and alerting tools, such as Splunk, ELK Stack, or OSSEC, should be used to detect and respond to unauthorized access attempts in real-time.

**Server logs**



1. Company suspects one of its employees of stealing proprietary source code and selling it to a competitor. They need evidence for possible legal action.

Cause of the Issue

The suspicion that an employee is stealing proprietary source code and selling it to a competitor at RP-MUSANZE College suggests an insider threat, where a trusted individual misuses their access for personal or financial gain. This could be due to weak access control policies, lack of proper data monitoring, or insufficient logging mechanisms. If employees have unrestricted access to source code repositories without monitoring or role-based access restrictions, they could easily copy, transfer, or sell sensitive information without detection. The absence of Data Loss Prevention (DLP) solutions and insider threat detection tools makes it harder for the company to track suspicious activities.

Solution to the Issue

To address this issue, RP-MUSANZE College should restrict access to source code repositories using Role-Based Access Control (RBAC), ensuring that only authorized employees can view or modify sensitive data. Audit logs and monitoring tools should be enabled on Git repositories, file servers, and cloud storage to track who accessed, modified, or exported critical files. Deploying Data Loss Prevention (DLP) solutions can help detect and prevent unauthorized file transfers. The security team should also implement User Behavior Analytics (UBA) tools like Splunk, Microsoft Defender for Endpoint, or Veriato to monitor unusual activities, such as large data transfers, unauthorized code downloads, or external sharing. Additionally, the company should consult legal experts to gather forensic evidence before taking legal action.