RWANDA POLYTECHNIC

MUSANZE COLLEGE

DEPARTMENT: ICT

PROGRAM: INFORMATION TECHNOLOGY

RQF LEVEL: 8

MODULE: CYBERSECURITY

Academic: 2024-2025

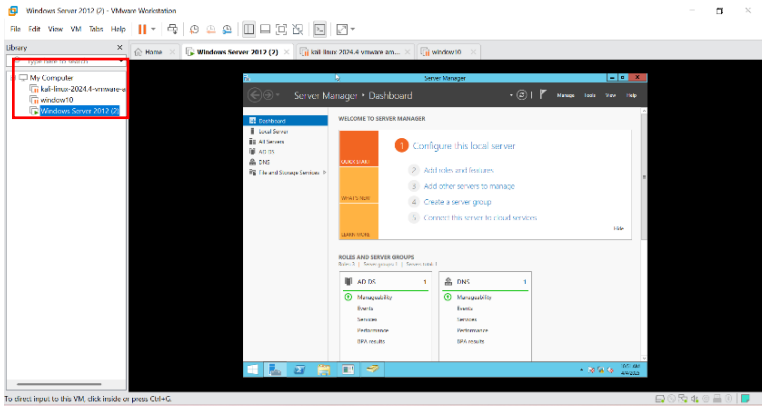
Examination practice

Date: 4/04/2025

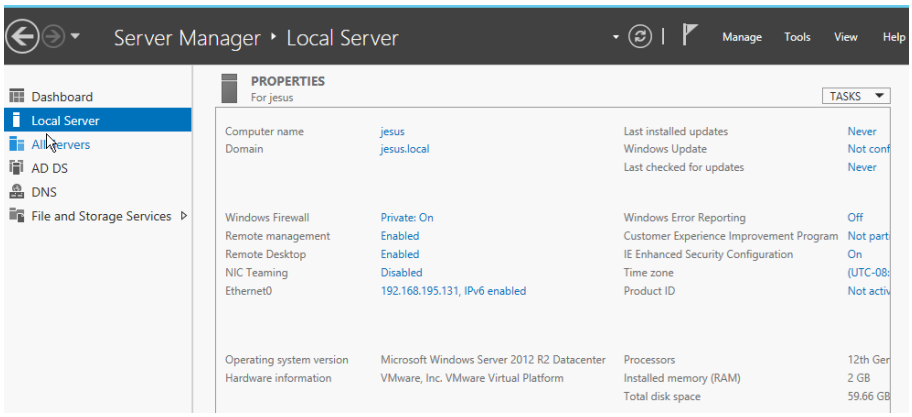
Name: NIYIGABA Claude

Reg No: 24RP14647

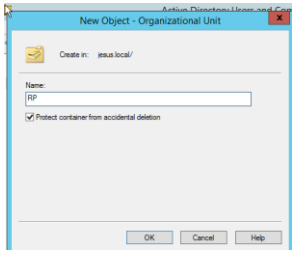
A. This win server, win client(10), kali os



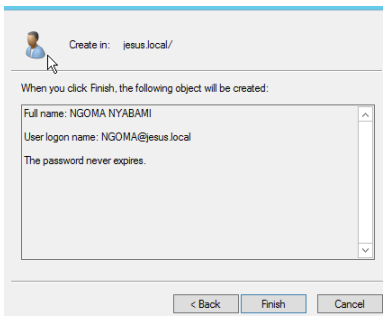
B. Domain name as called jesus.local



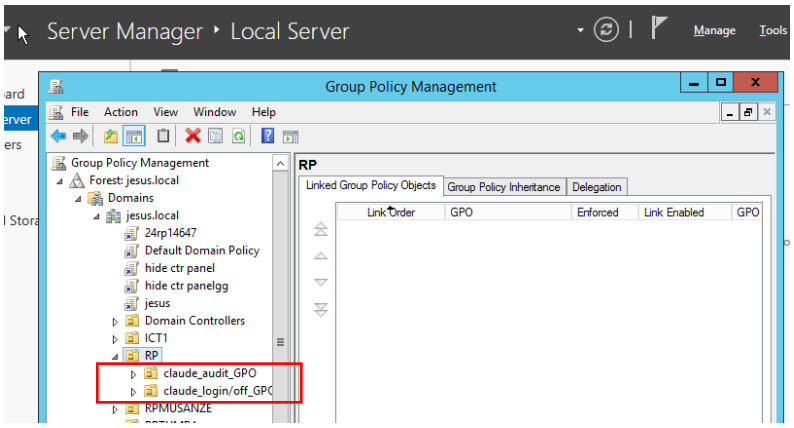
C. Greate OU



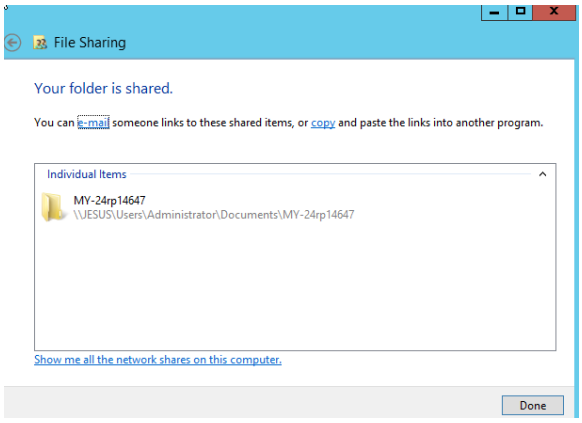
D. CREATE USER



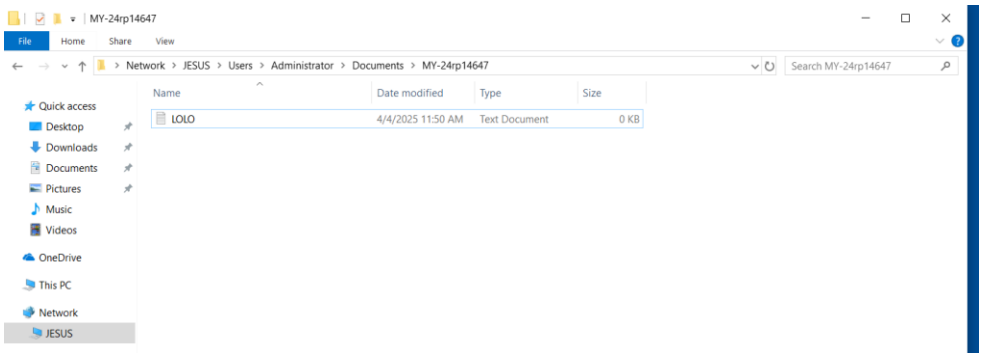
E. Group organization



F. Create folder and share



G. Access it via client and add lolo file



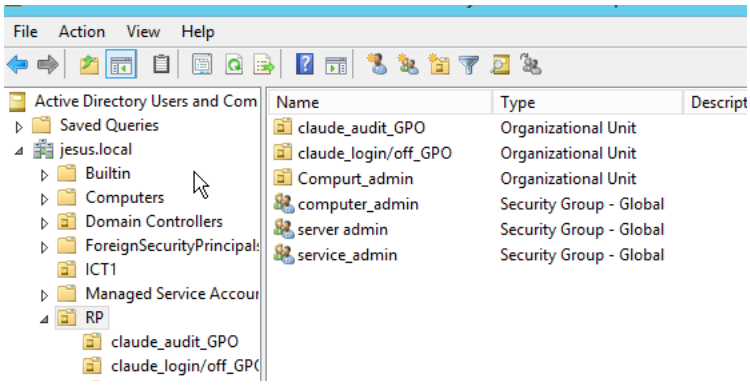
Starting a challenge

1. I was create organization unit and their users with membership and their roles

Where first user in group of chief has access to server_admin, computer-admin and service_admin

And second user group as called tutos hs roles on service_admin and computer-admin

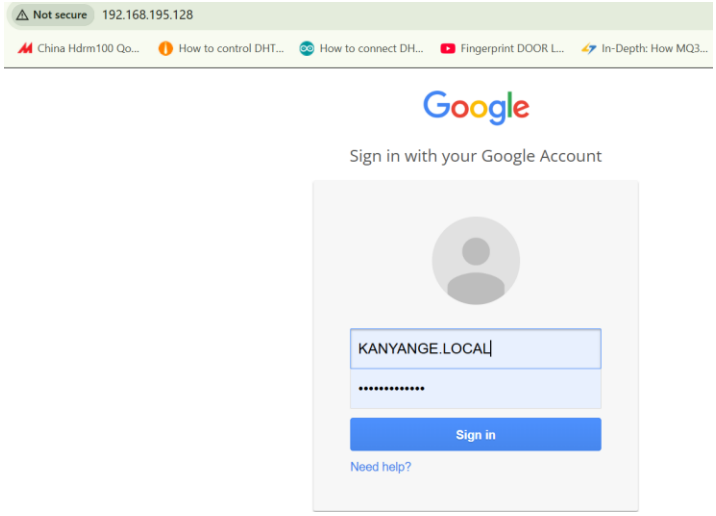
Third grou user are technician wheare has access role to computer-admin



2. Login credential. they suspect that their account might have been compromised

Answer: 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 Rwanda Polytechnic, 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.

The KANYANGE was fill fake google form like



After sending fake google form hacker can get her authentication

```
192.168.195.1 - - [04/Apr/2025 06:38:29] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzB
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=KANYANGE.LOCAL
POSSIBLE PASSWORD FIELD FOUND: Passwd=KANYANGE
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Solution: To mitigate this issue, RP College should implement SPF, DKIM, and DMARC on their email servers to authenticate email senders and block spoofed messages. Enabling MFA for employee accounts, student account will provide an extra layer of security, ensuring that even if credentials are compromised, unauthorized access is prevented.

3. Traffic is attempting to access the institution internal network. using snort rules

Cause of the Attack

The unusual increase in incoming traffic from a foreign IP address attempting to access RP 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.

```
Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{39731FBC-23FC-4298-BD80-D36223F0CB3A}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{B0D44564-71D6-4CBD-B807-3113F1492D86}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{A3B252B6-60B3-4FD1-8E57-08E9E6A2BB91}      WAN Miniport (IP)
    4   D0:39:57:18:CD:28       169.254.149.58  \Device\NPF_{9428FDC3-D23E-4457-AA44-4D7689B83B0C}      Bluetooth Device (Personal Area Network)
    5   D0:39:57:18:CD:27       192.168.10.113  \Device\NPF_{778925A0-89F7-4A3F-BE35-617BC2671673}      Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
    6   00:50:56:C0:00:08       192.168.195.1   \Device\NPF_{45A83533-3674-4E46-8CFB-D70D78C9A12D}      VMware Virtual Ethernet Adapter for VMnet8
    7   00:50:56:C0:00:01       192.168.232.1   \Device\NPF_{3D145C2D-C425-476F-941B-41E0053A8F03}      VMware Virtual Ethernet Adapter for VMnet1
    8   D6:39:57:18:CD:27       169.254.168.46  \Device\NPF_{0F28BA3B-21FC-45AB-B3FA-138F6EA9D1C9}      Microsoft Wi-Fi Direct Virtual Adapter #2
    9   D2:39:57:18:CD:27       169.254.233.64  \Device\NPF_{A0C754D1-1AF0-465D-8110-B7D7A6E2EE25}      Microsoft Wi-Fi Direct Virtual Adapter
   10   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
   11   08:8F:C3:F0:57:31       192.168.1.2     \Device\NPF_{578AA7D2-73BD-4F54-8C01-6C462219C39D}      Intel(R) Ethernet Connection (16) I219-V

C:\Snort\bin>
```

Solution to the Attack

To mitigate this issue, RP 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. 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.

Configuration firewall rule like

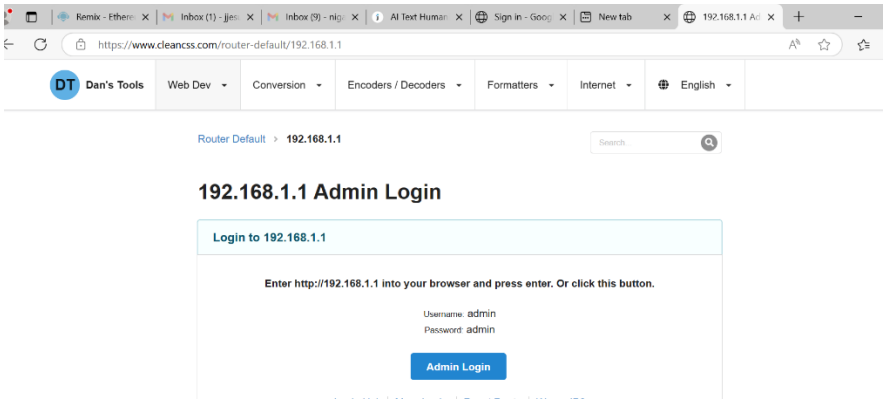
```
# LOCAL RULES
#-------------

Alert icmp  any any -> any any (msg:”testing ICMP alert”; sid:1000001;)
Alert udp  any any -> any any (msg:”testing udp alert”; sid:1000002;)
Alert tcp any any -> any any (msg:”testing tcp alert”; sid:1000003;)
drop ip [192.168.10.100] any (msg:"Blocking Malicious IP"; sid:1000002; rev:1;)
drop ip [192.168.10.100] any (msg:"Blocking Malicious IP"; sid:1000002; rev:1;)
```

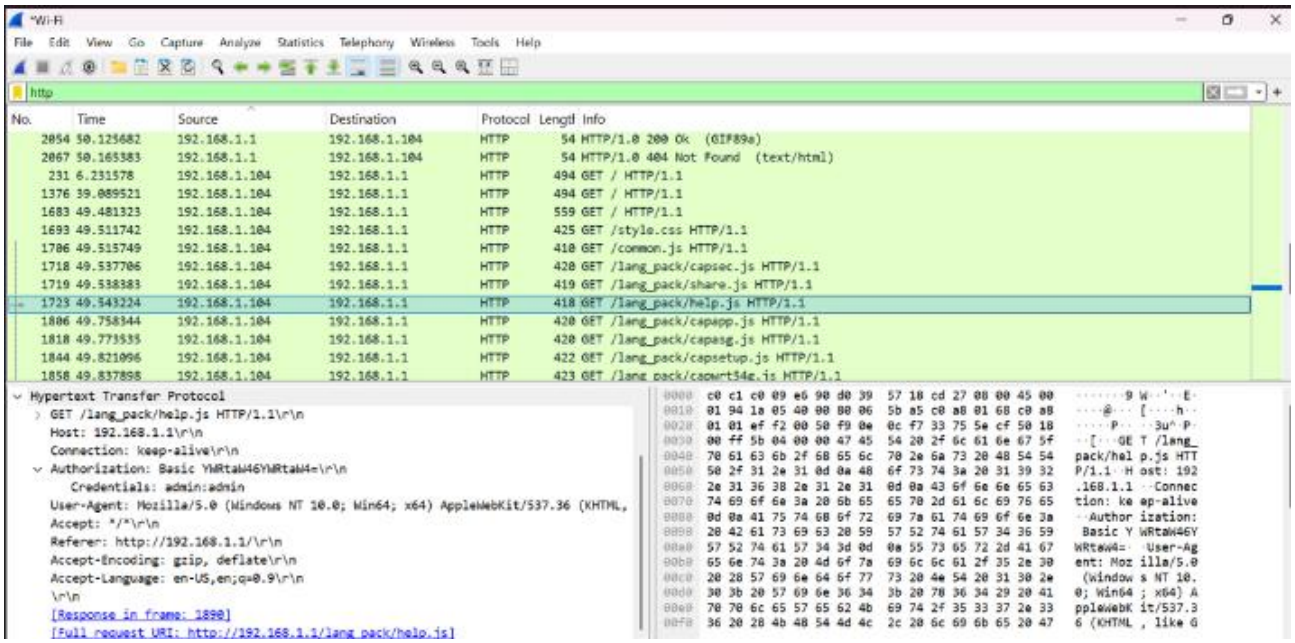
4. The institution is concerned about the security of data transmitted between their offices and data center. They suspect that data might be intercepted during transmission. (wireshake tool)

i. Cause of the Attack

RP 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.



ii. Scanning using wireshake



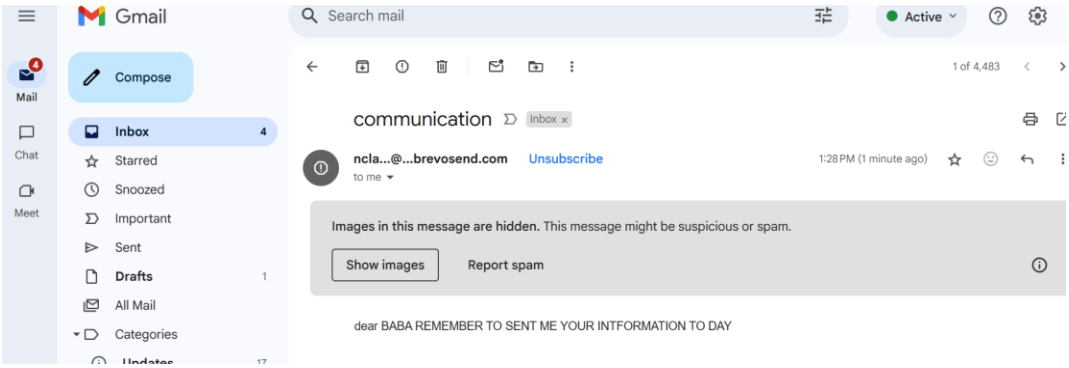
iii. Solution to the Attack

To prevent data interception, RP 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.will create a secure tunnel for data transmission, preventing unauthorized access.

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

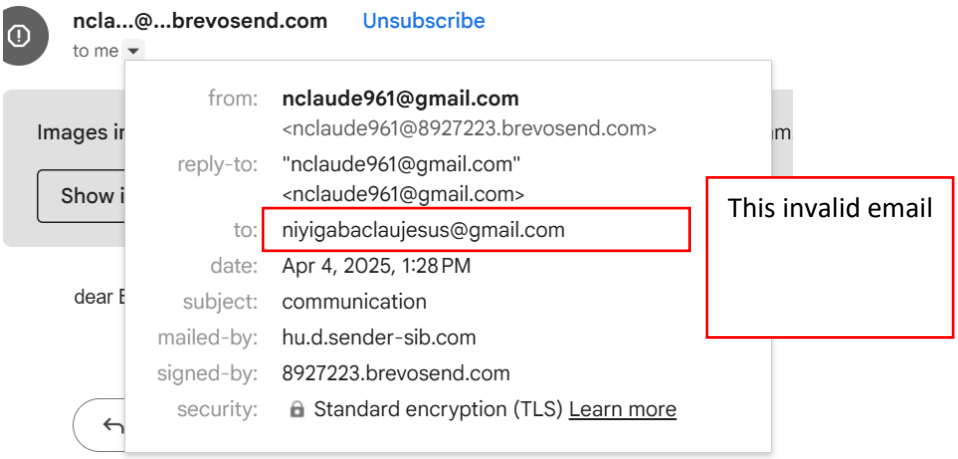
i. Cause of the Attack

The increase in phishing emails targeting RP College's trainner 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 trainer 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 stusents 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: 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.

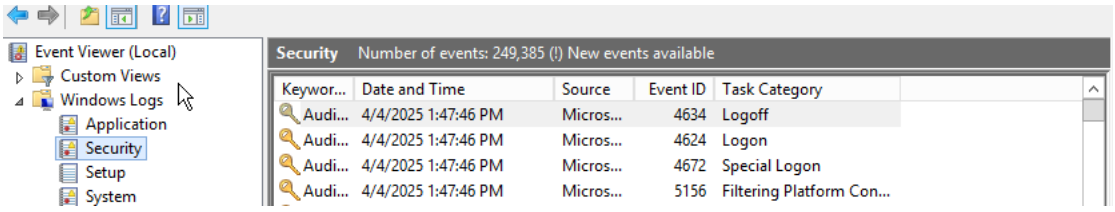
Right click see details

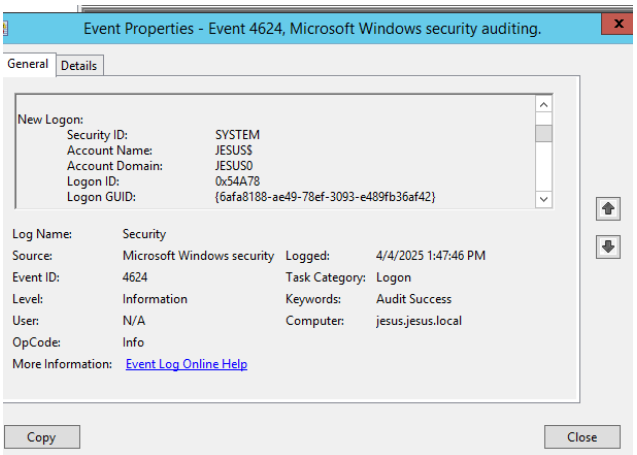


6. The IT security team detects a suspicious login attempt on their core server. This login attempt was made by a user who should not have access to the server

i. Cause of the Attack

The suspicious login attempt on RP 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.





ii. Solution to the Attack

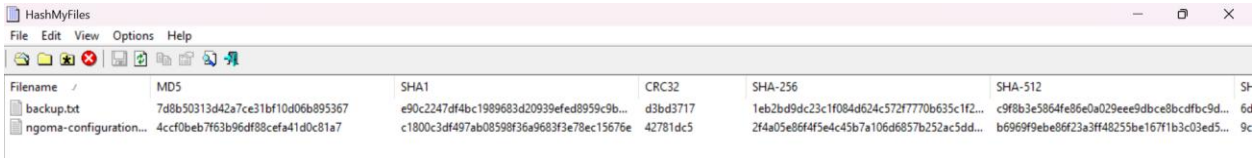
To mitigate this risk, RP College should enforce MFA for all privileged accounts, ensuring that even if credentials are stolen, unauthorized access is blocked. The institution should implement strict access controls, following the Principle of Least Privilege (PoLP), allowing only necessary users to 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.

7. Further, the main company network security admin realized that the routers configurations are being modified by their co-admins without consulting him/her. Using two file backup and ngoma-configuration

Cause of the Issue

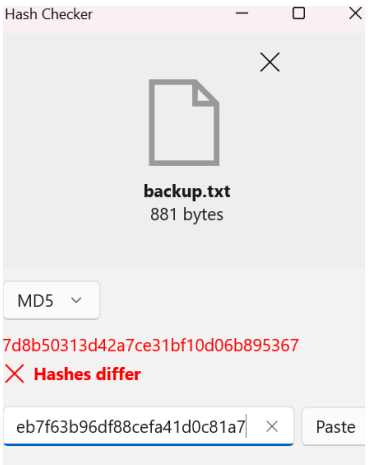
The unauthorized modification of router configurations by co-admins at RP College suggests a lack of proper access control, role-based privileges, and change management policies. Without proper logging and approval mechanisms, multiple administrators may have the ability to alter critical network configurations, 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.

i. Hashingmyfile

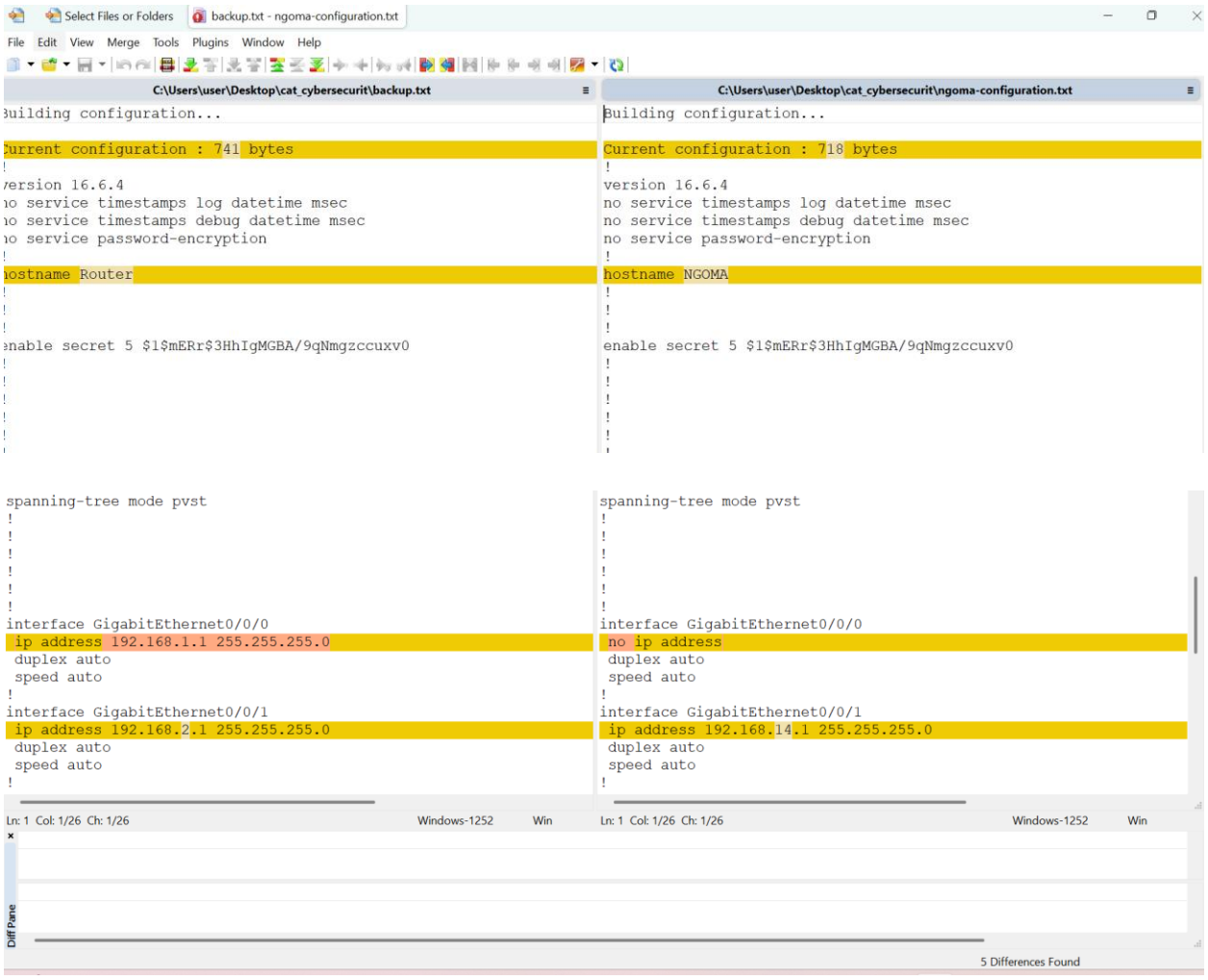


Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SH
backup.txt	7d8b50313d42a7ce31bf10d06b895367	e90c2247df4bc1989683d20939efed8959c9b...	d3bd3717	1eb2bd9dc23c1f084d624c572f7770b635c1f2...	c9f8b3e5864fe86e0a029eee9dbce8bcdfbc9d...	6d
ngoma-configuration...	4ccf0beb7f63b96df88cefa41d0c81a7	c1800c3df497ab08598f36a9683f3e78ec15676e	42781dc5	2f4a05e86f4f5e4c45b7a106d6857b252ac5dd...	b6969f9ebe86f23a3ff48255be167f1b3c03ed5...	9c

ii. Hash checker



iii. Winmerger



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

The system administrator at RP College was alerted by system logs indicating that unauthorized public IP addresses were accessing internal network devices, particularly routers within the 192.168.14.0/24 subnet. This suggests a serious security breach, where attackers from outside the organization are exploiting misconfigured firewall rules, exposed management ports (e.g., Telnet, SSH, HTTP/HTTPS), or weak authentication to access and potentially modify router configurations. Such unauthorized access can lead to routing changes, data redirection, man-in-the-middle attacks, or even full network compromise.

i. Solution to the Issue the Administrator must take immediate action:

i. Harden Router Security:
   a. Disable remote management on routers unless absolutely necessary.
   b. Restrict management access to only trusted IPs inside the 192.168.14.0/24 subnet.
   c. Change default usernames and enforce strong passwords on all network devices.

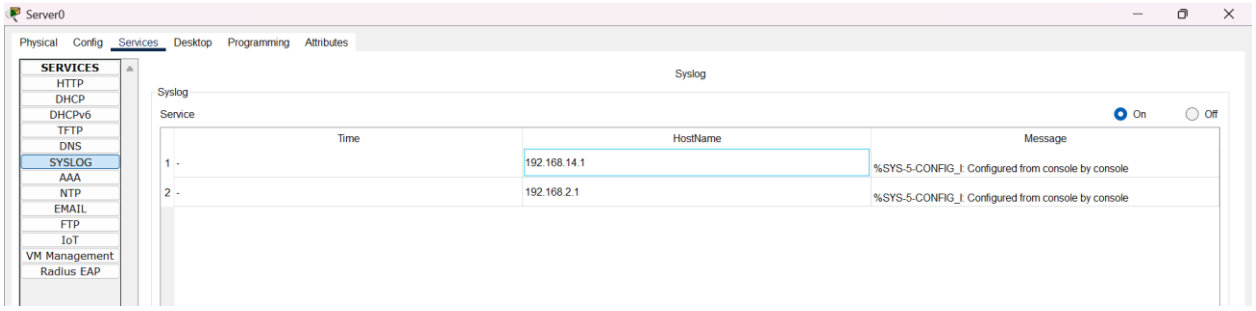
ii. Firewall and Access Control:
   a. Review and harden firewall rules to block all external access to internal devices.
   b. Only allow specific, whitelisted IPs for admin access (if remote access is needed).
   c. Implement Geo-IP blocking to prevent traffic from untrusted or foreign locations.

iii. Deploy IDS/IPS Tools:

   1. Use Snort, Suricata, or pfSense to detect and block intrusion attempts.
   2. Set rules in Snort to detect unauthorized config changes or access to routers on your LAN.

iv. Log Monitoring & Alerting: Set alerts for configuration changes on routers or login attempts from unknown IPs.

v. Audit Router Configs Regularly: Schedule automated backups and diff-checks of router configs to detect changes



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

To address this issue, RP 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 file servers, and 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, to monitor unusual activities, such as large data transfers, unauthorized code downloads, or external sharing. the company should consult legal experts to gather forensic evidence before taking legal action.