RWANDA POLYTECHNIC

MUSANZE COLLEGE

DEPARTMENT: ICT

PROGRAM: INFORMATION TECHNOLOGY

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

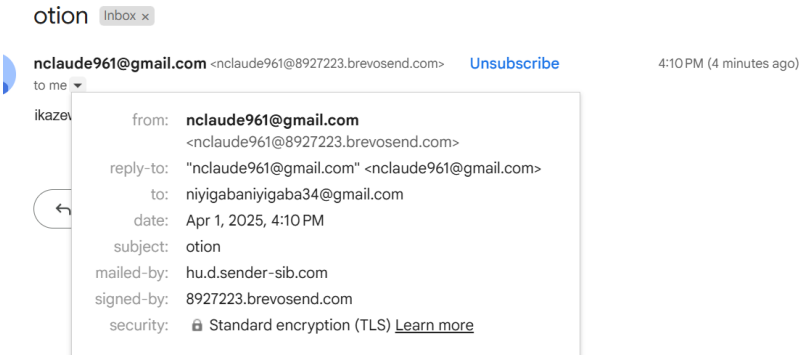
I can see this is a cybersecurity scenario exercise that describes several security issues at RCMU NANZE College and asks you to identify the causes and provide solutions.

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

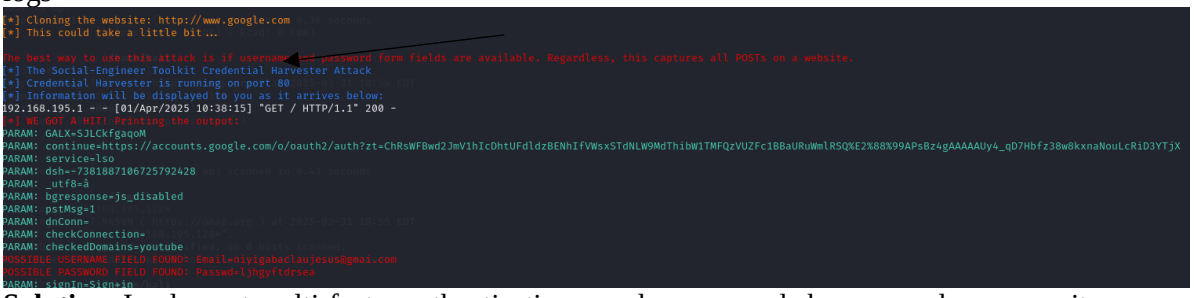
1. Analysis of Security Issues

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

```
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=niyigabaclaujesus@gmai.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=ljhgyftdrsea
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

B. Suspicious Traffic from Foreign IP

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

```
:\Snort\bin>snort -W

  ,,_     -*> Snort! <*-
 o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
  ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using PCRE version: 8.10 2010-06-25
          Using ZLIB version: 1.2.11

ndex   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:27       10.171.209.108  \Device\NPF_{778925A0-89F7-4A3F-BE35-617BC2671673}      Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
   5   00:50:56:C0:00:08       192.168.195.1   \Device\NPF_{45A83533-3674-4E46-8CFB-D70D78C9A12D}      VMware Virtual Ethernet Adapter for VMnet8
   6   00:50:56:C0:00:01       192.168.232.1   \Device\NPF_{3D145C2D-C425-476F-941B-41E0053A8F03}      VMware Virtual Ethernet Adapter for VMnet1
   7   D6:39:57:18:CD:27       169.254.168.46  \Device\NPF_{0F28BA3B-21FC-45AB-B3FA-138F6EA9D1C9}      Microsoft Wi-Fi Direct Virtual Adapter #2
   8   D2:39:57:18:CD:27       169.254.233.64  \Device\NPF_{A0C754D1-1AF0-465D-8110-B7D7A6E2EE25}      Microsoft Wi-Fi Direct Virtual Adapter
   9   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
  10   08:8F:C3:F0:57:31       192.168.1.2     \Device\NPF_{578AA7D2-73BD-4F54-8C01-6C462219C39D}      Intel(R) Ethernet Connection (16) I219-V

:\Snort\bin>
```

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

```
laxRss at the end of detection rules:1819871280
pcap DAQ configured to passive.
he DAQ version does not support reload.
cquiring network traffic from "\Device\NPF_{778925A0-89F7-4A3F-BE35-617BC2671673}".

       --== Initialization Complete ==--

  ,,_     -*> Snort! <*-
 o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
  ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using PCRE version: 8.10 2010-06-25
          Using ZLIB version: 1.2.11

          Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
          Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
          Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
          Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
          Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
          Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

otal snort Fixed Memory Cost - MaxRss:204944032
nort successfully validated the configuration!
nort exiting

:\Snort\bin>
```

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

```
:00fb:5353
4/01-18:20:52.076838  [**] [1:1000002:0] ΓÇ¥testing udp alertΓÇ¥ [**] [Priority: 0] {UDP} 10.171.209.108:5353 -> 224.0.0.251:5353
4/01-18:20:52.078869  [**] [1:1000002:0] ΓÇ¥testing udp alertΓÇ¥ [**] [Priority: 0] {UDP} fe80:0000:0000:0000:b1a9:7dca:1bbb:de7e:5353 -> ff02:0000:0000:0000:0000:0000:000
:00fb:5353
4/01-18:20:52.080485  [**] [1:1000002:0] ΓÇ¥testing udp alertΓÇ¥ [**] [Priority: 0] {UDP} 10.171.209.108:5353 -> 224.0.0.251:5353
4/01-18:20:52.082385  [**] [1:1000002:0] ΓÇ¥testing udp alertΓÇ¥ [**] [Priority: 0] {UDP} fe80:0000:0000:0000:b1a9:7dca:1bbb:de7e:5353 -> ff02:0000:0000:0000:0000:0000:000
:00fb:5353
4/01-18:20:52.461800  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 10.171.209.108:58320 -> 192.168.10.100:7680
4/01-18:20:52.865293  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 10.171.209.108:58318 -> 172.217.170.163:443
4/01-18:20:53.117080  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 10.171.209.108:58319 -> 172.217.170.163:443
4/01-18:20:53.169204  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.170:443 -> 10.171.209.108:58061
4/01-18:20:53.178967  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 10.171.209.108:58061 -> 172.217.170.170:443
4/01-18:20:53.179032  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 10.171.209.108:58061 -> 172.217.170.170:443
4/01-18:20:53.234269  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.170:443 -> 10.171.209.108:58061
4/01-18:20:53.246662  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.170:443 -> 10.171.209.108:58061
4/01-18:20:56.468051  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 10.171.209.108:58320 -> 192.168.10.100:7680
```

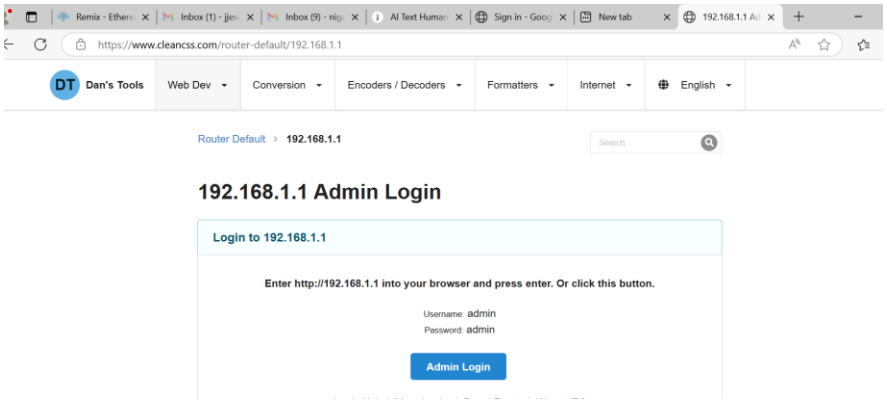
- **Solution**: Configure firewall rules to block suspicious IP ranges, implement geo-blocking if needed

Using firewall to block this

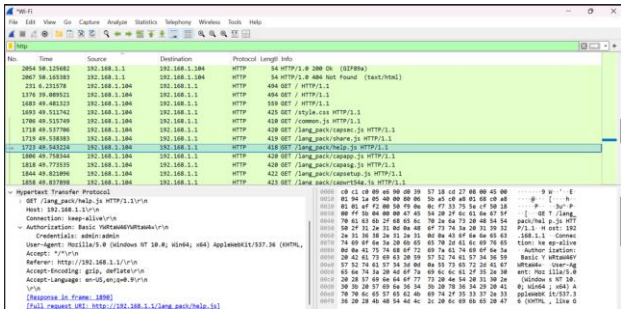
```
15  # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16  # to the VRT Certified Rules License Agreement (v2.0).
17  #
18  #-------------
19  # LOCAL RULES
20  #-------------
21
22  Alert icmp  any any -> any any (msg:"testing ICMP alert"; sid:1000001;)
23  Alert udp  any any -> any any (msg:"testing udp alert"; sid:1000002;)
24  Alert tcp any any -> any any (msg:"testing tcp alert"; sid:1000003;)
25
```

C. Data Transmission Security Concerns

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



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

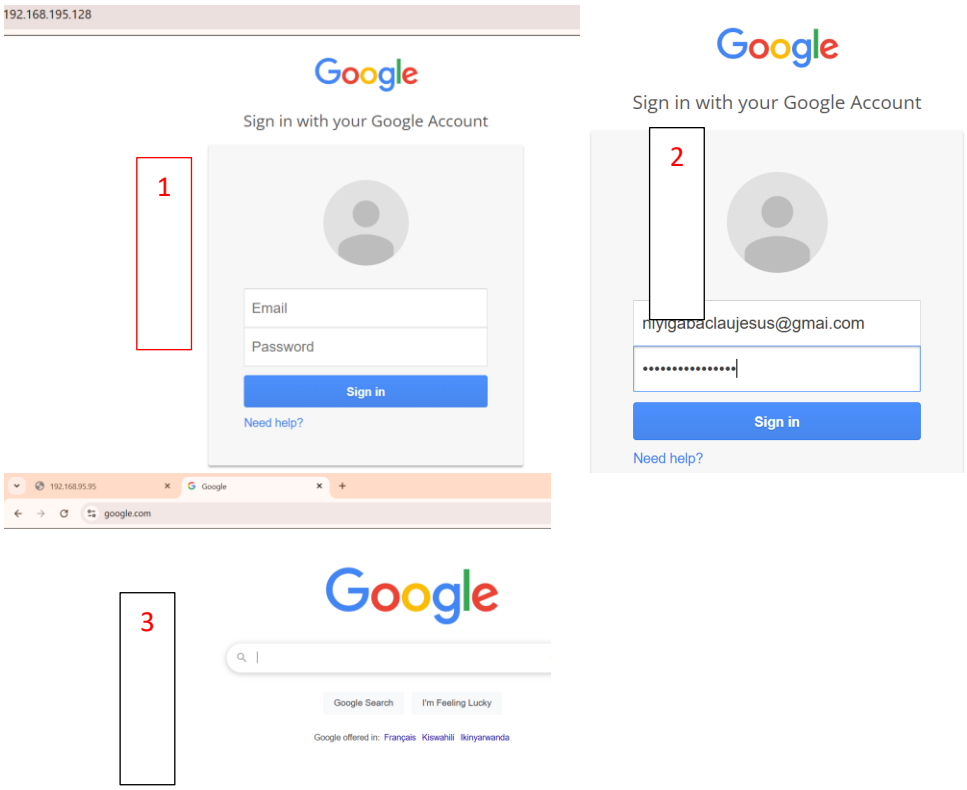


- **Solution**: Implement TLS/SSL for all communications, use VPN for remote office connections

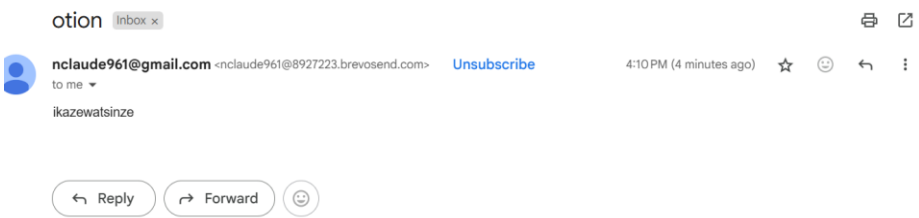
```
ASA Version 9.6(1)
!
hostname NIYIGABA-FIREWALL
domain-name WR
enable password Ne88Ah9pALg7rn0g encrypted
names
!
interface GigabitEthernet1/1
 nameif INSIDE
 security-level 100
 ip address 10.10.10.1 255.255.255.252
!
interface GigabitEthernet1/2
 nameif DMZ
 security-level 70
 ip address 172.16.10.1 255.255.255.240
!
interface GigabitEthernet1/3
 nameif OUTSIDE
 security-level 0
 ip address 20.20.20.1 255.255.255.252
!
interface GigabitEthernet1/4
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no nameif
<--- More --->
09:00:40: %OSPF-5-ADJCHG: Process 50, Nbr 3.1.3.2 on GigabitEthernet1/3 from LOADING to FULL,
Loading Done

09:00:45: %OSPF-5-ADJCHG: Process 50, Nbr 1.2.1.2 on GigabitEthernet1/1 from LOADING to FULL,
Loading Done
```

D. Possible Credential Compromise

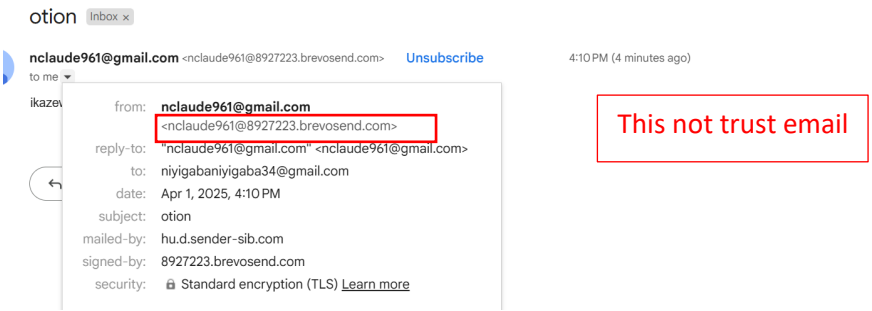
- **Cause**: Successful phishing attacks or social engineering this came from link



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

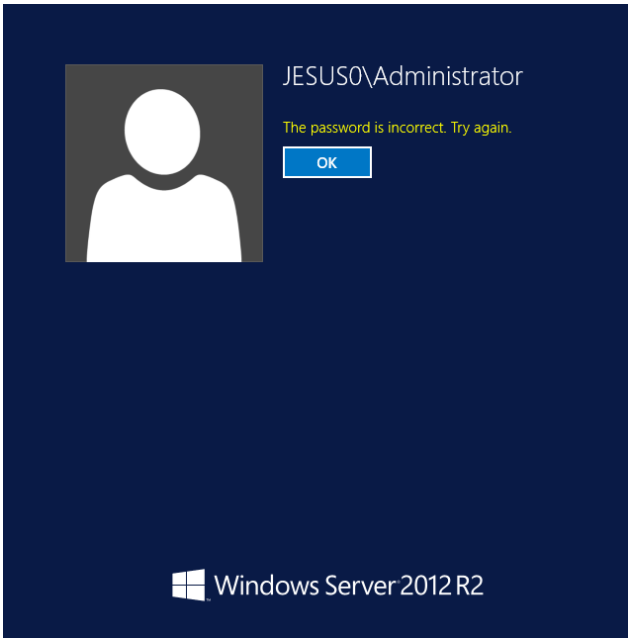


- **Solution**: Reset compromised credentials, implement phishing awareness training, deploy email filtering

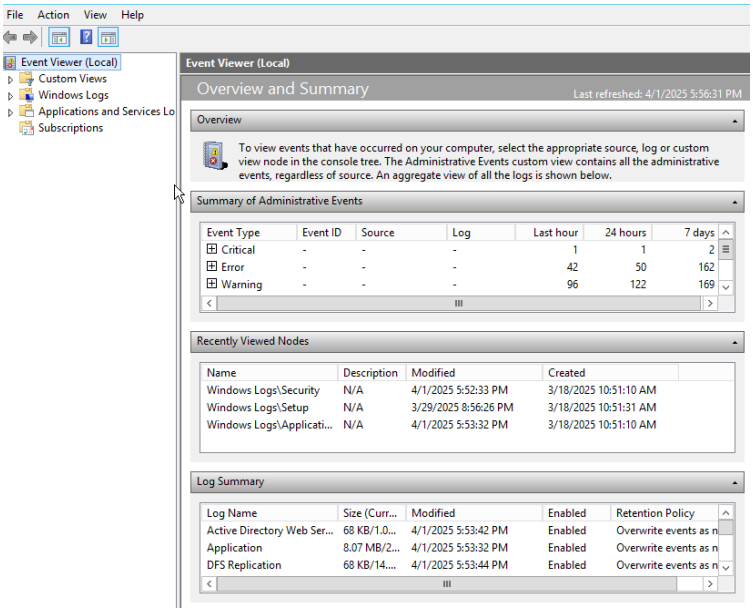


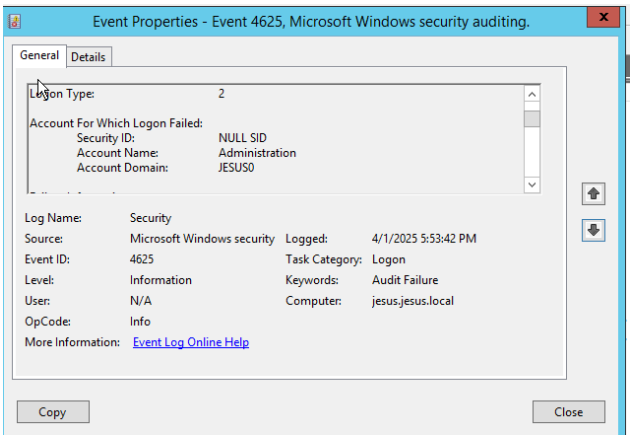
E. Suspicious Login Attempts

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

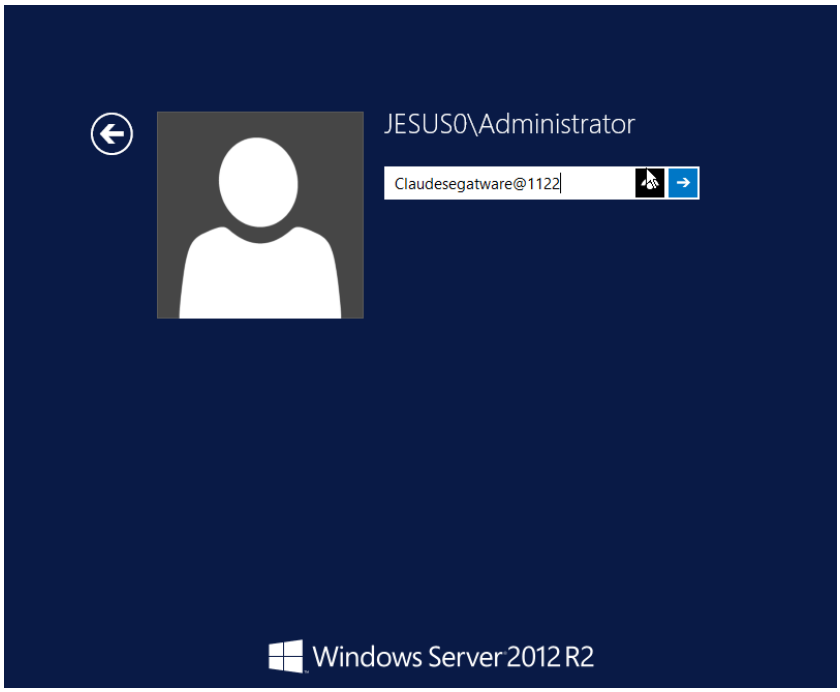


- **Investigation**: Check server logs for login patterns and source IPs





- **Solution**: using strong password



F. Router Configuration Changes

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

Change network configuration

This site can't be reached

192.168.95.95 took too long to respond.

Try:

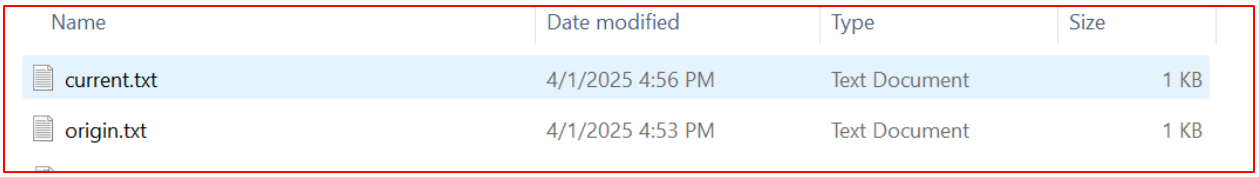
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Details

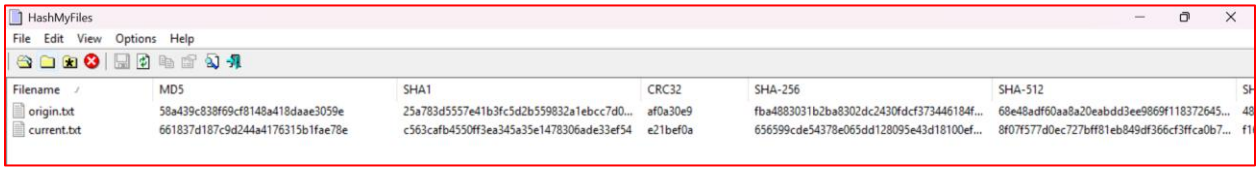
- **Investigation**: Review change logs on network devices

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

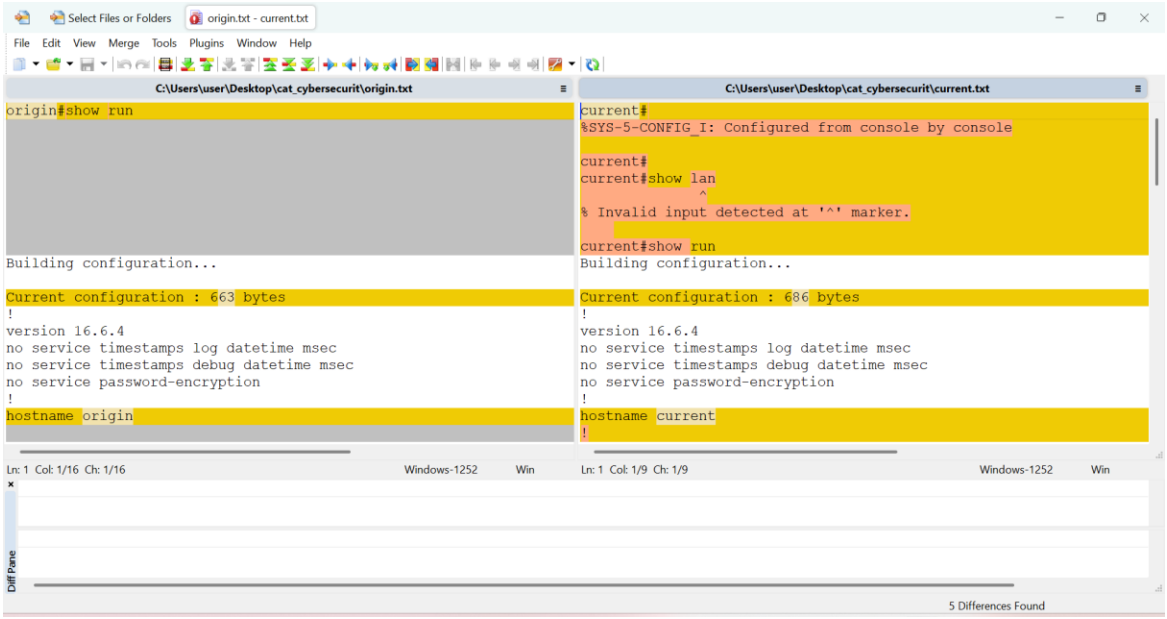


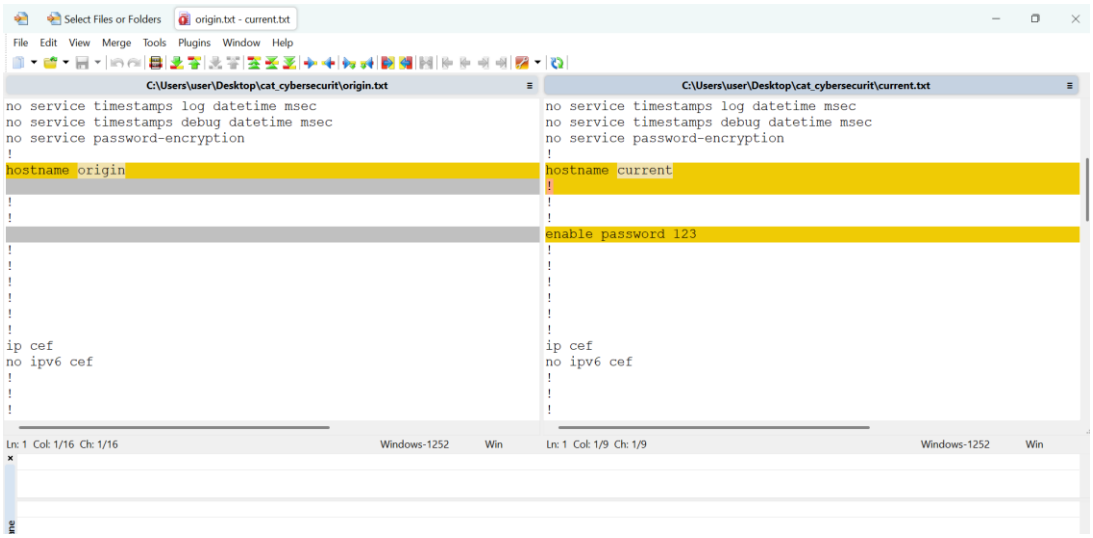
Name	Date modified	Type	Size
current.txt	4/1/2025 4:56 PM	Text Document	1 KB
origin.txt	4/1/2025 4:53 PM	Text Document	1 KB

  - ❖ Using hash my file(origin has different hash with current)

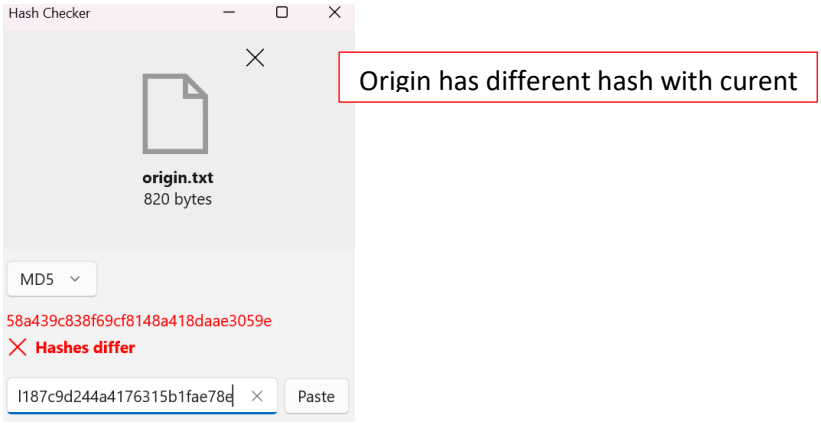


  - ❖ Using winmerge(origin was modified with current)





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



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

```
current>
current>
current>
current>
current>
current>en
Password:
Password:
Password:
current#
current#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
current(config)#
current(config)#
current(config)#
```

Using strong password

G. Unauthorized Public IP Access

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

```
15  # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16  # to the VRT Certified Rules License Agreement (v2.0).
17  #
18  #-------------
19  # LOCAL RULES
20  #-------------
21
22  Alert icmp  any any -> any any (msg:"testing ICMP alert"; sid:1000001;)
23  Alert udp  any any -> any any (msg:"testing udp alert"; sid:1000002;)
24  Alert tcp any any -> any any (msg:"testing tcp alert"; sid:1000003;)
25
```

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

```
03/22-15:13:56.491931  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.163:443 -> 192.168.10.109:6300
9
03/22-15:13:56.567361  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.163:443 -> 192.168.10.109:6300
5
03/22-15:13:57.395913  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.398403  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63012
03/22-15:13:57.398497  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.398629  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.398676  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.401039  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63012
03/22-15:13:57.401039  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63012
03/22-15:13:57.409431  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63012
03/22-15:13:57.409868  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63013 -> 192.168.10.1:53
03/22-15:13:57.410024  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
03/22-15:13:57.411998  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63013
03/22-15:13:57.412034  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63013 -> 192.168.10.1:53
03/22-15:13:57.412207  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63013 -> 192.168.10.1:53
03/22-15:13:57.412250  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63013 -> 192.168.10.1:53
03/22-15:13:57.415234  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63014
03/22-15:13:57.415322  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
03/22-15:13:57.415489  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
03/22-15:13:57.415551  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
03/22-15:13:57.418755  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63013
03/22-15:13:57.418979  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63013
03/22-15:13:57.418979  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63014
03/22-15:13:57.418979  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63014
03/22-15:13:57.428639  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.1:53 -> 192.168.10.109:63014
03/22-15:13:57.454779  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.161.47.103:443 -> 192.168.10.109:54628
03/22-15:13:57.455532  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:54628 -> 172.161.47.103:443
03/22-15:13:57.457381  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63012 -> 192.168.10.1:53
03/22-15:13:57.477489  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 192.168.10.109:63014 -> 192.168.10.1:53
```

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

```
ASA Version 9.6(1)
!
hostname NIYIGABA-FIREWALL
domain-name WR
enable password Ne88Ah9pALg7rn0g encrypted
names
!
interface GigabitEthernet1/1
 nameif INSIDE
 security-level 100
 ip address 10.10.10.1 255.255.255.252
!
interface GigabitEthernet1/2
 nameif DMZ
 security-level 70
 ip address 172.16.10.1 255.255.255.240
!
interface GigabitEthernet1/3
 nameif OUTSIDE
 security-level 0
 ip address 20.20.20.1 255.255.255.252
!
interface GigabitEthernet1/4
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no nameif
 no security-level
 no ip address
 shutdown
!
```

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

2. Comprehensive Solution Plan

1. **Immediate Actions**:

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

2. **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)

3. **Remediation Phase**:

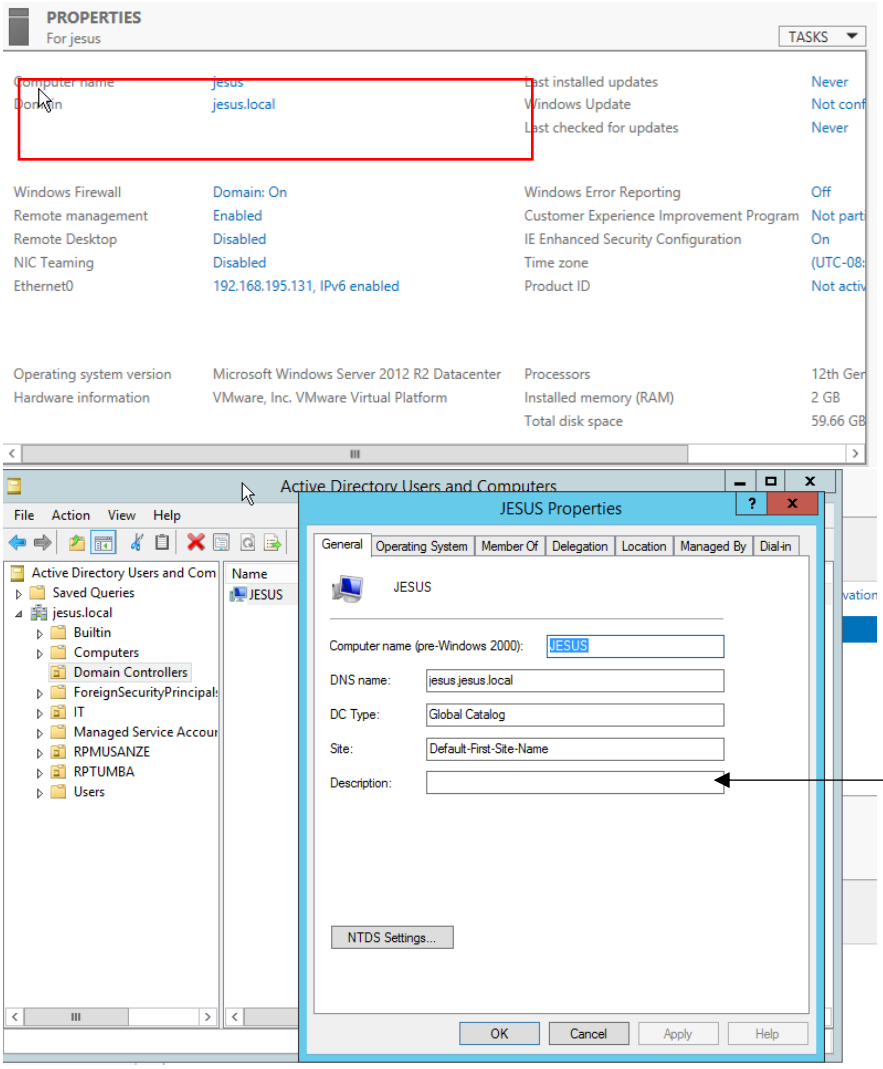
    - Implement proper encryption for data transmission
    - Configure firewall rules to block unauthorized access
    - Patch identified vulnerabilities
    - Establish proper authentication mechanisms

4. **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

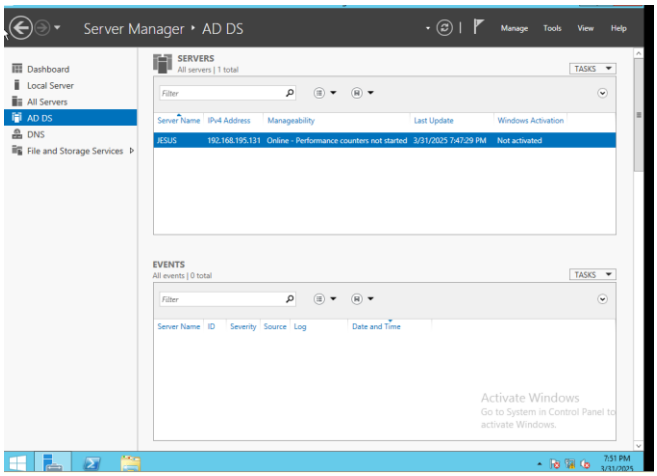
TASK 1 CREATE DOMAIN CONTROL THAT SHOULD HAVE NAME AND DOMAIL NAME

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

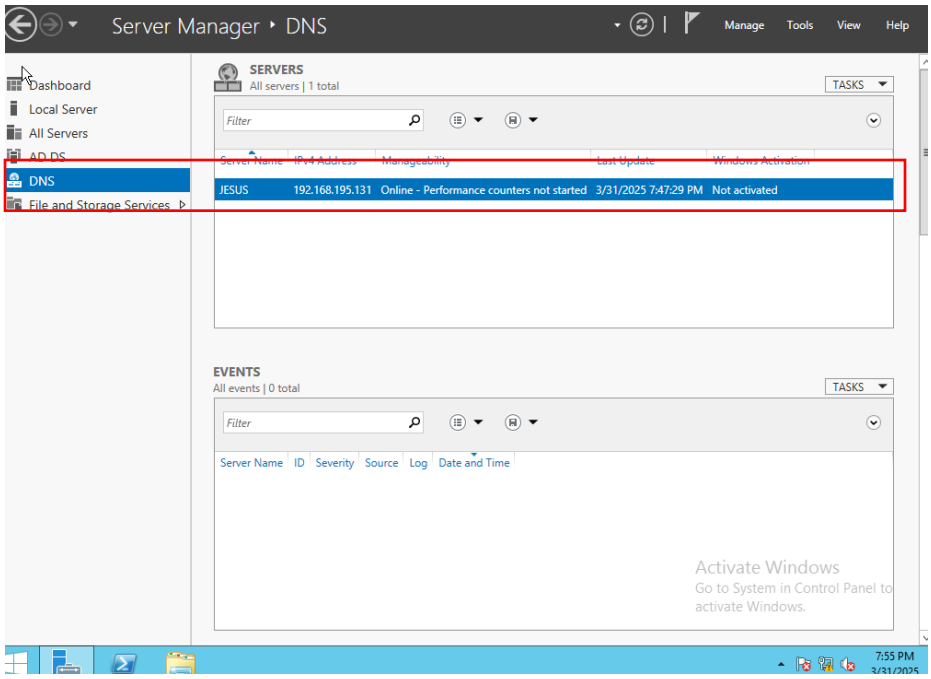


Task 2 enable the following services: DNS and AD DS

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

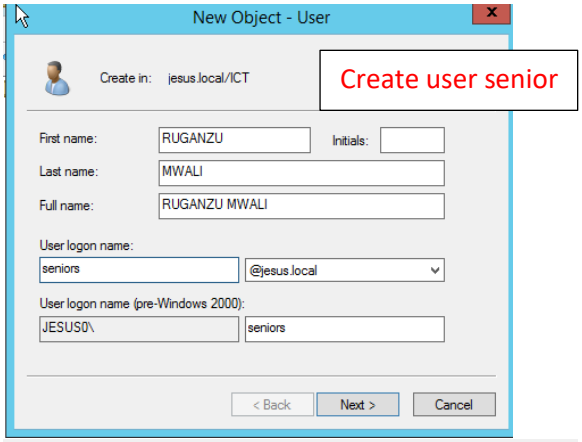


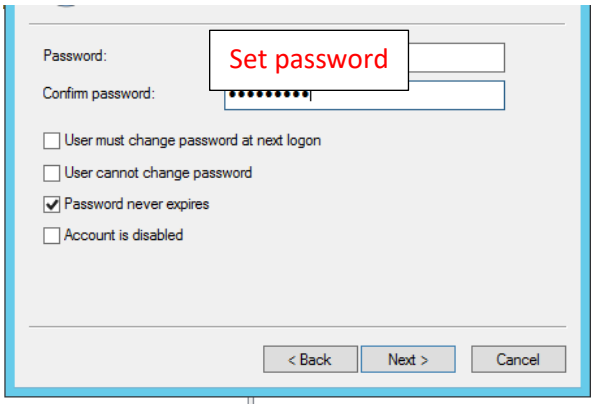
ii. DNS server

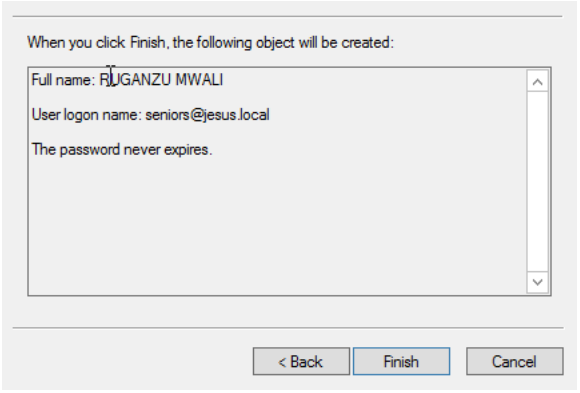


Task 3 create grouper of user ICT with add users in progress

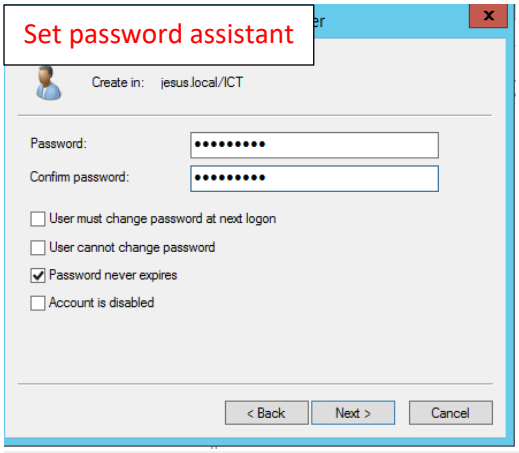
i. Ruganzu mwali user and their roles

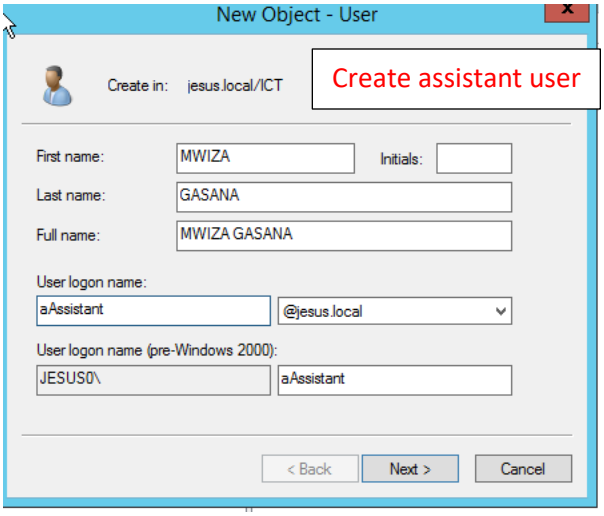


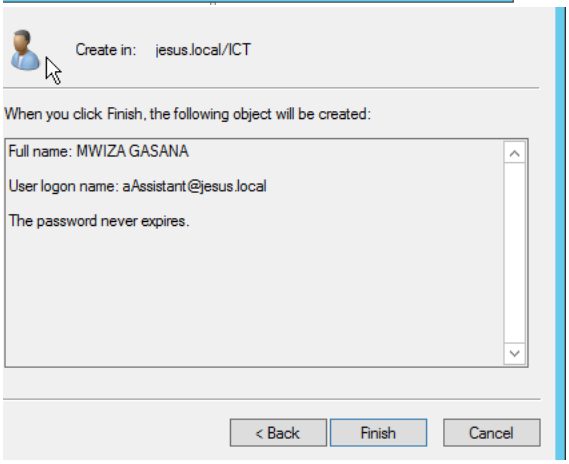




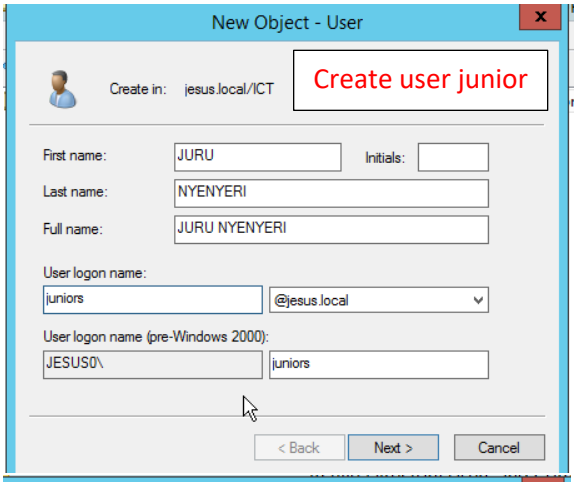
ii. Assistant group user and role

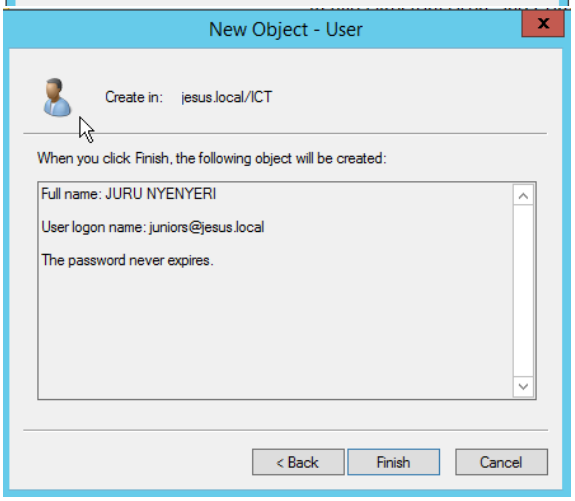




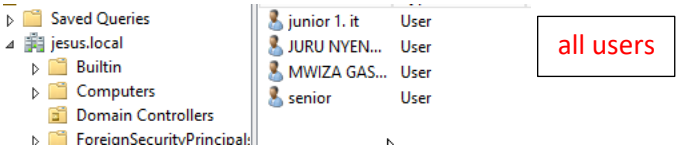


iii. Junior group and user juru and their role





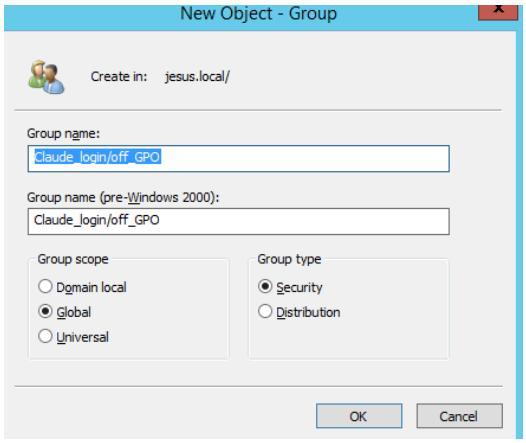
All users



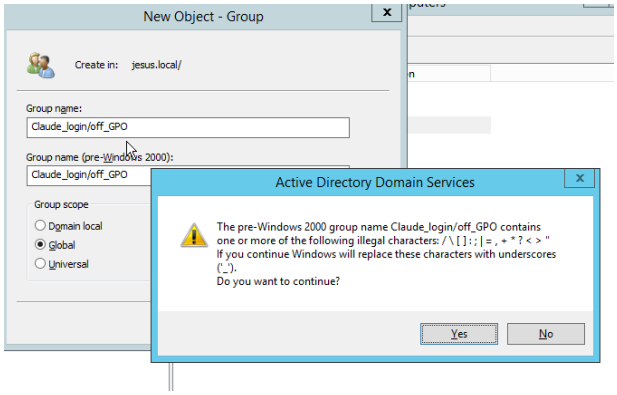
Task 4 create TWO GPO WITH MY LAST NAME

i. Claude_login/off_GPO

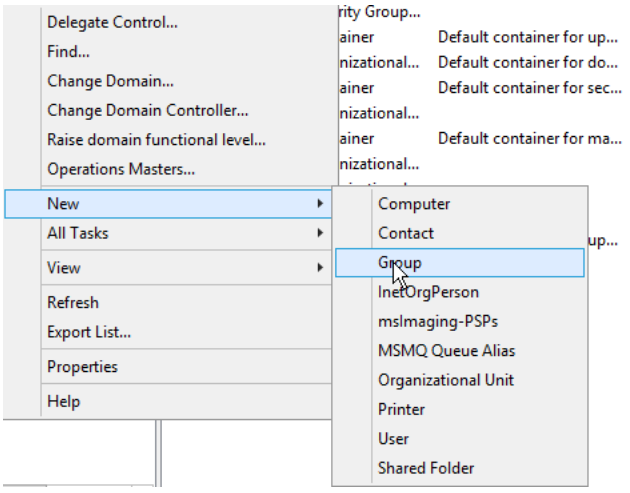
Step 1 select domain name and new open group

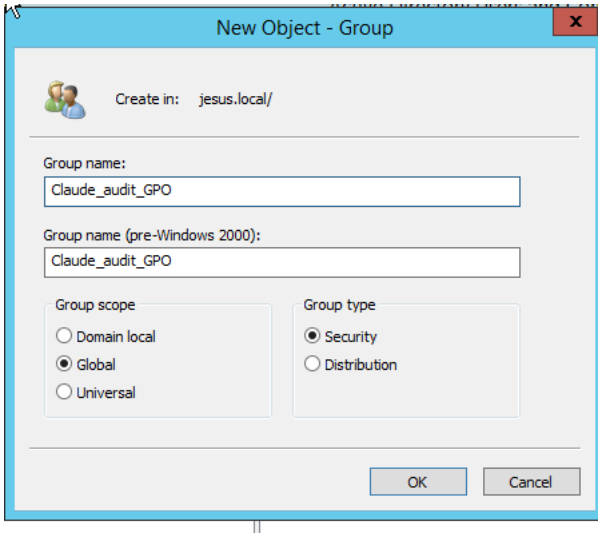


Step 2 after write group name ok

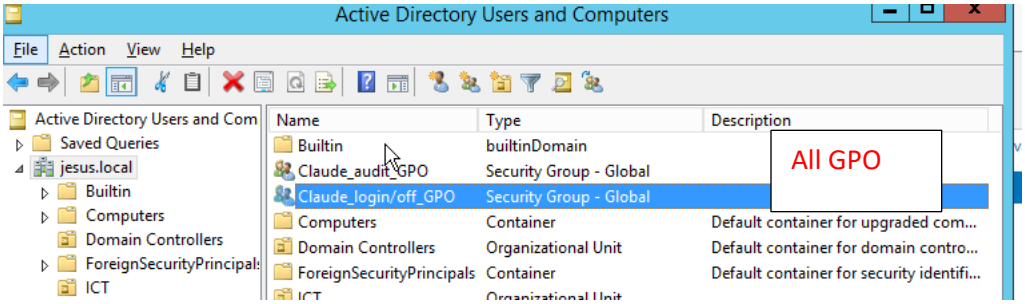


ii. Claude_audit_GPO

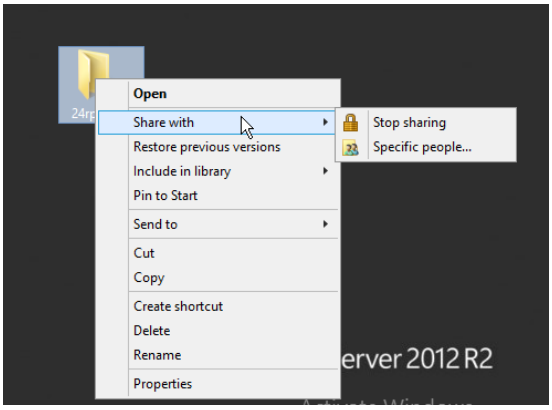




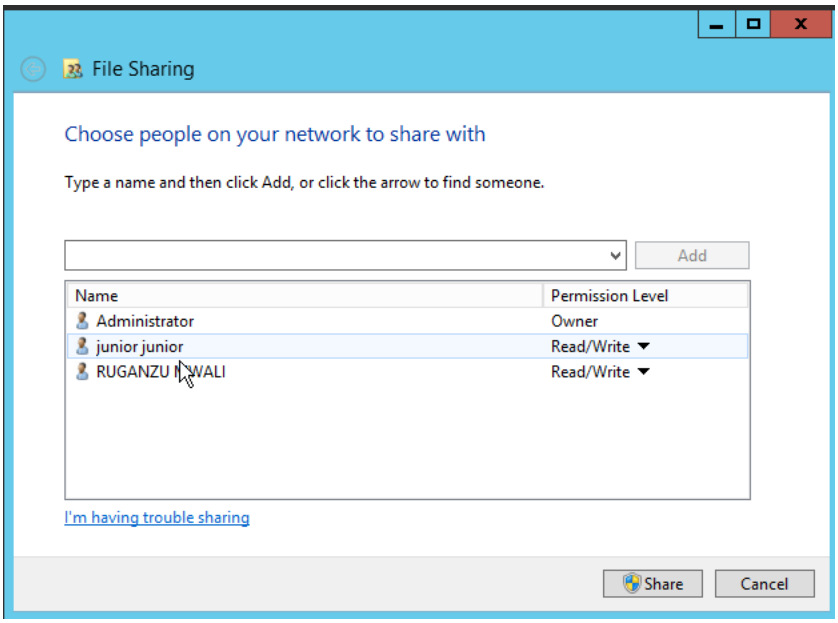
All group



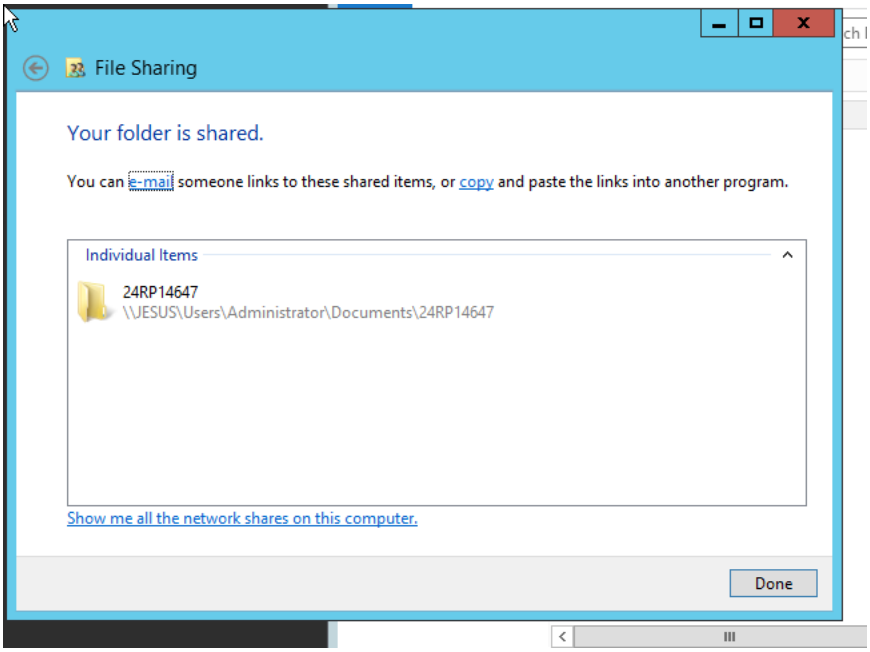
TASK 5 SHARE FOLDER



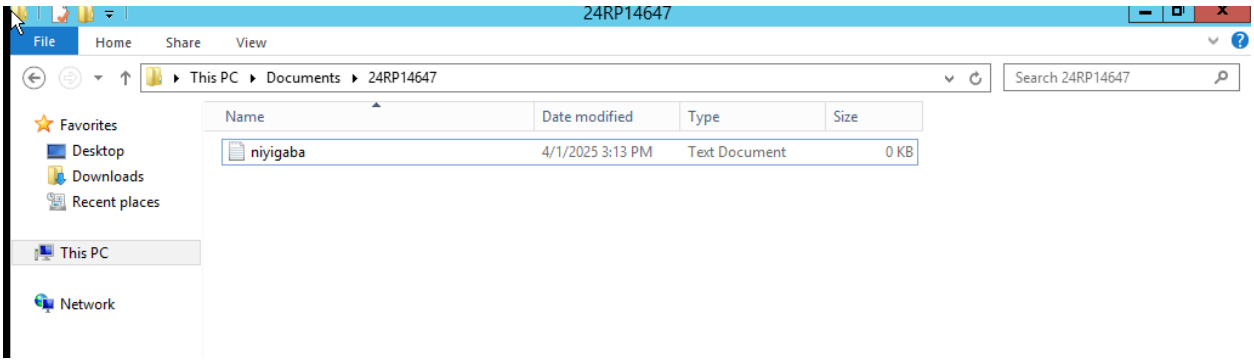
After open specific set access



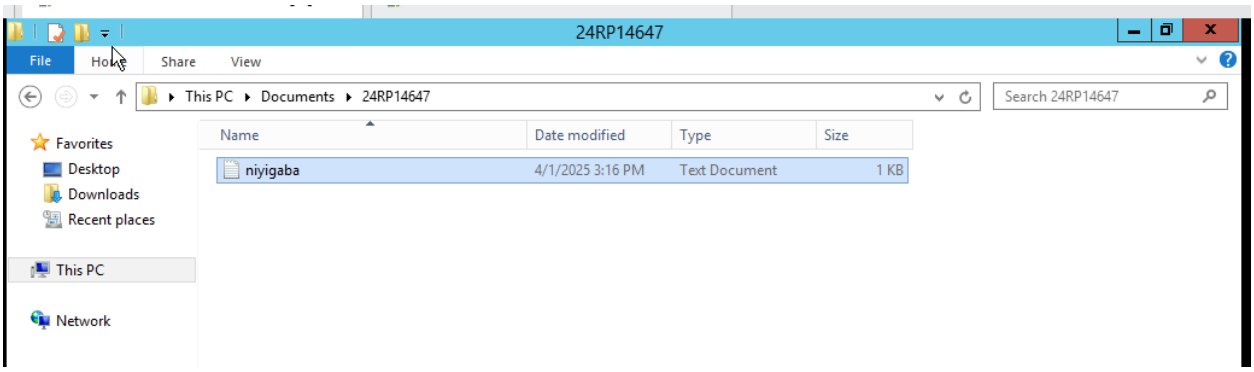
Share



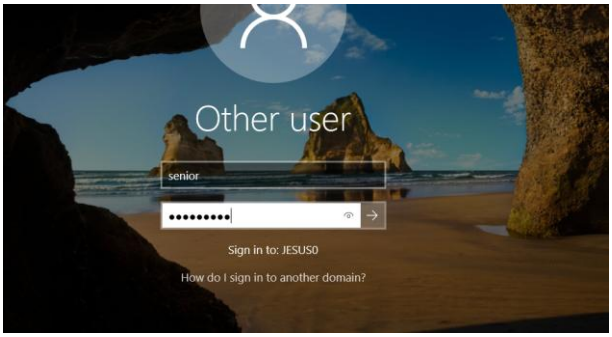
Task 6 creat file and security



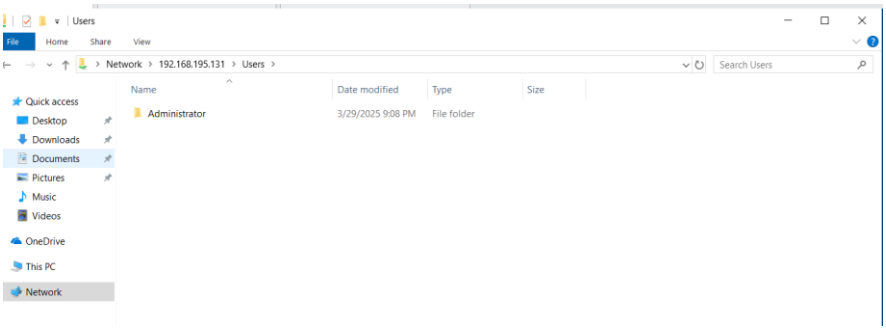
Then increase size of file



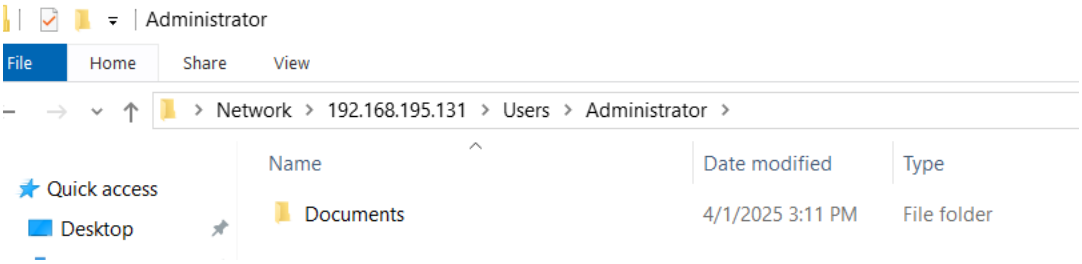
Then get share using window client



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