

**DEPARTMENT: ICT**

**PROGRAM: INFORMATION TECHNOLOGY**

**RQF LEVEL: 8**

**RQF LEVEL: 8**

**MODULE: CYBERSECURITY**

**Academic: 2024-2025**

**CAT PRATICE**

**Date: 1/04/2025**

**Name: NIYIGABA Claude**

**Reg No: 24RP14647**

**Email: niyigabaclaujesus@gmail.com**

**CHALLENGE**

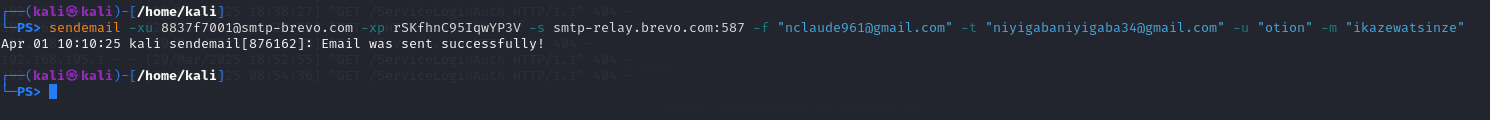
I can see this is a cybersecurity scenario exercise that describes several security issues at RCMU NANZE College and asks you to identify the causes and provide solutions.

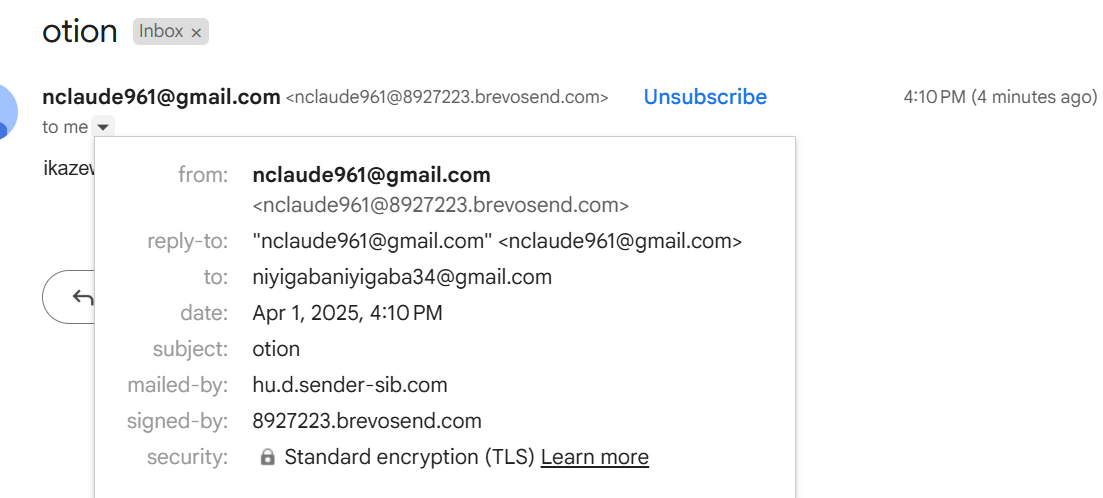
Let me analyze each of the security issues mentioned and suggest appropriate solutions:

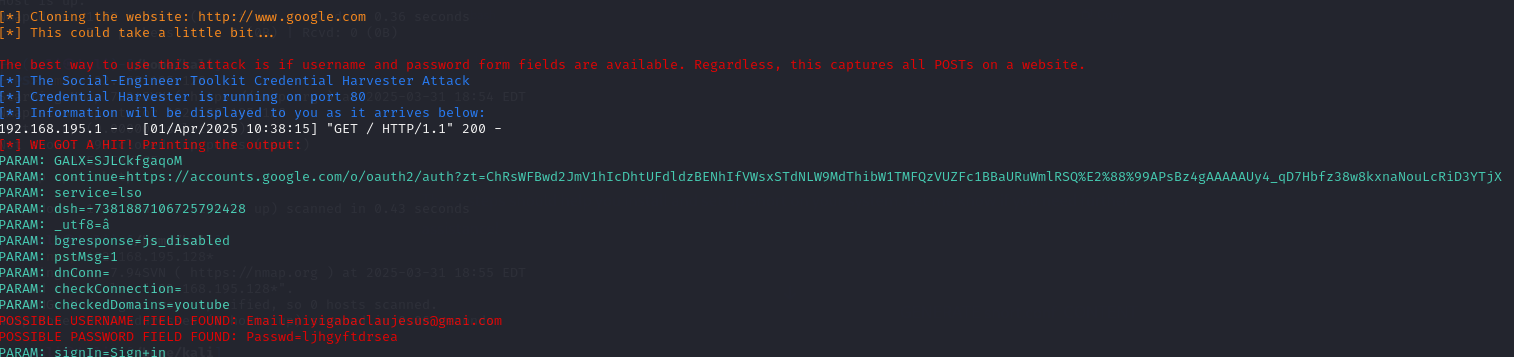
### Analysis of Security Issues

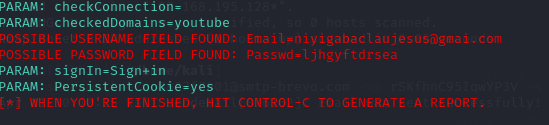
**A. Login Credential Issues**

* **Cause1**: Potential credential theft through phishing, keyloggers, or credential stuffing attacks



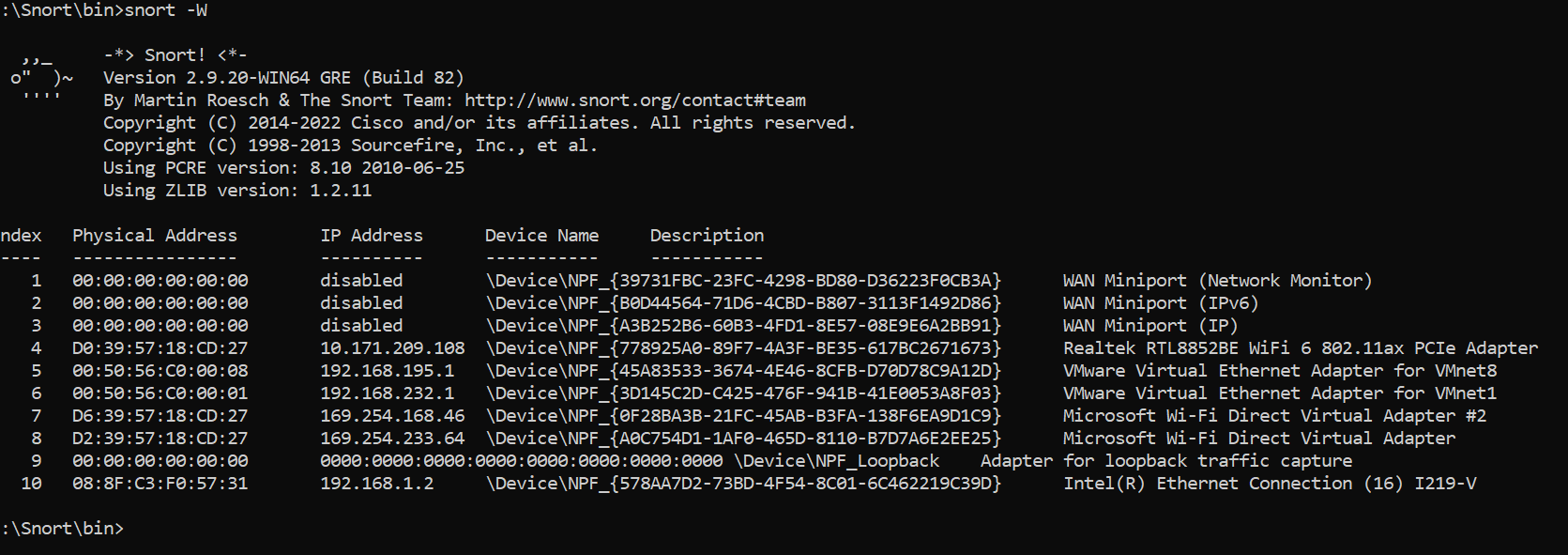


* **Investigation**: Use Wireshark to monitor for suspicious network traffic and check login attempt logs
* **Solution**: Implement multi-factor authentication, regular password changes, and user security awareness training

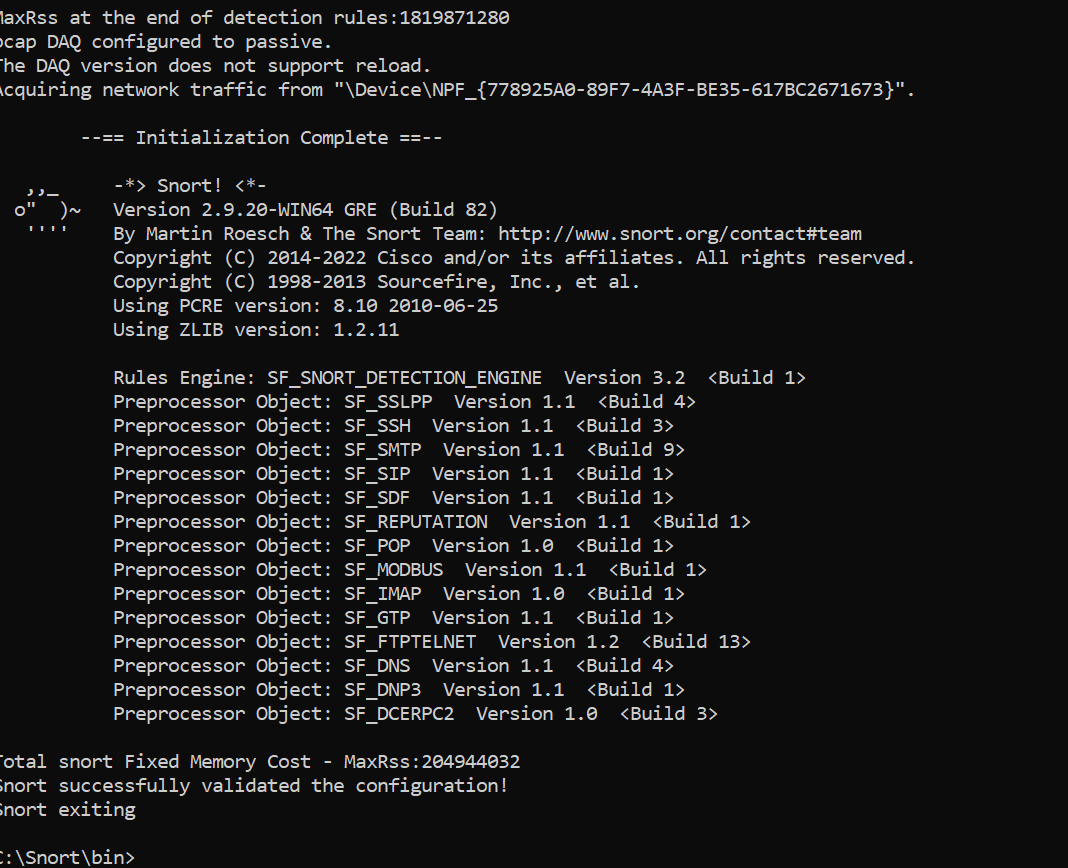


**B. Suspicious Traffic from Foreign IP**

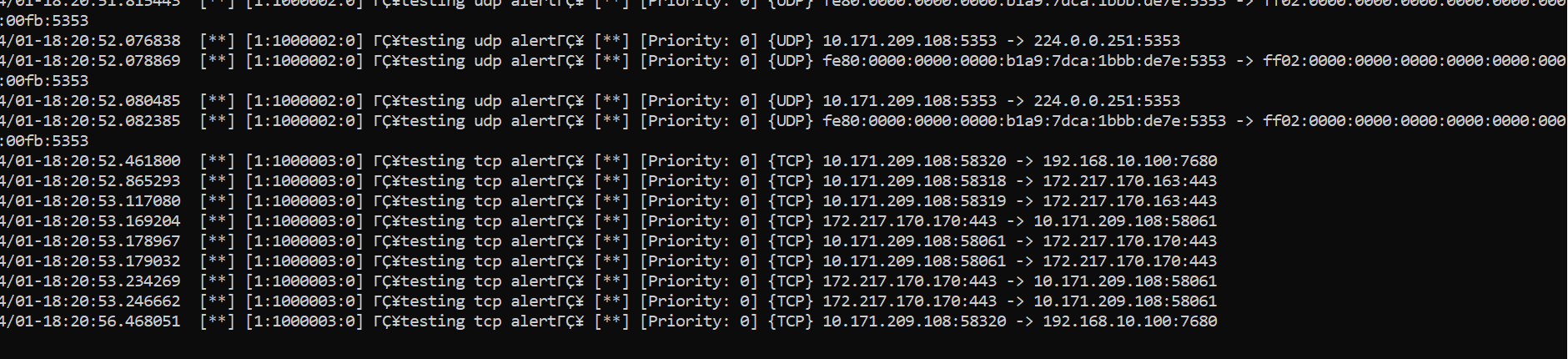
* **Cause**: Potential malicious activity or unauthorized access attempt from external source



* **Investigation**: Use packet tracer and Wireshark to analyze the traffic patterns

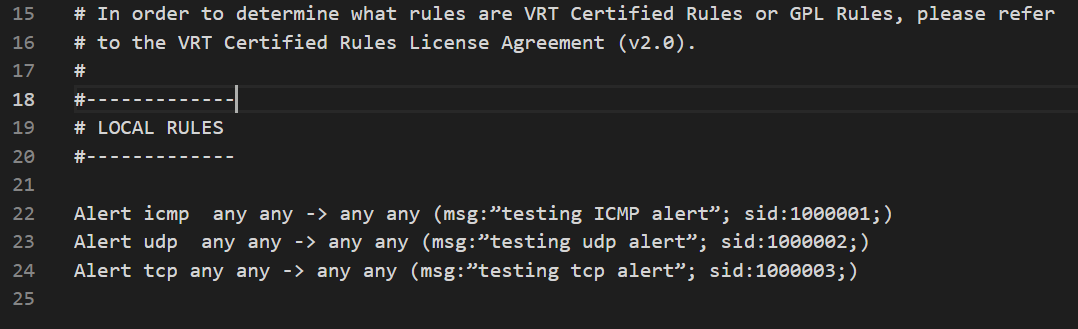


Using this command for :Snort -i 4 -c c:\snort\etc\snort.conf -A console



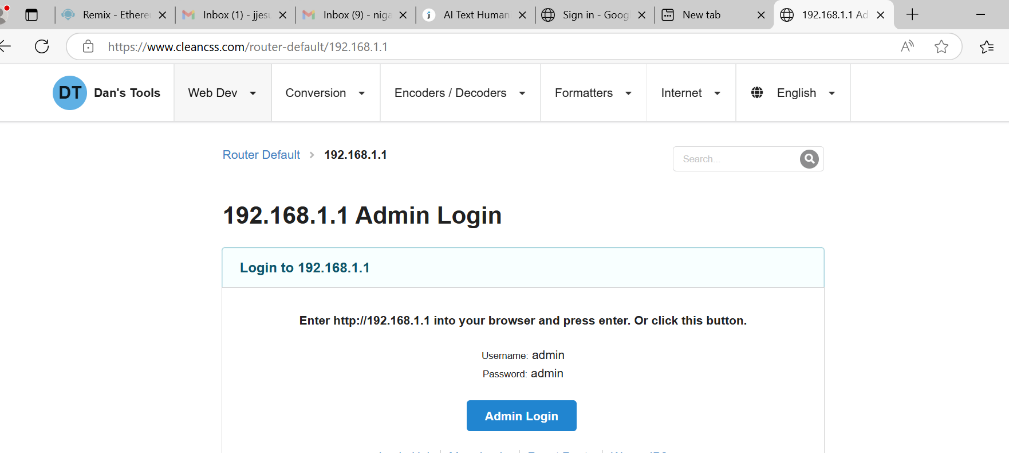
* **Solution**: Configure firewall rules to block suspicious IP ranges, implement geo-blocking if needed

**Using firewall to block this**

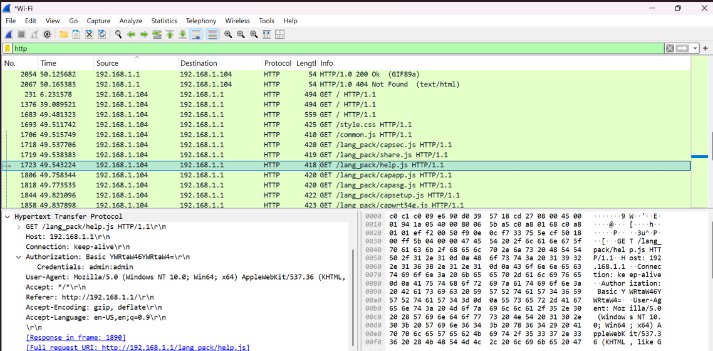


**C. Data Transmission Security Concerns**

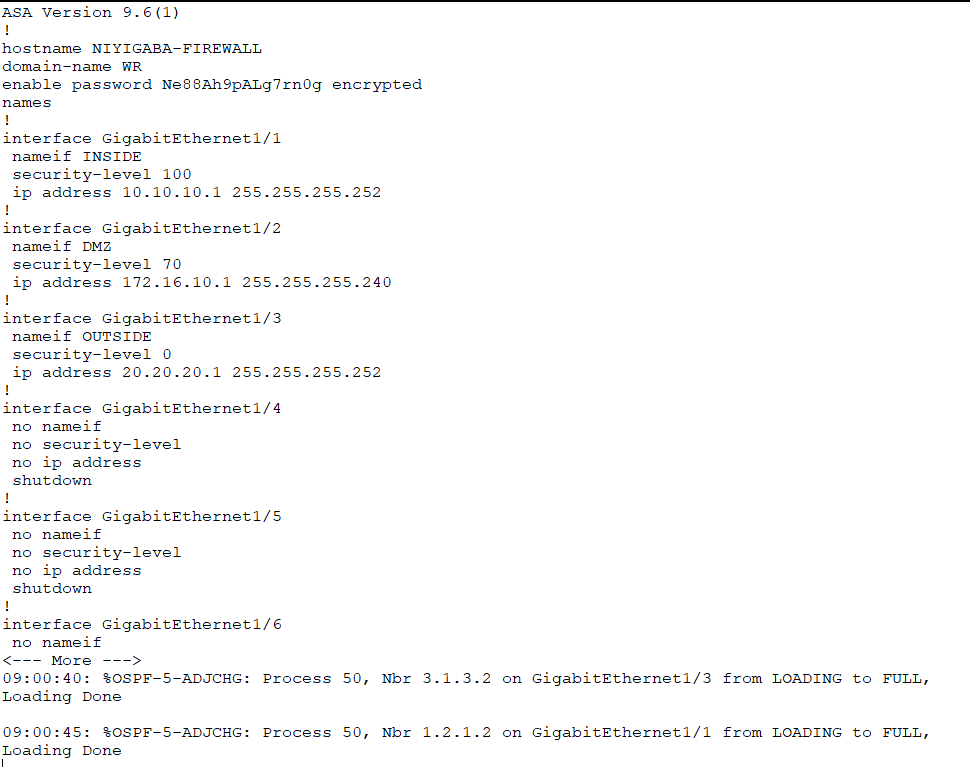
* **Cause**: Lack of encryption for data in transit



* **Investigation**: Use Wireshark to verify if communication is unencrypted

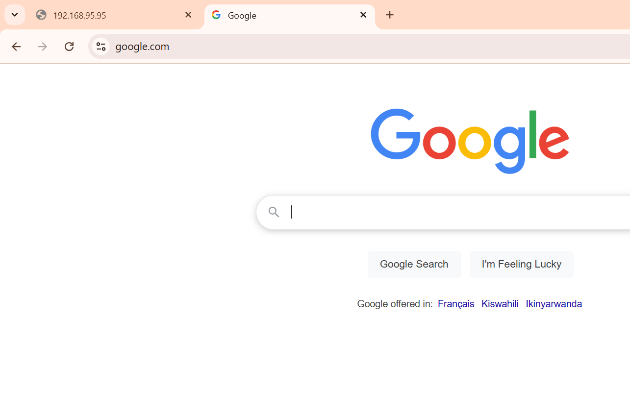
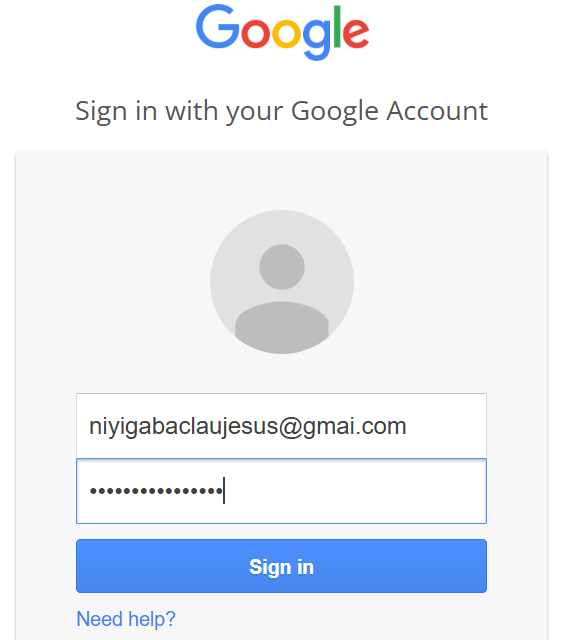
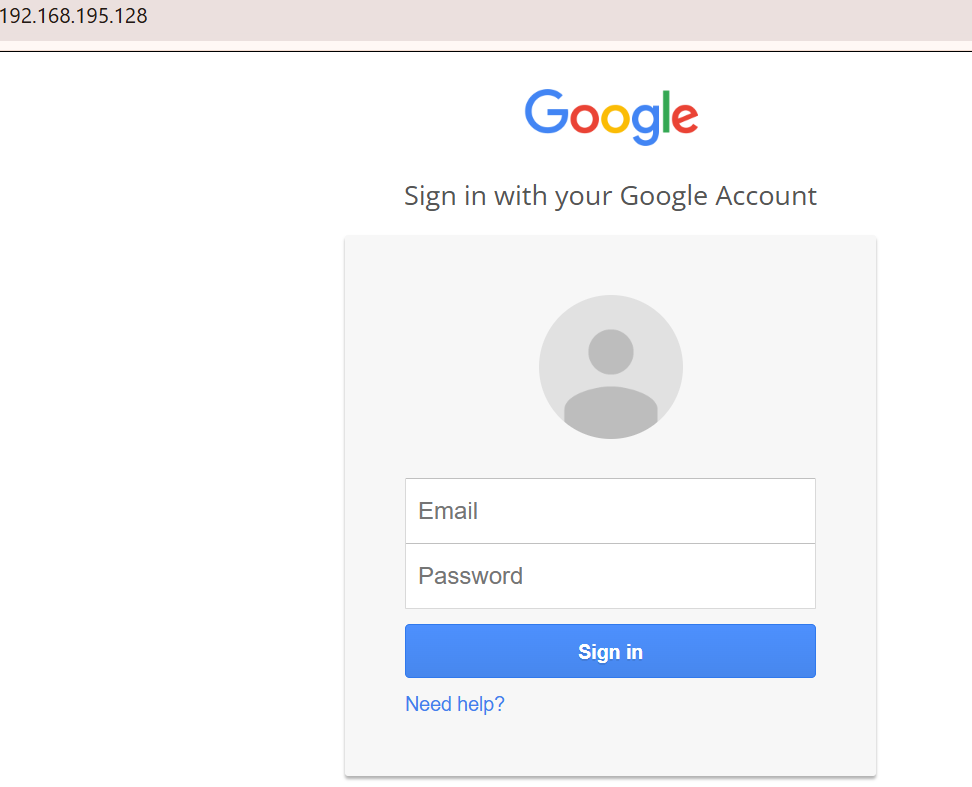


* **Solution**: Implement TLS/SSL for all communications, use VPN for remote office connections



**D. Possible Credential Compromise**

* **Cause**: Successful phishing attacks or social engineering this came from link

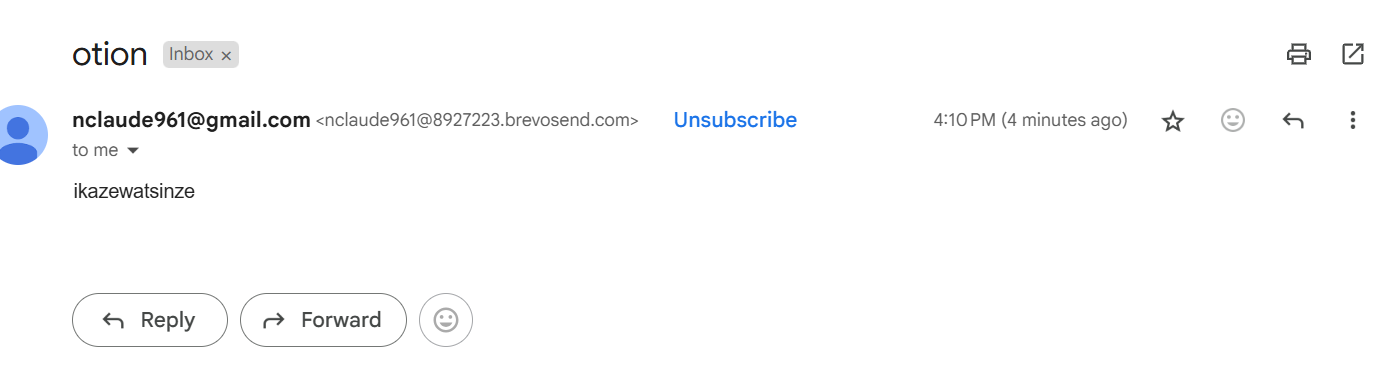


3

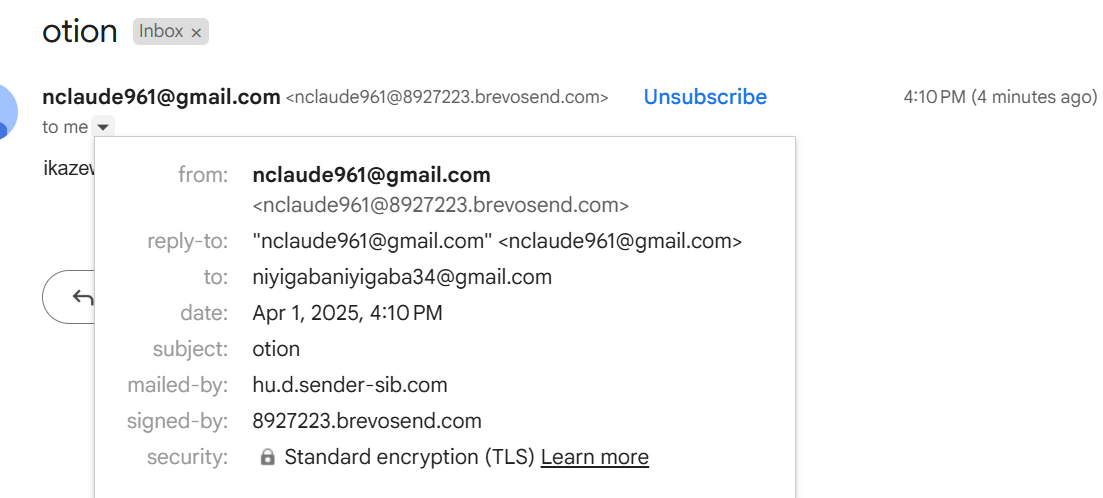
2

1

* **Investigation**: Check email logs and user activity logs



* **Solution**: Reset compromised credentials, implement phishing awareness training, deploy email filtering



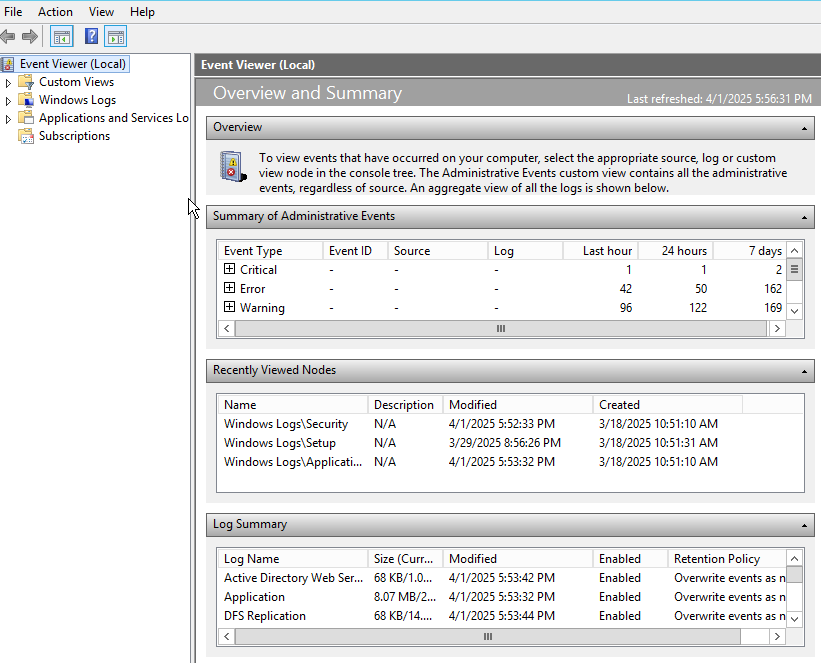
This not trust email

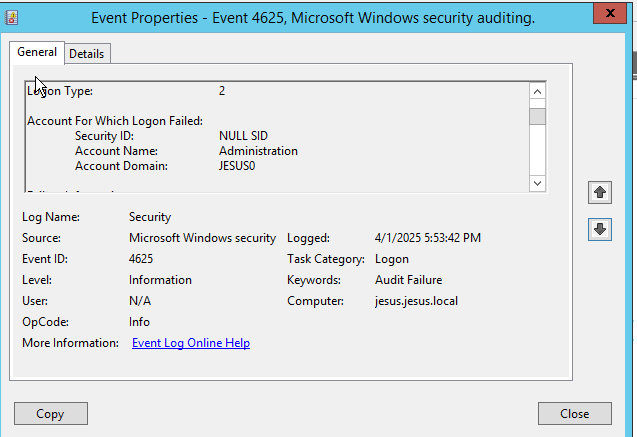
**E. Suspicious Login Attempts**

* **Cause**: Brute force attack or unauthorized access attempt



* **Investigation**: Check server logs for login patterns and source IPs



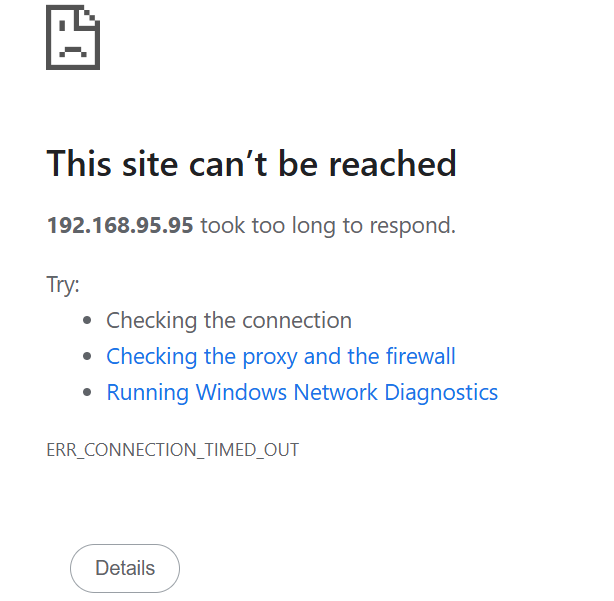


* **Solution**: using strong password



**F. Router Configuration Changes**

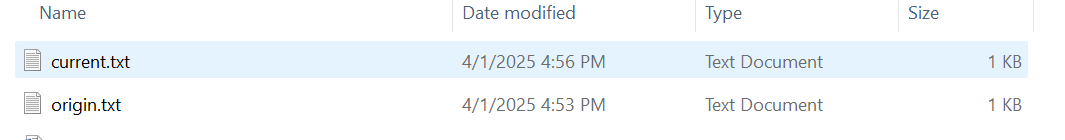
* **Cause**: Insider threat - unauthorized changes by co-admin without consultation



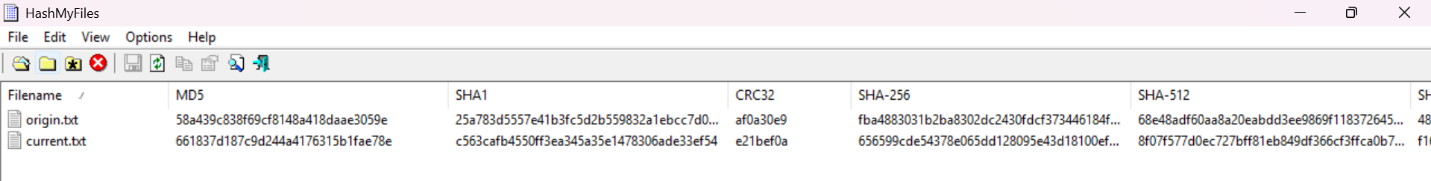
**Change network configuration**

* **Investigation**: Review change logs on network devices

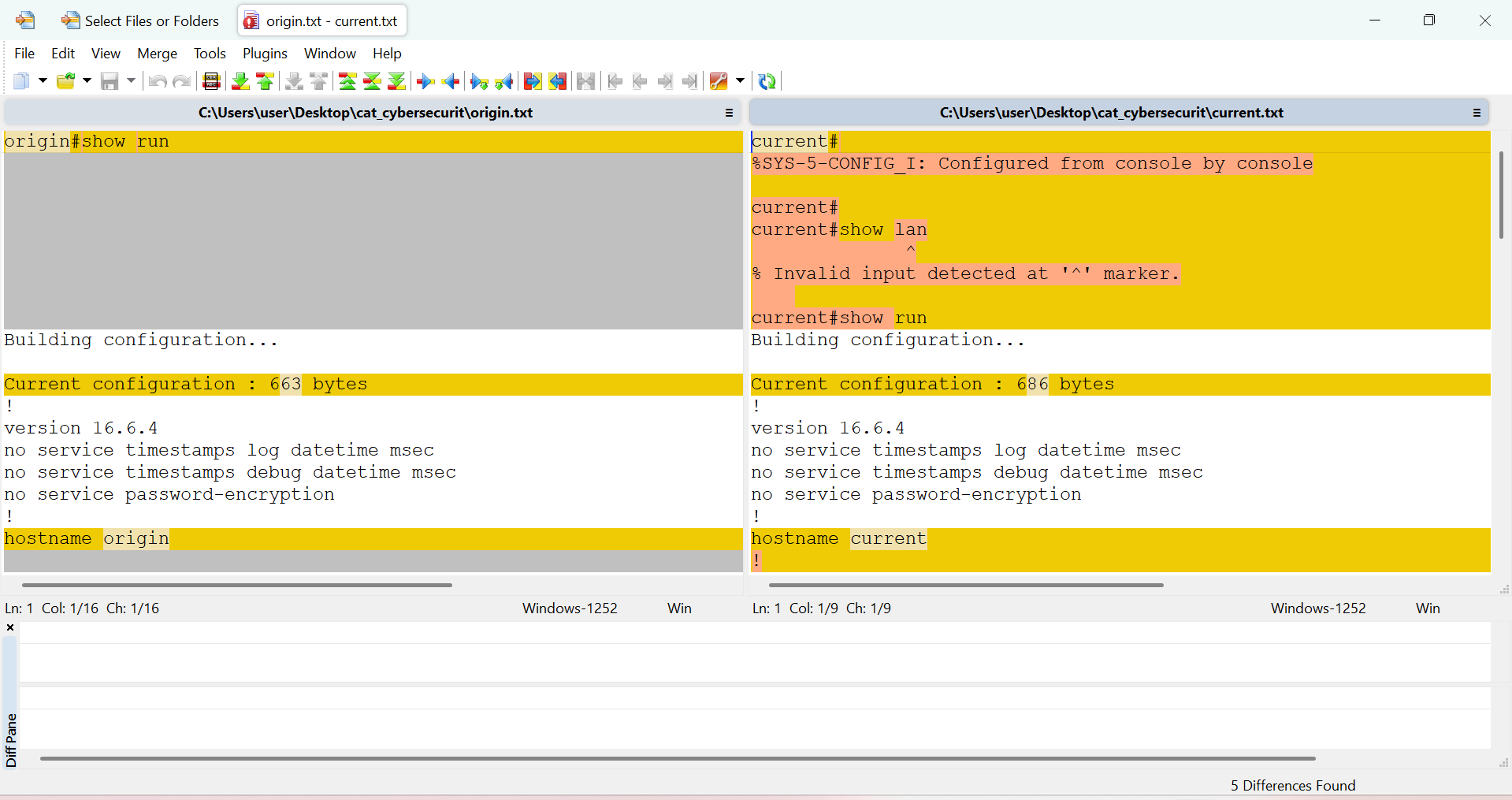
**I take my original script and compare with current script: origin.txt and current.txt**

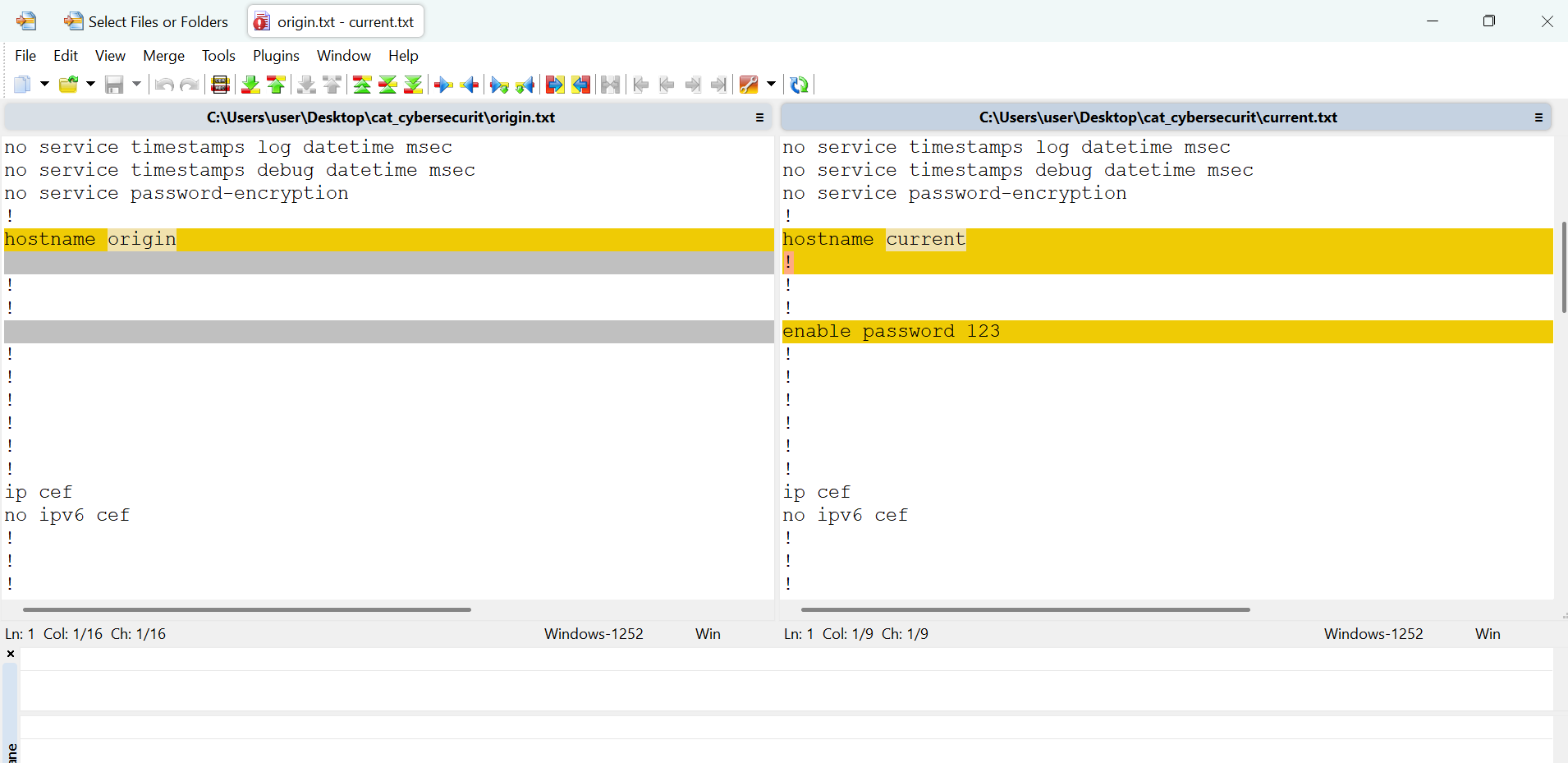


* Using hash my file( origin has different hash with current)

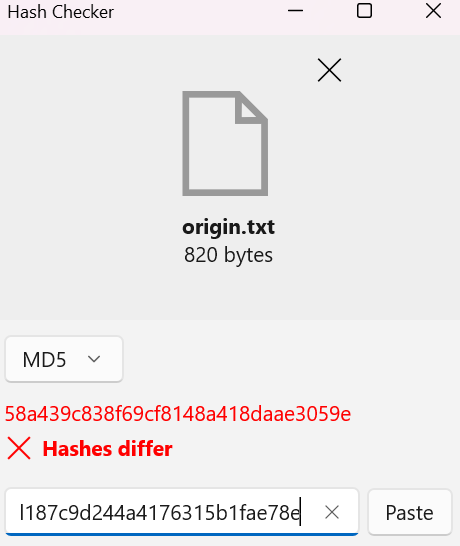


* Using winmerge(origin was modified with current)



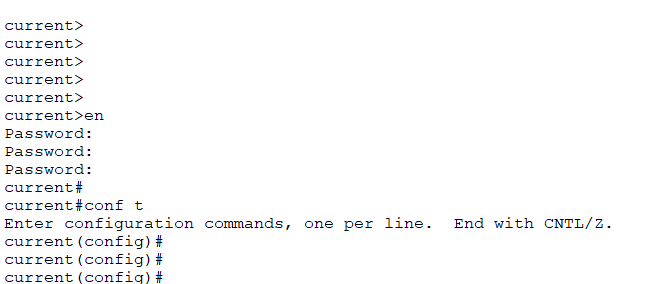


* Using hash checker(compare origin hash and current hash)



Origin has different hash with curent

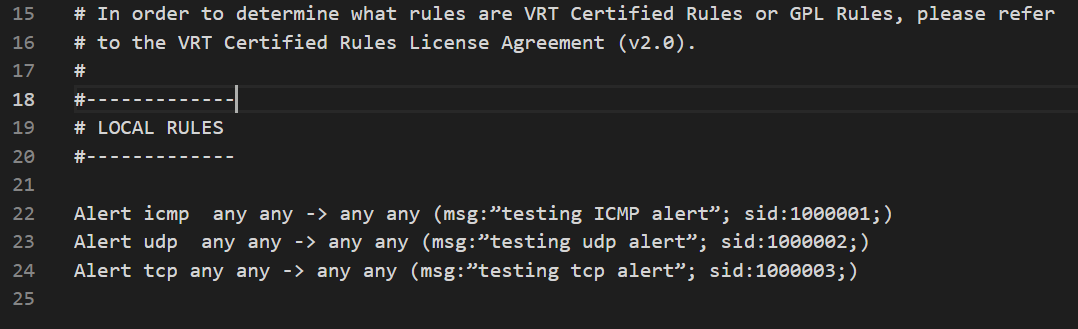
* **Solution**: Implement change management policies, require approval for configuration changes, use TACACS+ for admin authentication



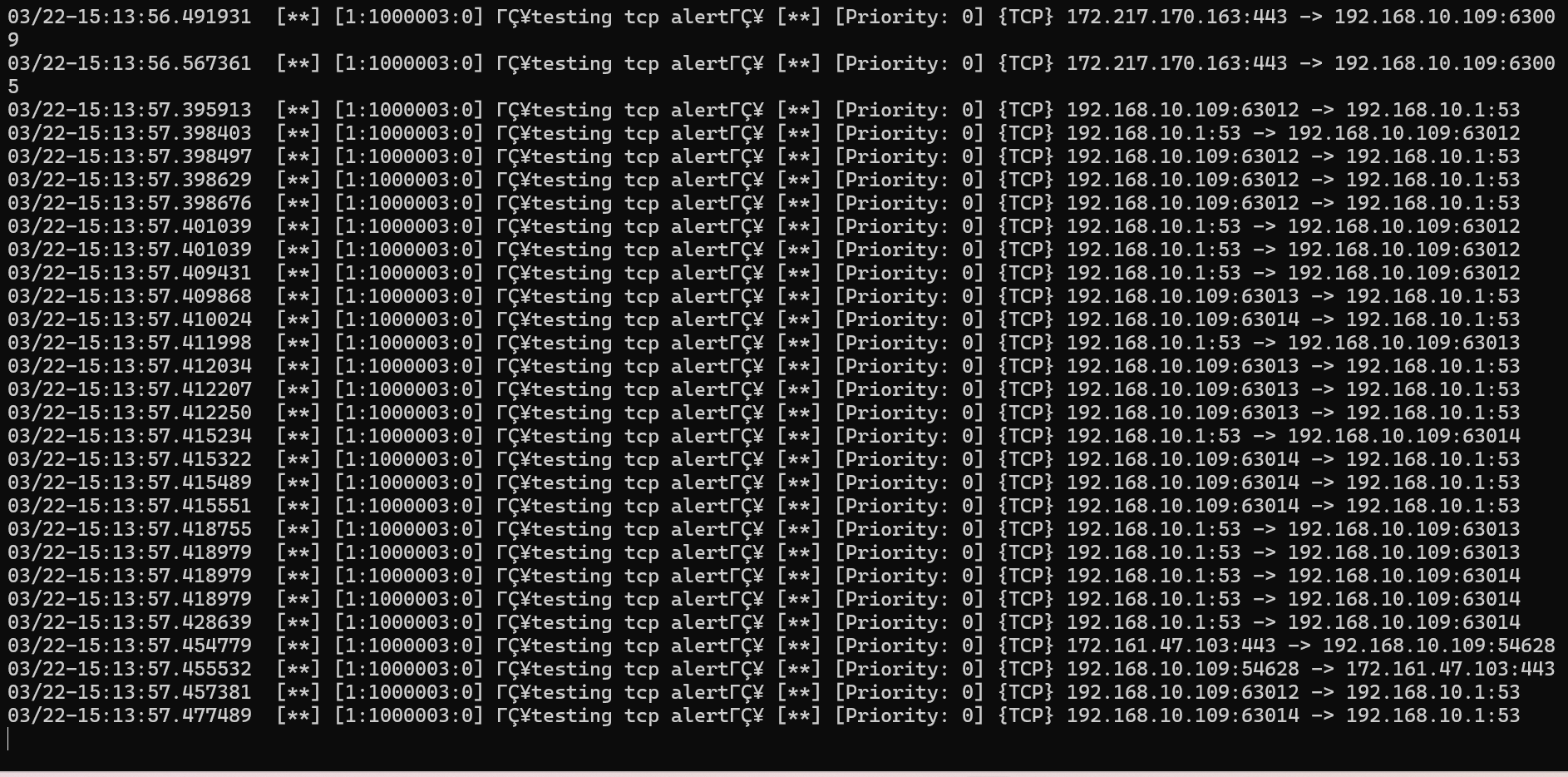
Using strong password

**G. Unauthorized Public IP Access**

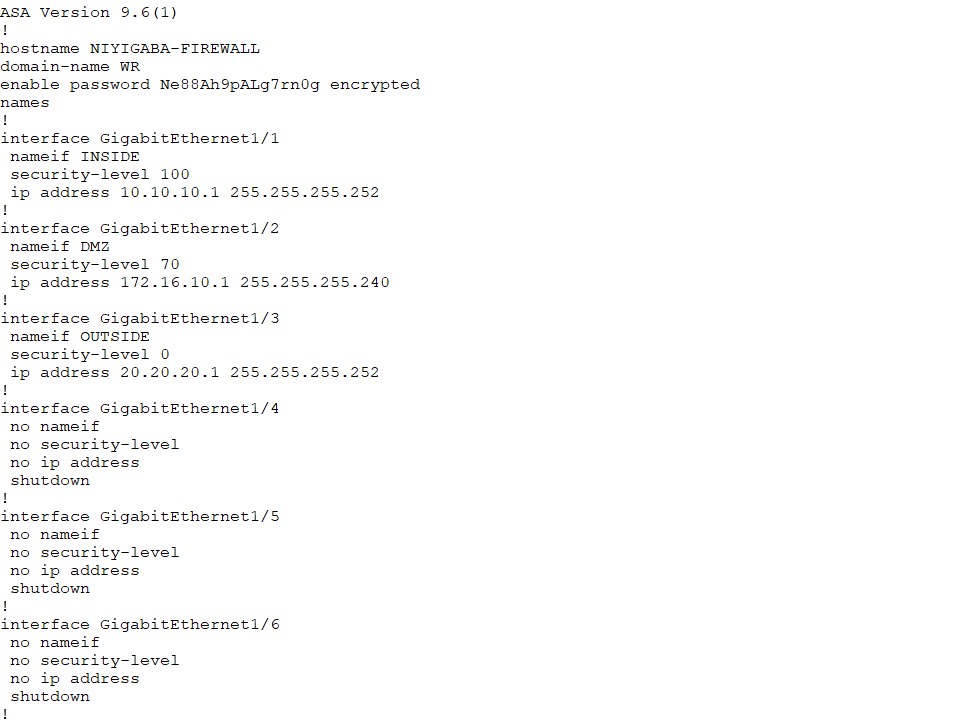
* **Cause**: Misconfigured access controls or firewall rules



* **Investigation**: Review system logs and firewall configurations



* **Solution**: Implement proper network segmentation, review and restrict access control lists



**H. Suspected Data Theft**

* **Cause**: Insider threat - employee stealing proprietary code
* **Investigation**: Monitor employee's network activity, check USB logs, review code repository access logs
* **Solution**: Implement data loss prevention (DLP) system, restrict code access based on need-to-know

### Comprehensive Solution Plan

1. **Immediate Actions**:

* Isolate affected systems
* Block suspicious foreign IP addresses
* Reset compromised credentials
* Preserve logs for forensic analysis

1. **Investigation Phase**:

* Use Wireshark to capture and analyze network traffic
* Review system logs for suspicious activities
* Identify entry points and vulnerabilities
* Document findings and evidence (especially for potential legal action)

1. **Remediation Phase**:

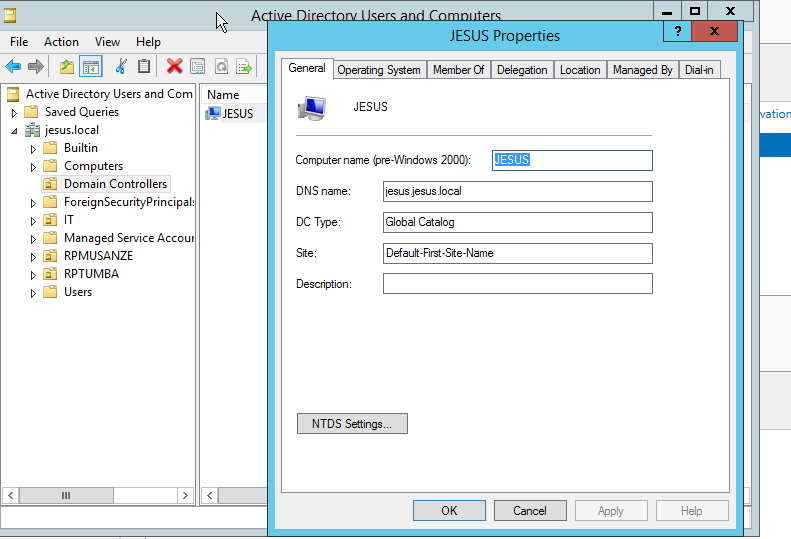
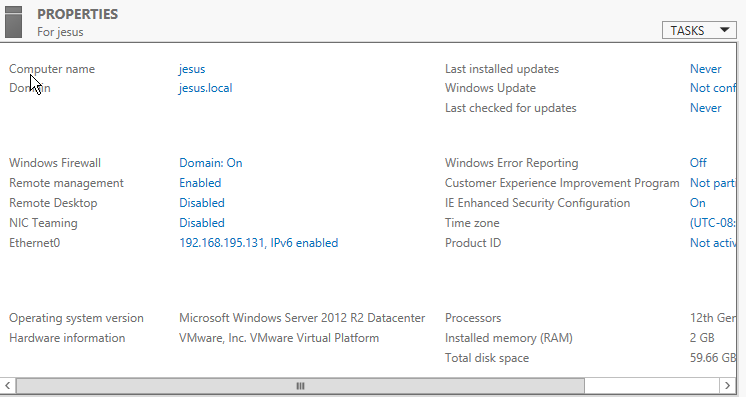
* Implement proper encryption for data transmission
* Configure firewall rules to block unauthorized access
* Patch identified vulnerabilities
* Establish proper authentication mechanisms

1. **Long-term Solutions**:

* Implement regular security awareness training
* Develop and enforce security policies and procedures
* Establish change management processes
* Implement network monitoring and threat detection tools
* Regular security audits and penetration testing

**TASK 1 CREATE DOMAIN CONTROL THAT SHOULD HAVE NAME AND DOMAIL NAME**

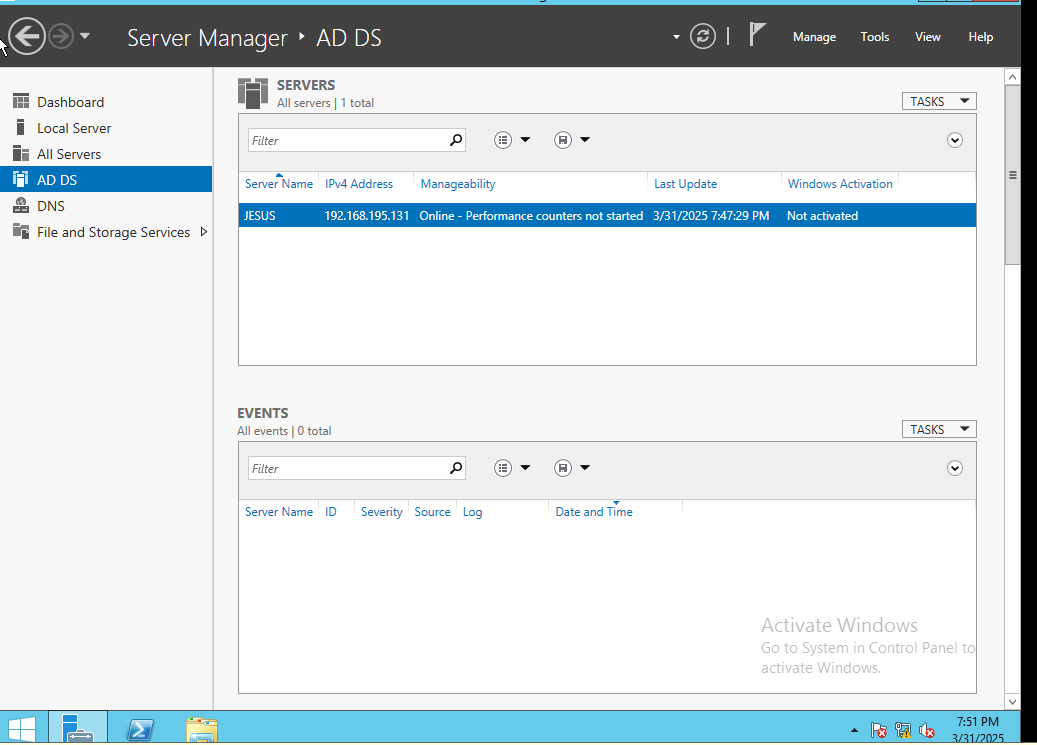
My domain name is jesus.local and computer name is jesus



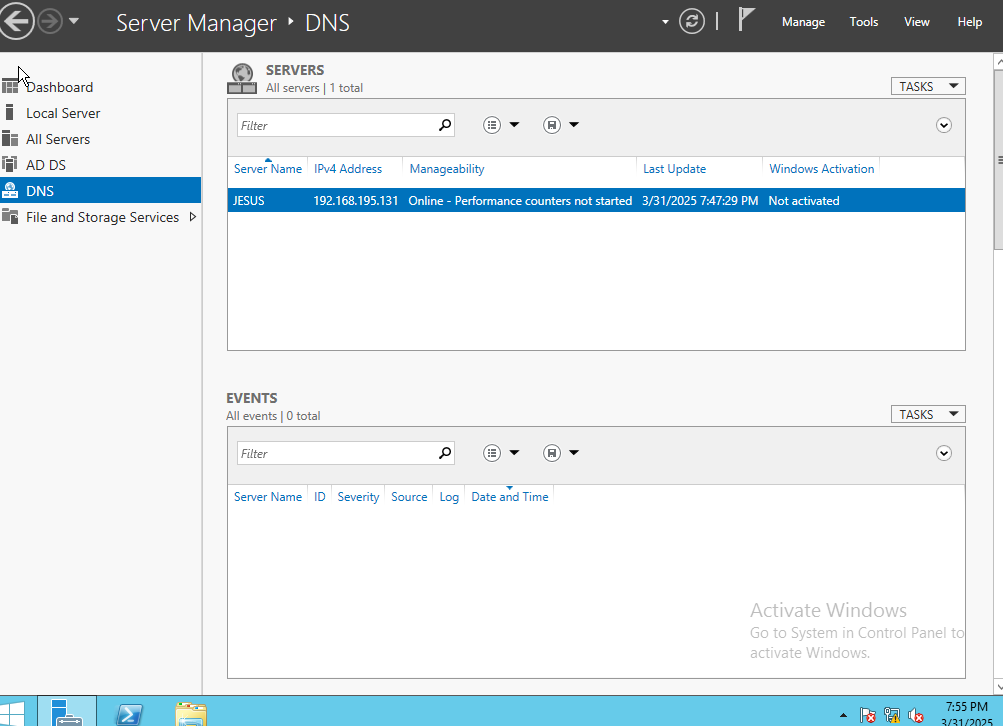
**This is my domain name**

**Task 2 enable the following services: DNS and AD DS**

1. AD DS with server name JESUS and ip address: 192.168.195.131

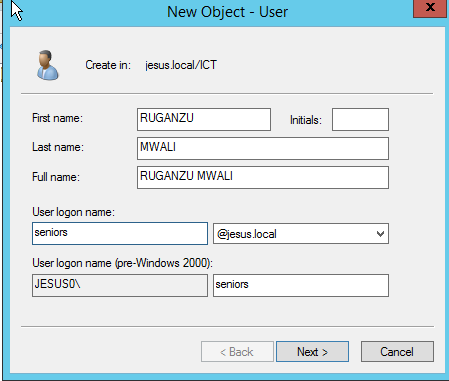
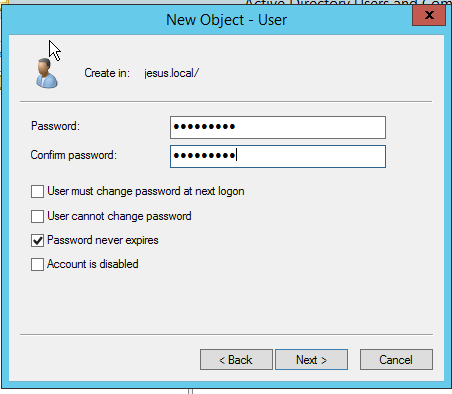
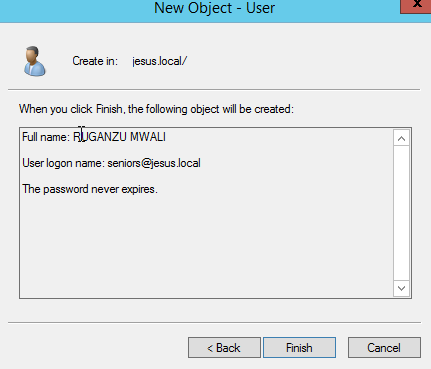


1. DNS server



**Task 3 create grouper of user ICT with add users in progress**

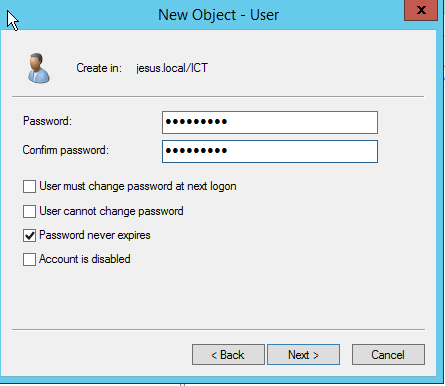
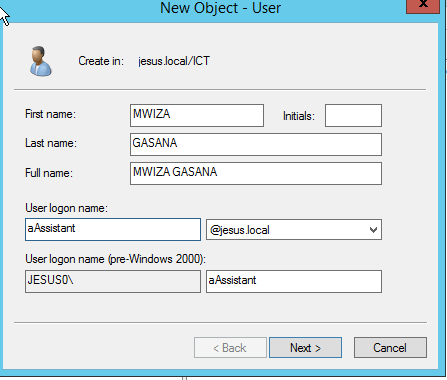
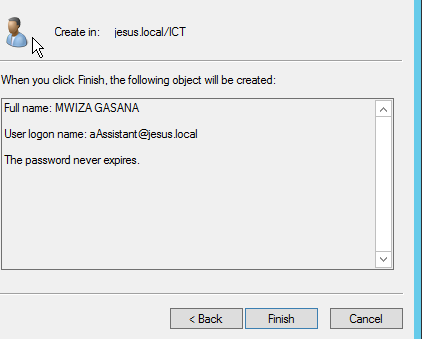
1. Ruganzu mwali user and their roles

Create user senior

Set password

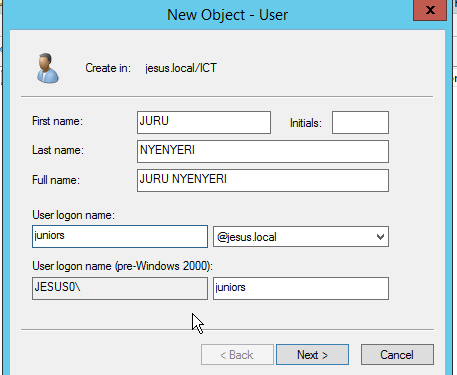
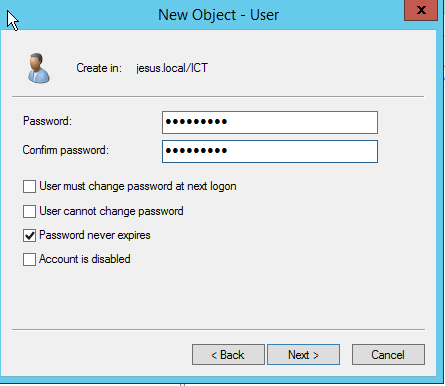
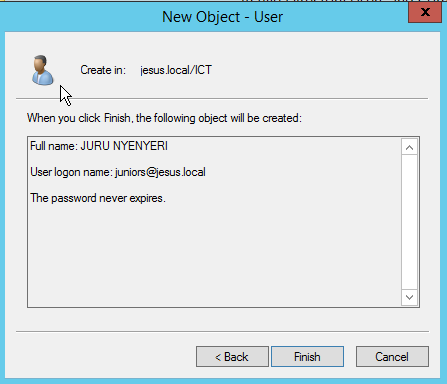
1. Assistant group user and role

Create assistant user

Set password assistant

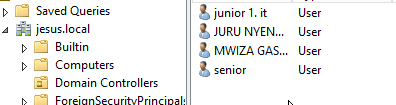
1. Junior group and user juru and their role

Create password junior

Create user junior

**All users**

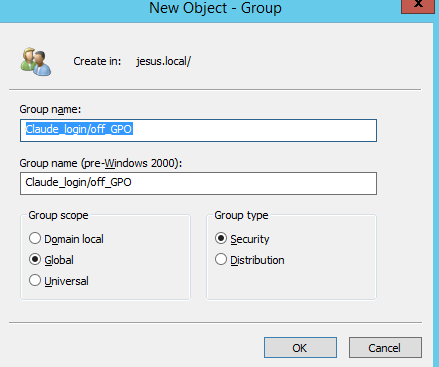


all users

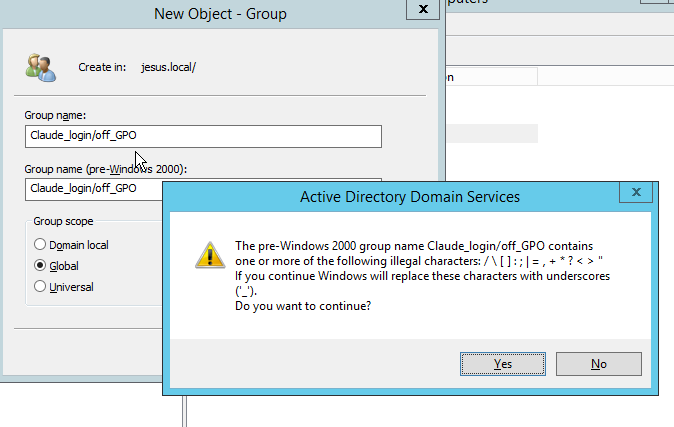
Task 4 create TWO GPO WITH MY LAST NAME

1. Claude\_login/off\_GPO

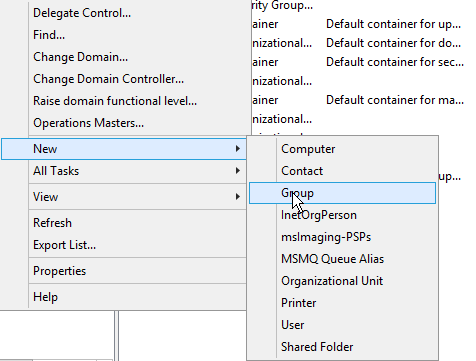
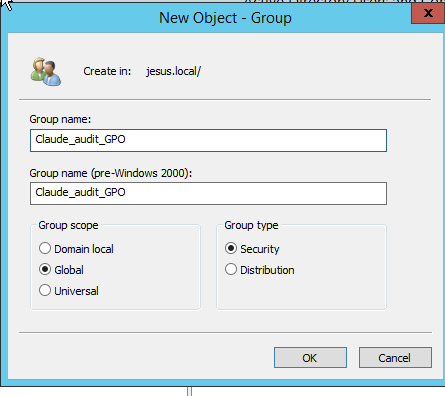
Step 1 select domain name and new open group



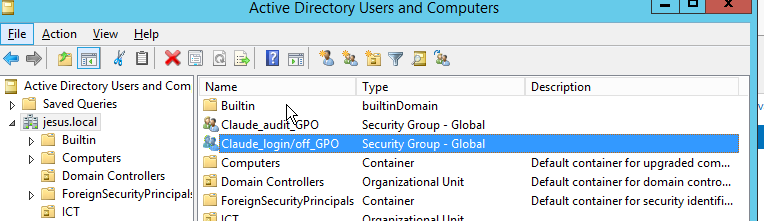
**Step 2 after write group name ok**



1. Claude\_audit\_GPO

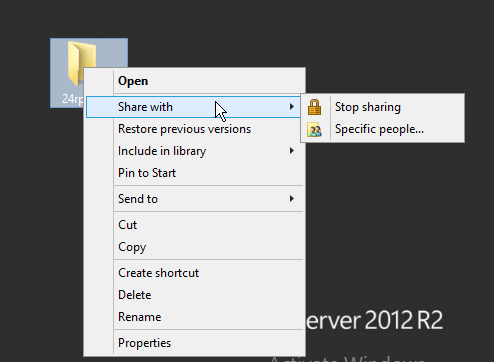
 

All group

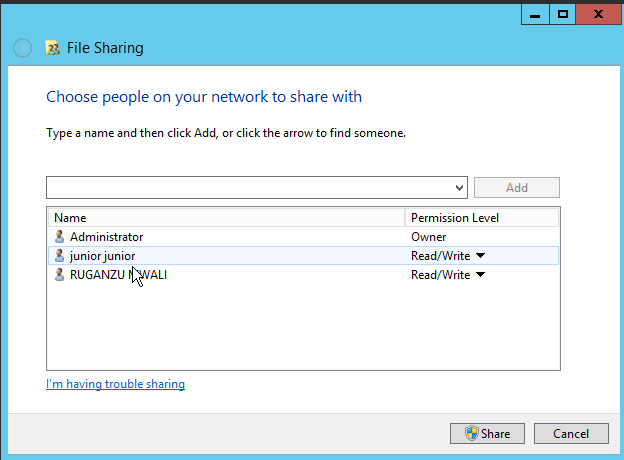


All GPO

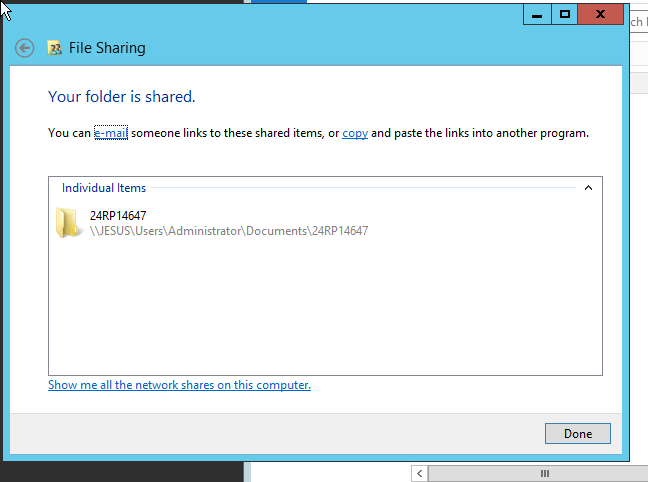
TASK 5 SHARE FOLDER



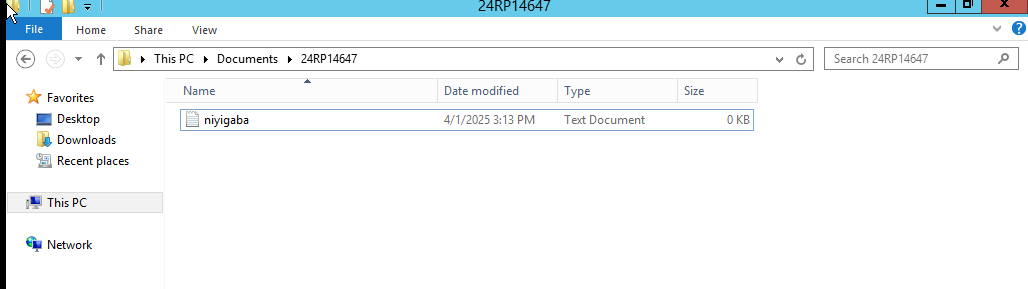
After open specific set access



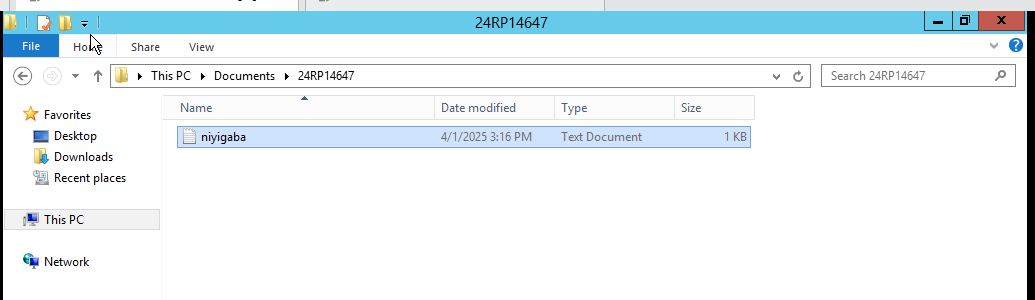
Share



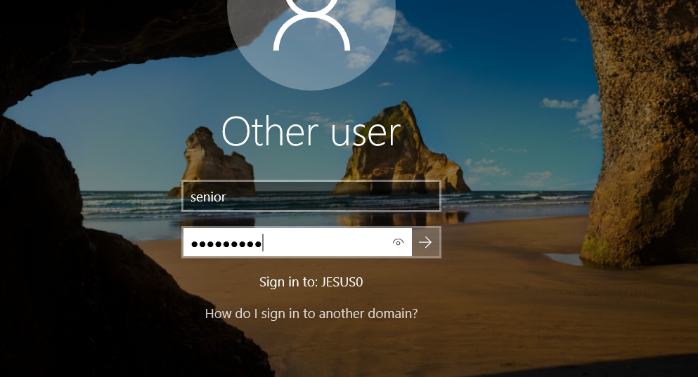
Task 6 creat file and security



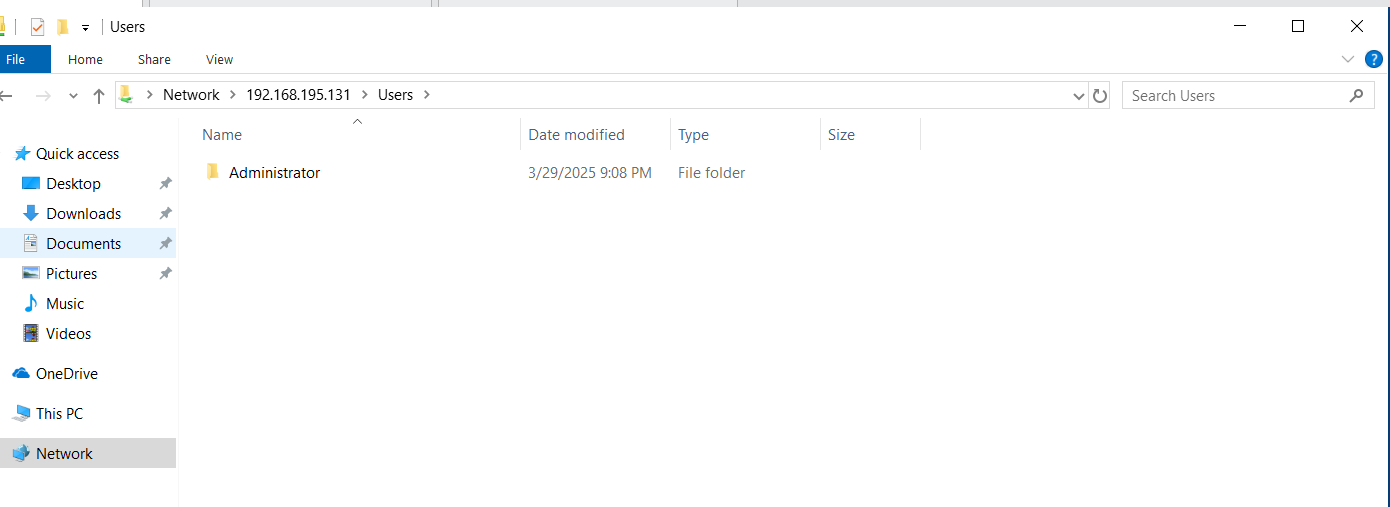
**Then increase size of file**



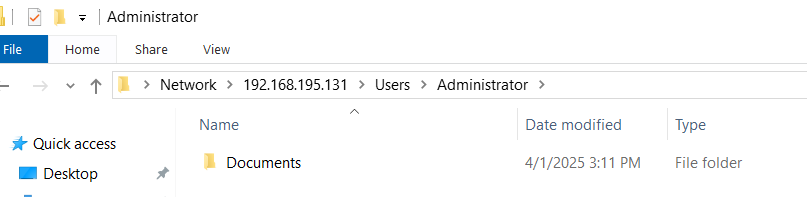
**Then get share using window client**



After login as user from domain name window + r and type server ip get this admin sharing



Then open admin user



This result from sharing

