RP/IPRC MUSANZE

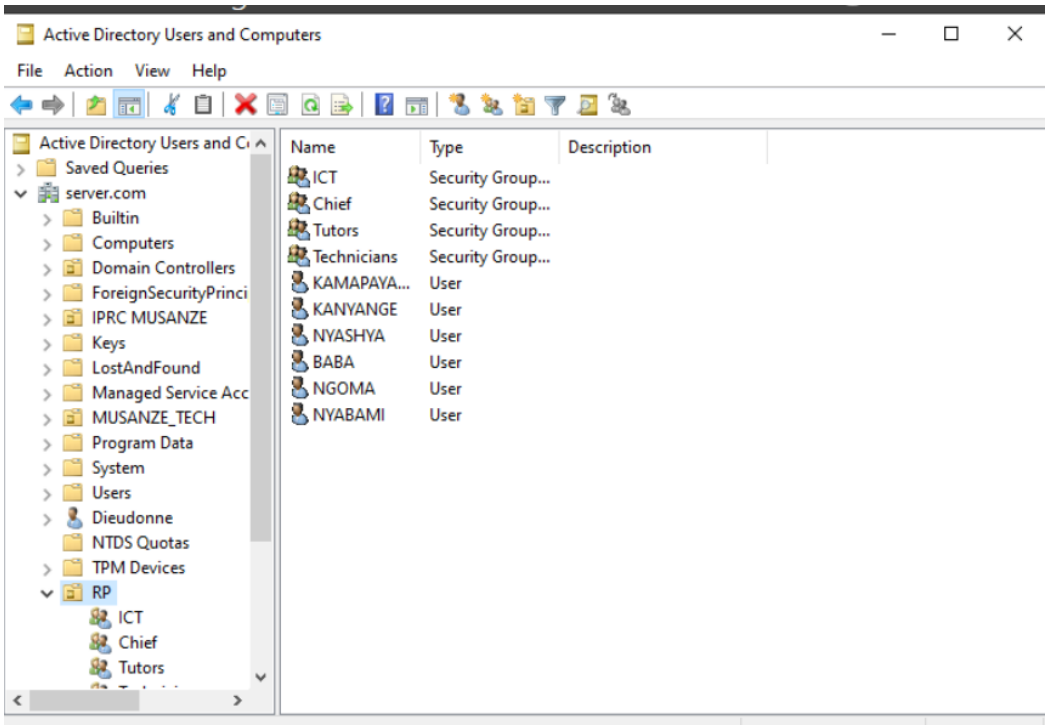
REGISTRATION NUMBER: 23RP00022

MODULE CODE & NAME: CYBER SECURITY(ITLCS 801)

On May 03rd ,2024

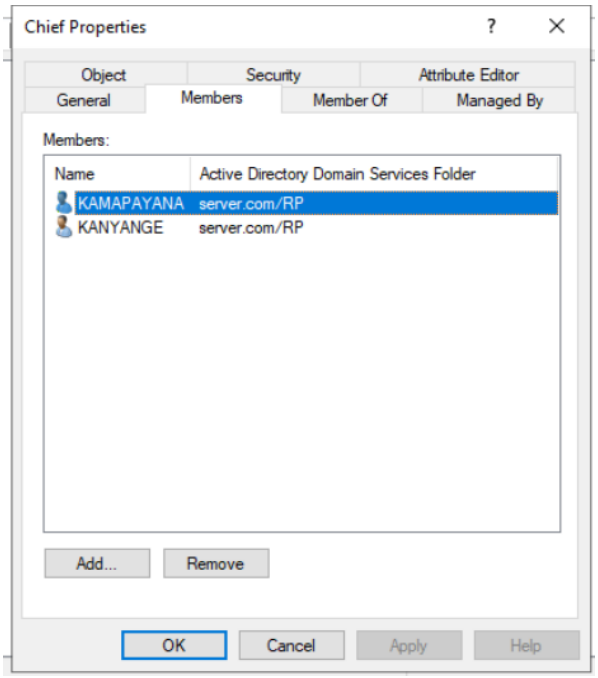
CYBER SECURITY (ITLCS 801) PRACTICAL EXAM

1. Two pages with screenshot about the implementation of OU, users groups membership and roles
    - this image show OU and its components.

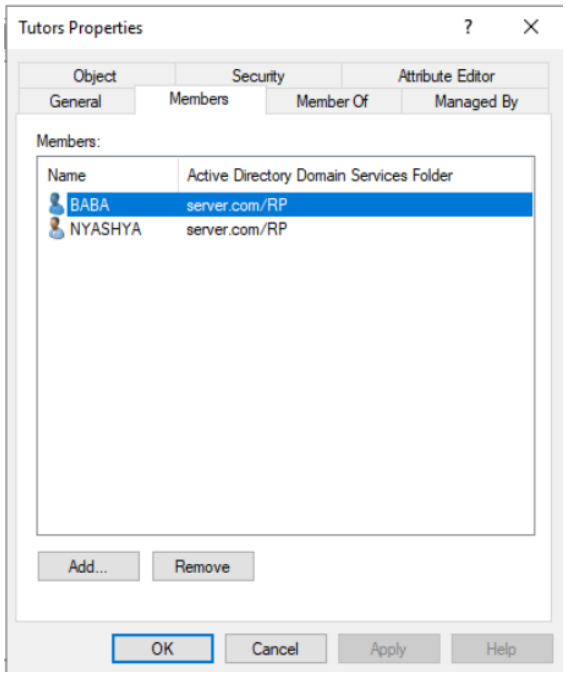


    - this image show that Group Users ICT has different group of user which are Chief, Tutors and technicians.
    - these images show members of each group of users

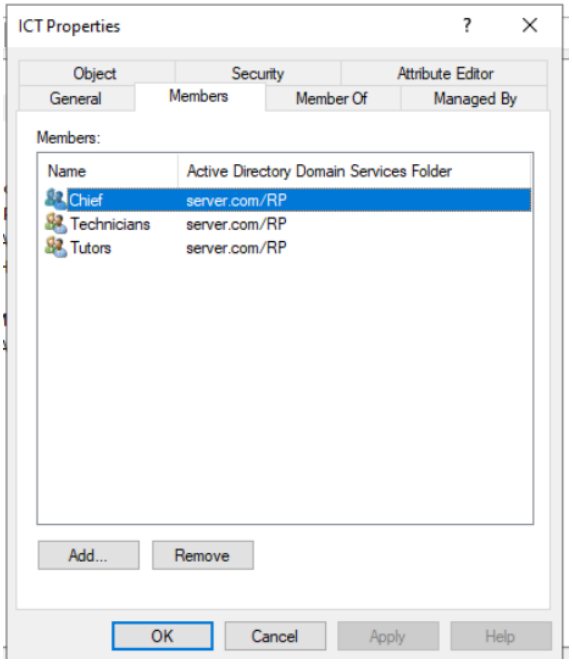
Here it shows members of Chief Group

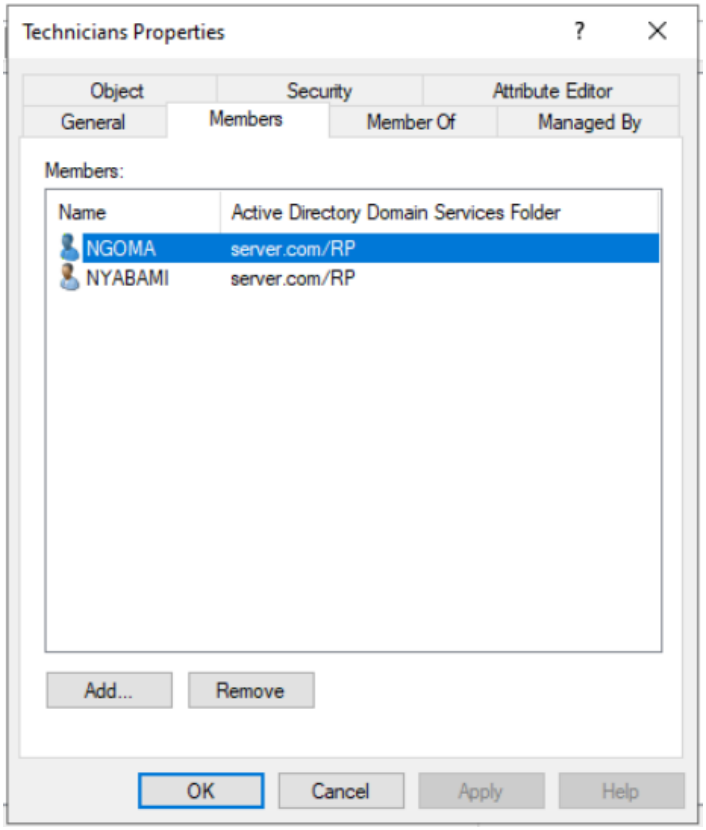


Her it shows members of tutors Group

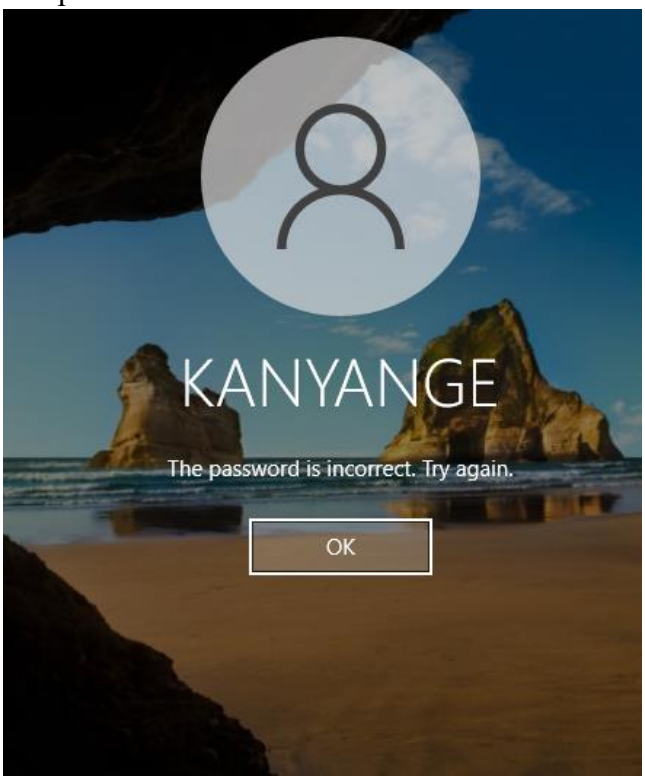


Here it shows members of Chief Group

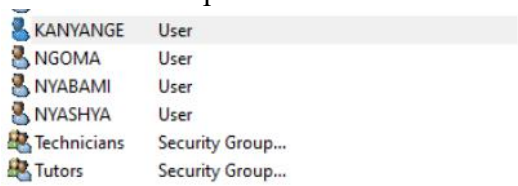


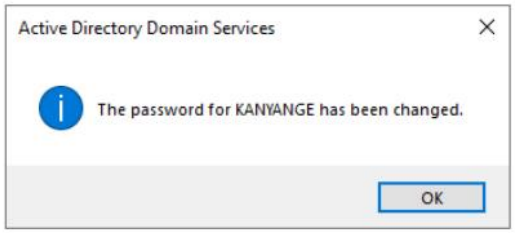


2. Kanyange has been experiencing difficulties with their login credentials, account has been compromised

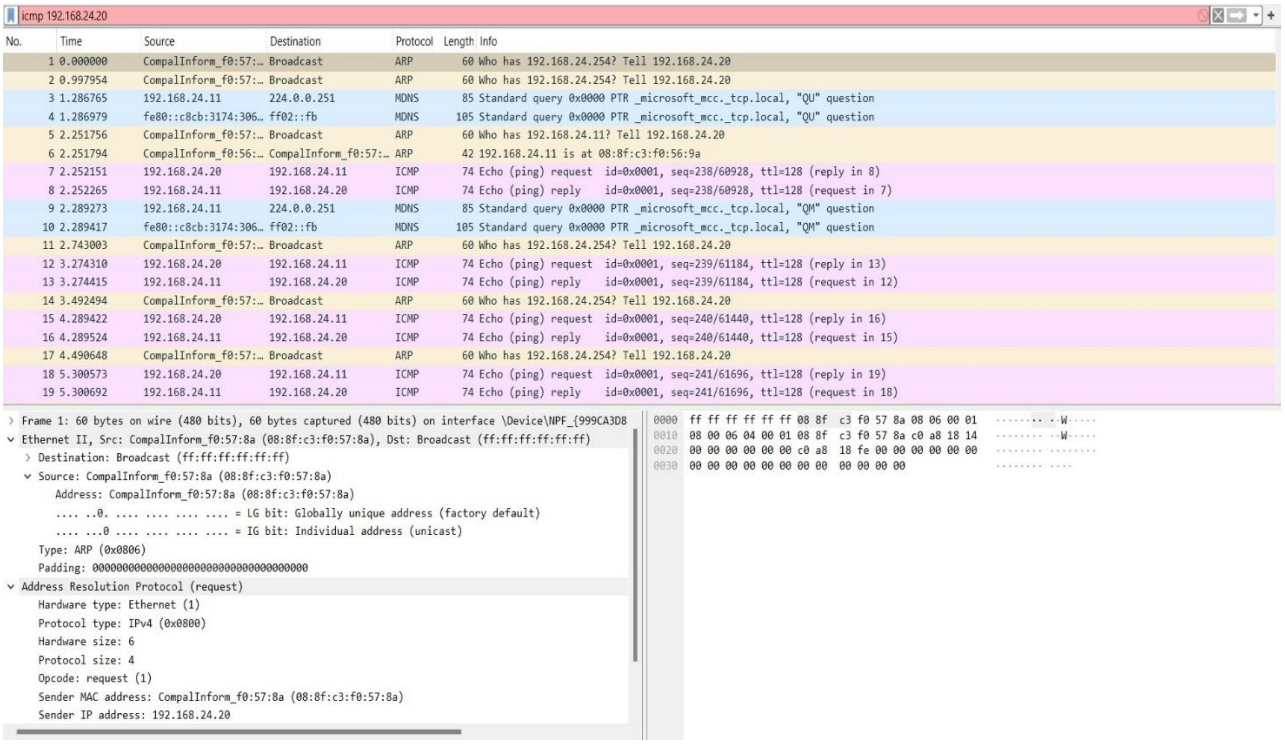


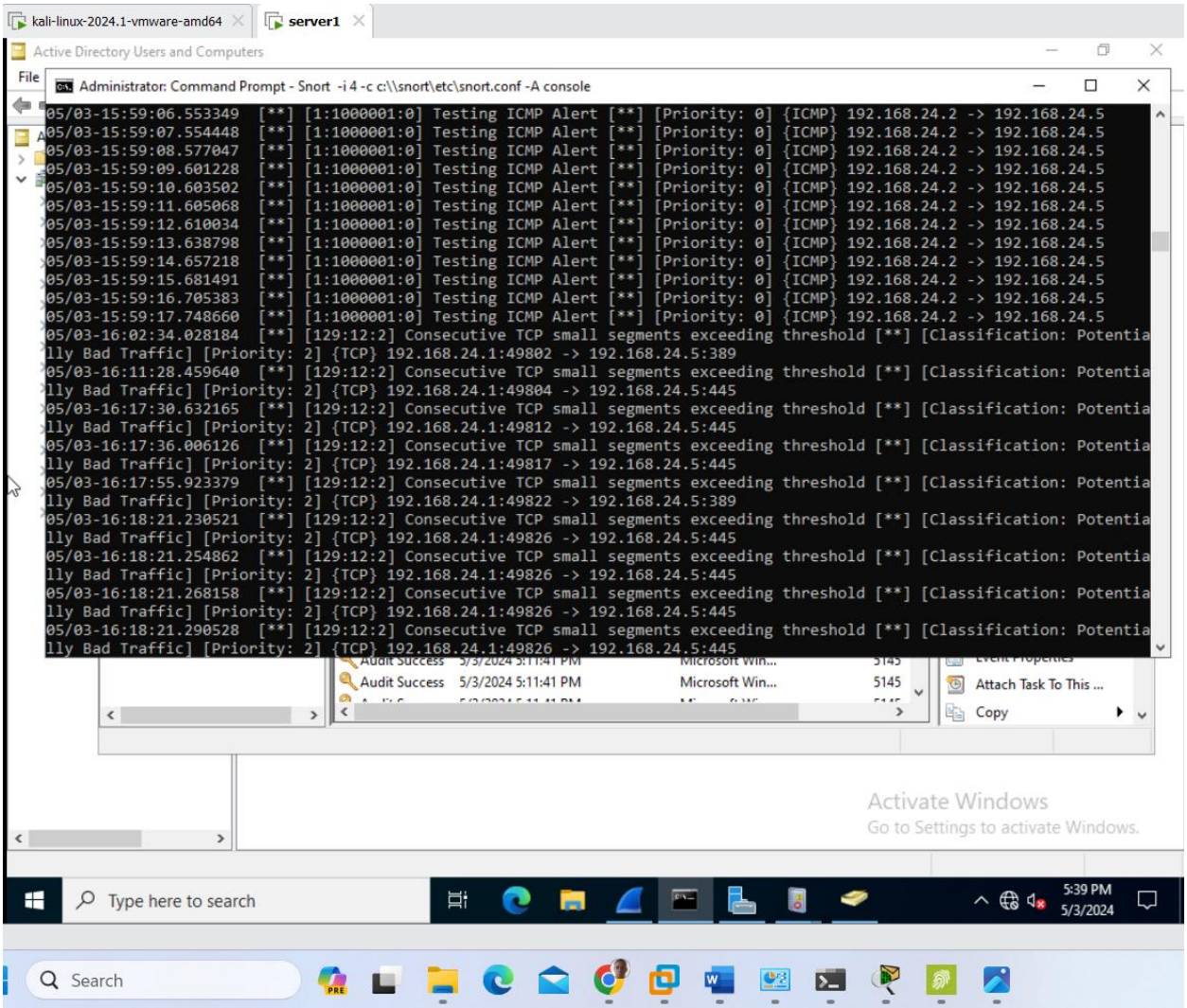
the solution is to reset password and I advise her to use strong password at least 8 characters which contains letters (upper and lower case), symbols, numbers and special characters. The password must be look like Jc3*l$Br@6.9?





3. Incoming traffic from foreign country




kali-linux-2024.1-vmware-amd64
server1
Active Directory Users and Computers
File
Administrator: Command Prompt - Snort -i 4 -c c:\\snort\etc\snort.conf -A console
05/03-15:59:06.553349 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:07.554448 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:08.577047 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:09.601228 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:10.603502 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:11.605068 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:12.610034 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:13.638798 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:14.657218 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:15.681491 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:16.705383 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-15:59:17.748660 [**] [1:1000001:0] Testing ICMP Alert [**] [Priority: 0] {ICMP} 192.168.24.2 -> 192.168.24.5
05/03-16:02:34.028184 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49802 -> 192.168.24.5:389
05/03-16:11:28.459640 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49804 -> 192.168.24.5:445
05/03-16:17:30.632165 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49812 -> 192.168.24.5:445
05/03-16:17:36.006126 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49817 -> 192.168.24.5:445
05/03-16:17:55.923379 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49822 -> 192.168.24.5:389
05/03-16:18:21.230521 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49826 -> 192.168.24.5:445
05/03-16:18:21.254862 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49826 -> 192.168.24.5:445
05/03-16:18:21.268158 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49826 -> 192.168.24.5:445
05/03-16:18:21.290528 [**] [129:12:2] Consecutive TCP small segments exceeding threshold [**] [Classification: Potentia
lly Bad Traffic] [Priority: 2] {TCP} 192.168.24.1:49826 -> 192.168.24.5:445
Audit Success 5/3/2024 5:11:41 PM Microsoft Win... 5145
Attach Task To This ...
Copy
Activate Windows
Go to Settings to activate Windows.
Type here to search
5:39 PM
5/3/2024
Search

The solution is to block the foreign IP that is in our network and for here the foreign IP is ping and no response is getting

375	478.526531	192.168.24.20	192.168.24.11	ICMP	74 Echo (ping) request id=0x0001, seq=247/63232, ttl=128 (no response found!)
376	479.644000	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
377	480.619998	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
378	481.626685	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
379	483.511010	192.168.24.20	192.168.24.11	ICMP	74 Echo (ping) request id=0x0001, seq=248/63488, ttl=128 (no response found!)
380	487.038497	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
381	487.621634	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
382	488.516278	192.168.24.20	192.168.24.11	ICMP	74 Echo (ping) request id=0x0001, seq=249/63744, ttl=128 (no response found!)
383	488.626876	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
384	489.631689	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
385	490.622097	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
386	491.627953	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
387	492.622506	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
388	506.019141	192.168.24.20	192.168.24.11	ICMP	74 Echo (ping) request id=0x0001, seq=250/64000, ttl=128 (no response found!)
389	506.211865	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11
390	507.134187	CompalInform_f0:56:…	Broadcast	ARP	42 Who has 192.168.24.254? Tell 192.168.24.11

```
ame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{999CA3D8
thernet II, Src: CompalInform_f0:57:8a (08:8f:c3:f0:57:8a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory de
    .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
 Source: CompalInform_f0:57:8a (08:8f:c3:f0:57:8a)
    Address: CompalInform_f0:57:8a (08:8f:c3:f0:57:8a)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 Type: ARP (0x0806)
 Padding: 000000000000000000000000000000000000
dress Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
```

```
0000  ff ff ff ff ff ff 08 8f  c3 f0 57 8a 08 06 00 01   ........ ..W.....
0010  08 00 06 04 00 01 08 8f  c3 f0 57 8a c0 a8 18 14   ........ ..W.....
0020  00 00 00 00 00 00 c0 a8  18 fe 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

4. They suspect that data might be intercepted during transmissions from colleges to the data center

   This image bellow show how data that are in transmission can tracked by attacker when they use Transport input Telnet.

```
..............

User Access Verification

Password: .............x.............ANSI..en......123

S1>eenn

Password: 123

S1#ccoonnffiigg  tt

Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#iinntteerr.. ... ... .tt  vvllaann  11

S1(config-if)#
```

As solution I advise RP to use ssh instead of using telnet and other security mechanisms. and here my physical devices(Switch) does not support SSH .

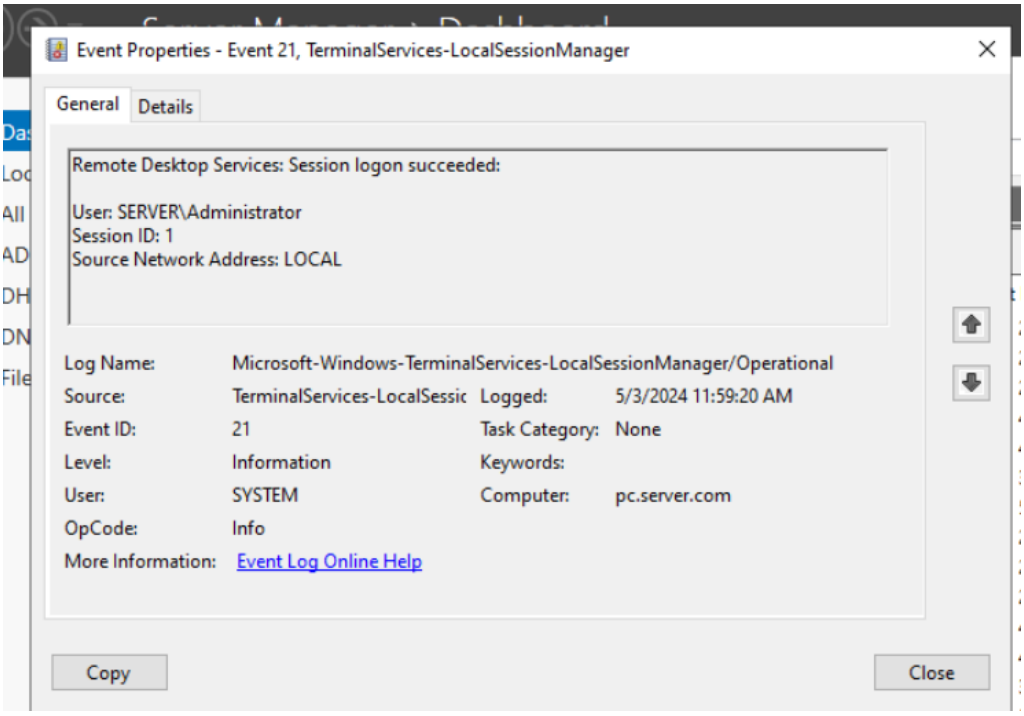
5. After analyzing the email that was sent to targeted employee conclude that email was phishing from attacker with following evidences:

    - The message ID has no mining and is not from RP mail server.
    - the sender detail emails and name is not clear
    - the email was from outside the RP domain

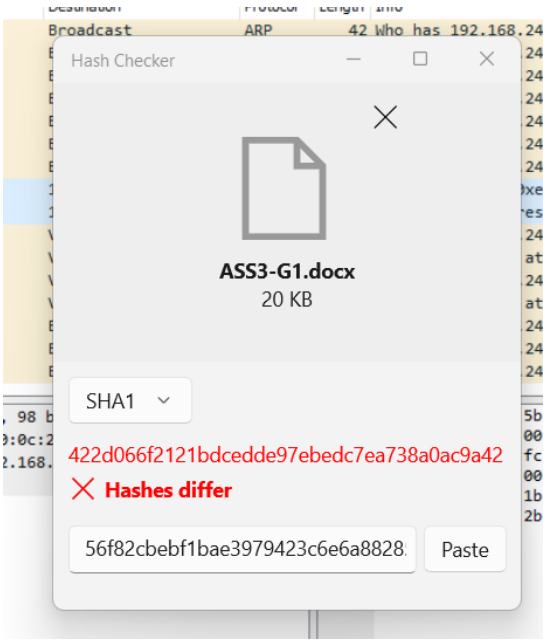
    As solution

    - I advise RP to train employees regularly to recognize phishing emails.
    - I advise employee to use advanced email filtering to block suspicious emails.
    - I advise employee to put it in in SPAM box and report the sender.

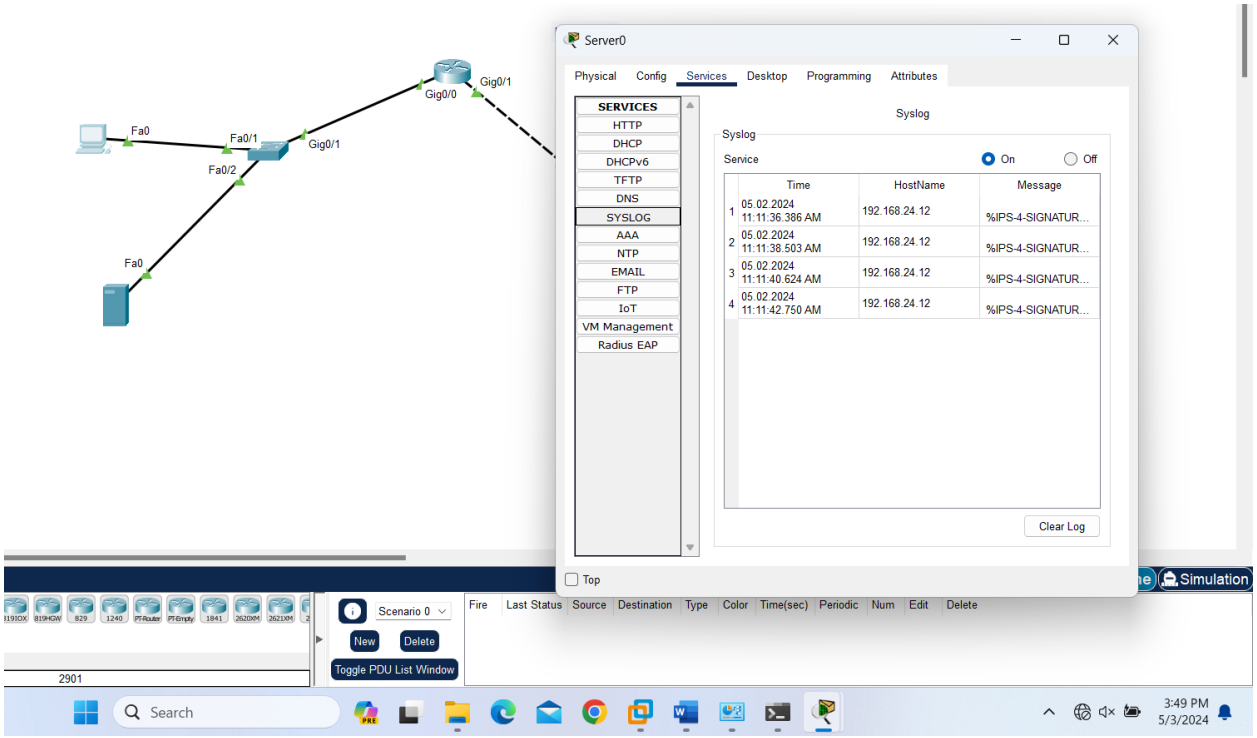
6. this image that show the user who does not have an access logged on to the server



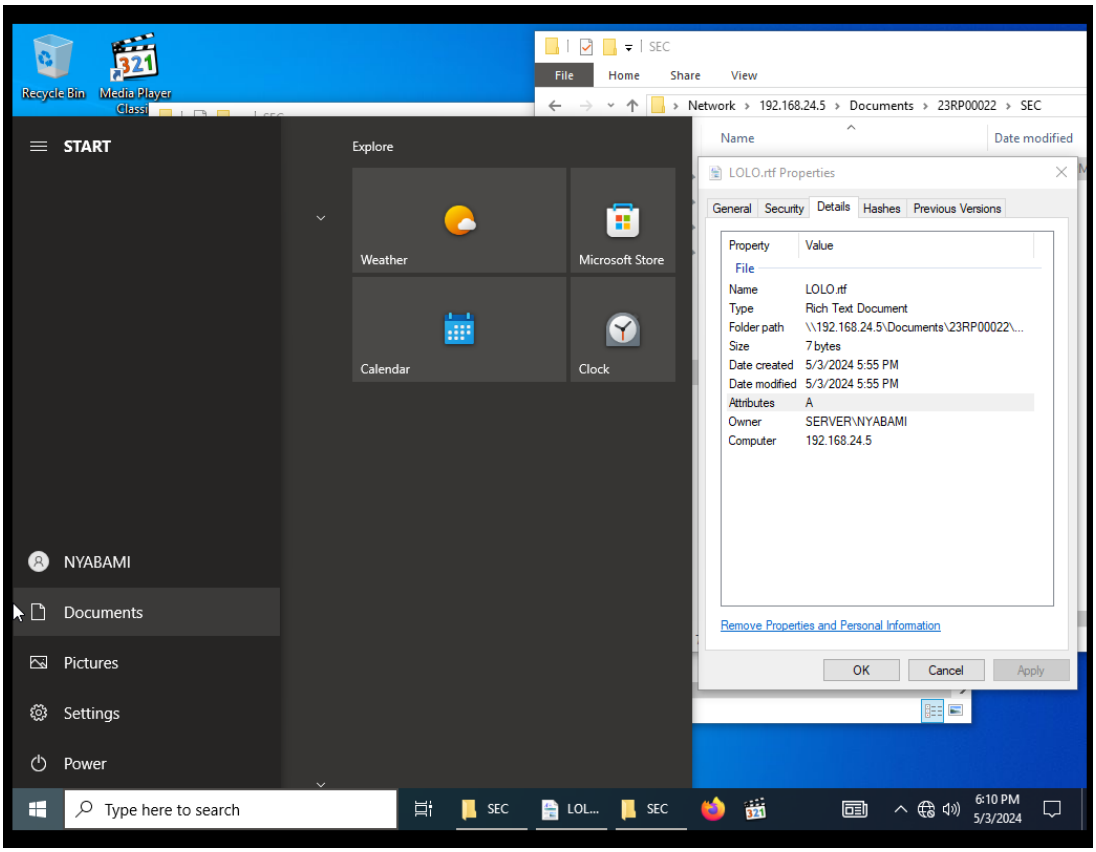
7. Senior network realized that the routers are configurations are being modified by Ngoma without consulting him/her
    the solution: I advise them to use hashing software like hash cheker.exe. to se if configuration has been modified.

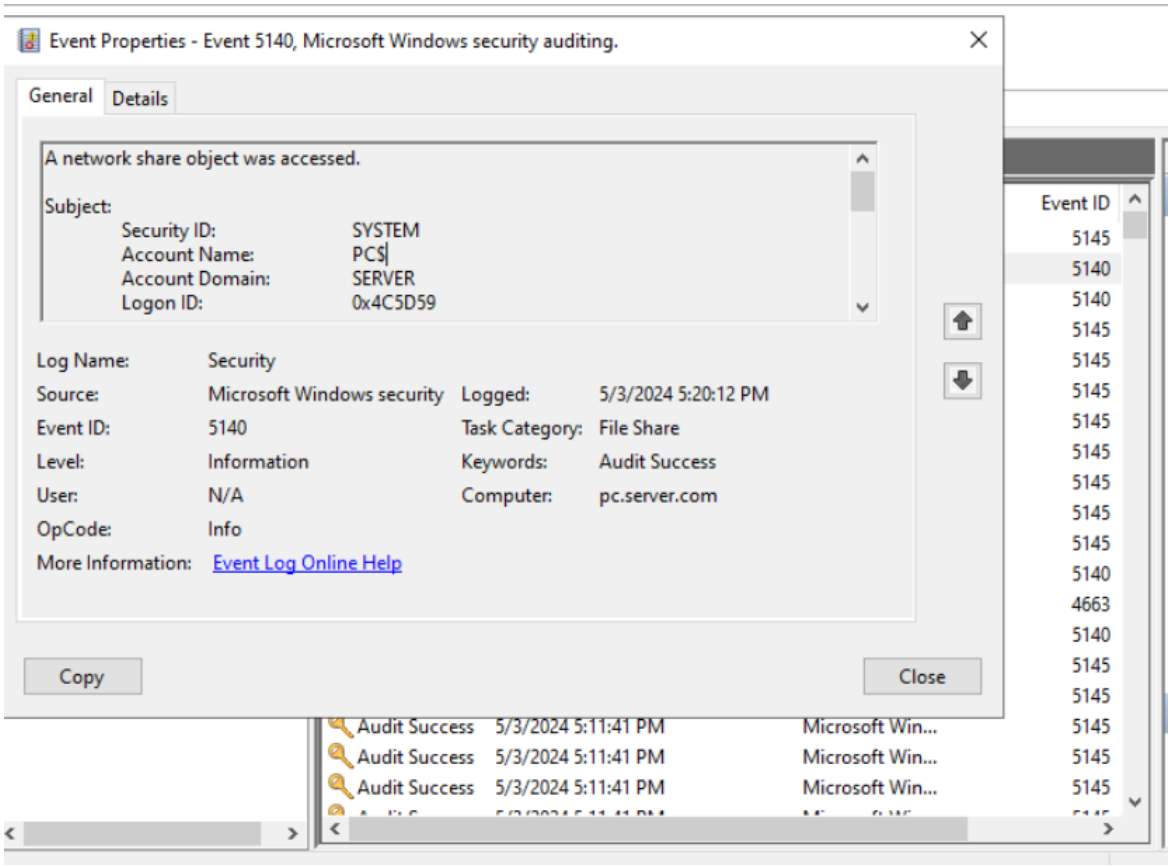


8. The system administrator was alerted by some system logs about unauthorized public IPs.



9. Institution suspects one of its employees (NYABAMI) of stealing propriety source of code and selling it to a competitor. the evidence needed are:




Event Properties - Event 5140, Microsoft Windows security auditing.
General
Details
A network share object was accessed.
Subject:
Security ID: SYSTEM
Account Name: PC$
Account Domain: SERVER
Logon ID: 0x4C5D59
Log Name: Security
Source: Microsoft Windows security
Logged: 5/3/2024 5:20:12 PM
Event ID: 5140
Task Category: File Share
Level: Information
Keywords: Audit Success
User: N/A
Computer: pc.server.com
OpCode: Info
More Information: Event Log Online Help
Copy
Close
Event ID
5145
5140
5140
5145
5145
5145
5145
5145
5145
5145
5145
5145
5140
4663
5140
5145
5145
Audit Success 5/3/2024 5:11:41 PM Microsoft Win... 5145
Audit Success 5/3/2024 5:11:41 PM Microsoft Win... 5145
Audit Success 5/3/2024 5:11:41 PM Microsoft Win... 5145