

DEPARTMENT: ICT
PROGRAM: INFORMATION TECHNOLOGY

RQF LEVEL: 8

MODULE: CYBERSECURITY

Academic: 2024-2025

ASSIGNMENT 2

Date: 2/04/2025

Name: NIYIGABA Claude

Reg No: 24RP14647

Assignment 2

Q. In summary, with examples of screenshots from snort and RBAC/window server, describe the best practices measures to implement for protection of information.

I. with examples of screenshots from snort

1. Snort -v

```
C:\Snort\bin>snort -v
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{39731FBC-23FC-4298-BD80-D36223F0CB3A}".
Decoding Ethernet

--== Initialization Complete ==--

o''-~
'''
--> Snort! <*-
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

Commencing packet processing (pid=26428)
```

2. Cmd snort/bin > snort -W / show interfaces

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

o''-~
'''
--> Snort! <*-
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

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 Ar
ea Network)
5  D0:39:57:18:CD:27      192.168.10.109 \Device\NPF_{778925A0-89F7-4A3F-BE35-617BC2671673}  Realtek RTL8852BE Wi-Fi 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 Adapt
er for VMnet8
7  00:50:56:C0:00:01      192.168.232.1  \Device\NPF_{3D145C2D-C425-476F-941B-41E0053A8F03}  VMware Virtual Ethernet Adapt
er for VMnet1
8  D6:39:57:18:CD:27      169.254.168.46 \Device\NPF_{0F28BA3B-21FC-45AB-B3FA-138F6EA9D1C9}  Microsoft Wi-Fi Direct Virtua
l Adapter #2
9  D2:39:57:18:CD:27      169.254.233.64 \Device\NPF_{A0C754D1-1AF0-465D-8110-B7D7A6E2EE25}  Microsoft Wi-Fi Direct Virtua
l Adapter
10 00:00:00:00:00:00      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>
```

3. Snort -I 4 -c c:\snort\etc\snort.conf -T for checking error

```

MaxRss at the end of rules:615907472

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -----
| Storage Format      : Full-Q
| Finite Automaton   : DFA
| Alphabet Size      : 256 Chars
| Sizeof State       : Variable (1,2,4 bytes)
| Instances          : 225
|   1 byte states    : 212
|   2 byte states    : 11
|   4 byte states    : 2
| Characters         : 226099
| States             : 179269
| Transitions        : 31396069
| State Density      : 68.4%
| Patterns           : 10652
| Match States       : 10948
| Memory (MB)        : 160.31
|   Patterns         : 1.24
|   Match Lists      : 2.82
|   DFA
|     1 byte states  : 1.24
|     2 byte states  : 18.60
|     4 byte states  : 136.03
+-----
[ Number of patterns truncated to 20 bytes: 618 ]

MaxRss at the end of detection rules:615907472
MaxRss at the end of detection rules:615907472
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring 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_SMP 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>

Total snort Fixed Memory Cost - MaxRss:1744646816
Snort successfully validated the configuration!

```

4. Checking white.list and black.list are exit

- | | |
|---|-------------|
|  backdoor.rules | 4/16/2024 1 |
|  bad-traffic.rules | 4/16/2024 1 |
|  black.list | 3/17/2025 1 |
|  blacklist.rules | 3/17/2025 1 |

5. Create Local.rules file for protection

```

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

```

6. Snort -i 4 -c c:\snort\etc\snort.conf -A console for checking service

```

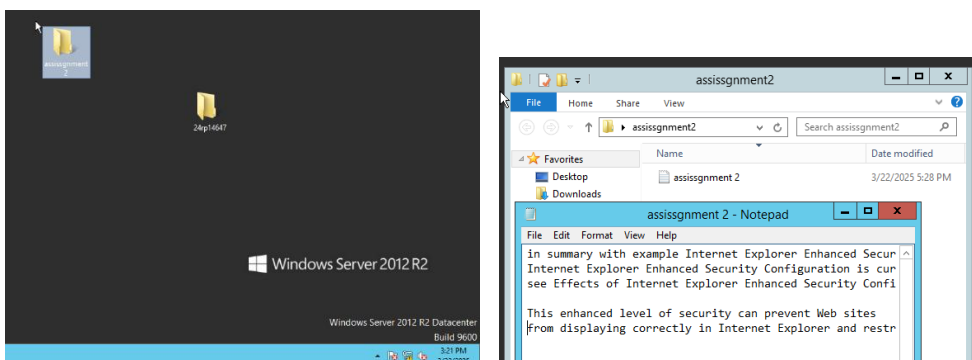
03/22-15:13:56.491931  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.163:443 -> 192.168.10.109:6300
9
03/22-15:13:56.567361  [**] [1:1000003:0] ΓÇ¥testing tcp alertΓÇ¥ [**] [Priority: 0] {TCP} 172.217.170.163:443 -> 192.168.10.109:6300
5
03/22-15:13:57.395913  [**] [1:1000003:0] 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

```

I. RBAC/window server, describe the best practices measures to implement for protection of information.

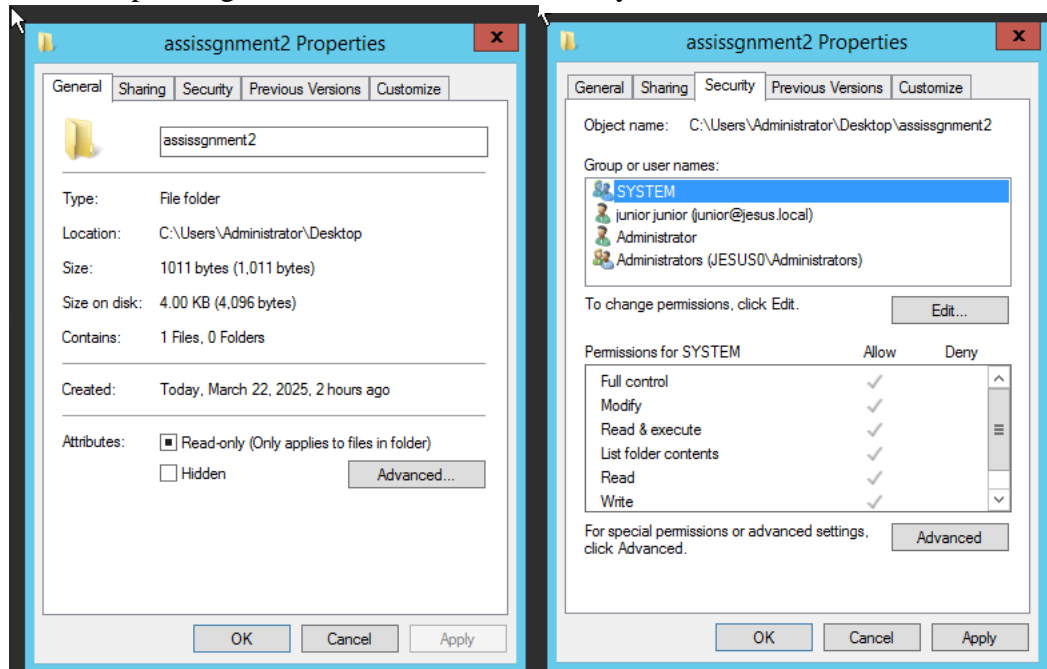
1. Create a folder and create file use to protect

I was create this folder for prevent access and manage user access and create file used to managing user where some user has full access other don't have it



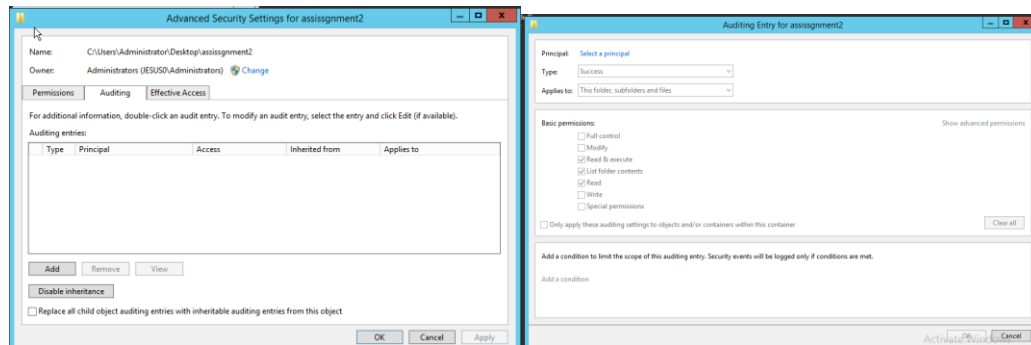
2. Selection on folder for security and permission to the users:

- I. Now I was select assissgnment2 and make it as right click, select advance for separating user access and select security

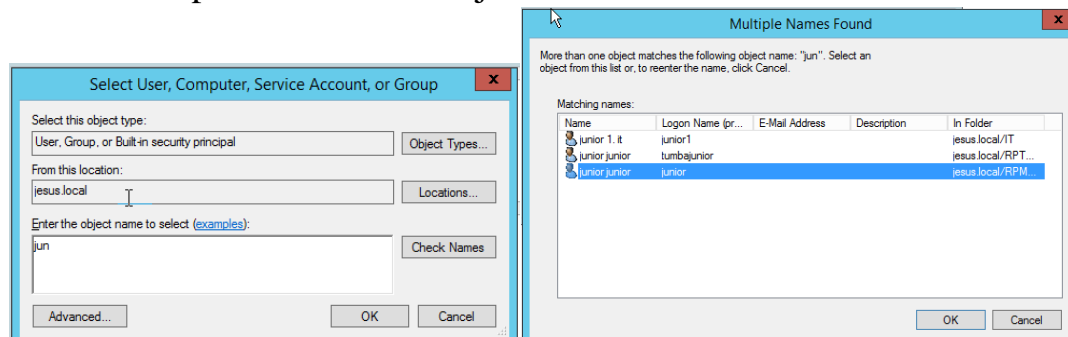


- II. This a picture that show user access now select auditing and add users want to access and select principle

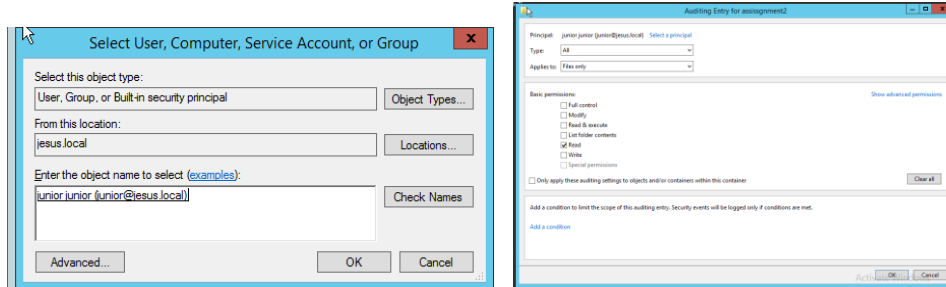
- ❖ Read
- ❖ Read and execute
- ❖ Read folder content



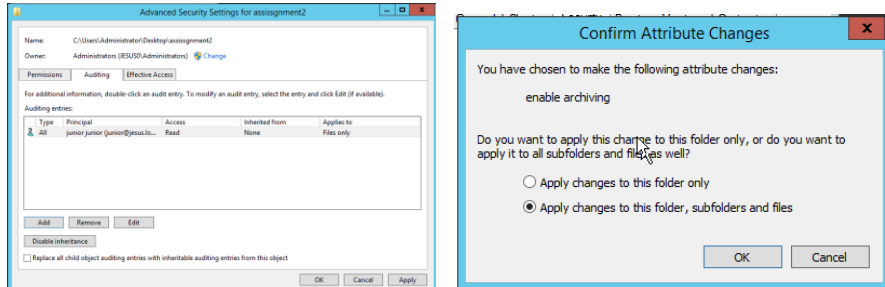
- III. Example of user used as junior has select from user list



IV. After select junior@jesus.local now has access for read only



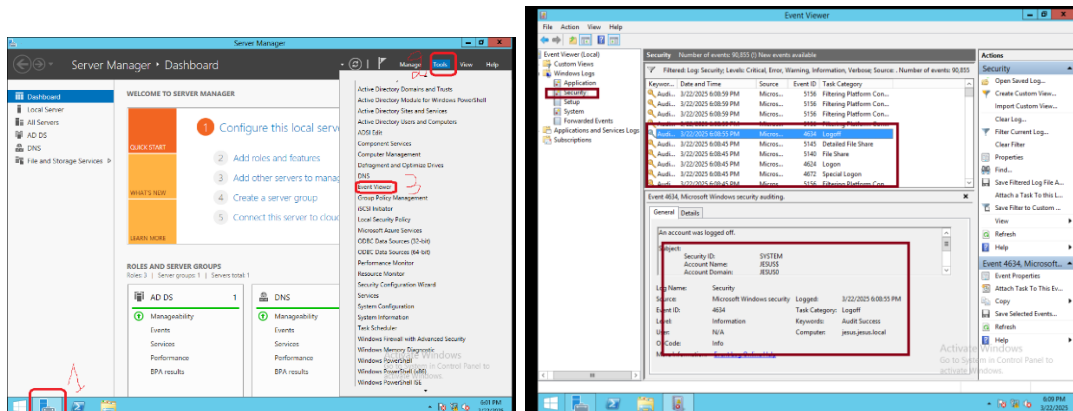
V. Conform that permission rules



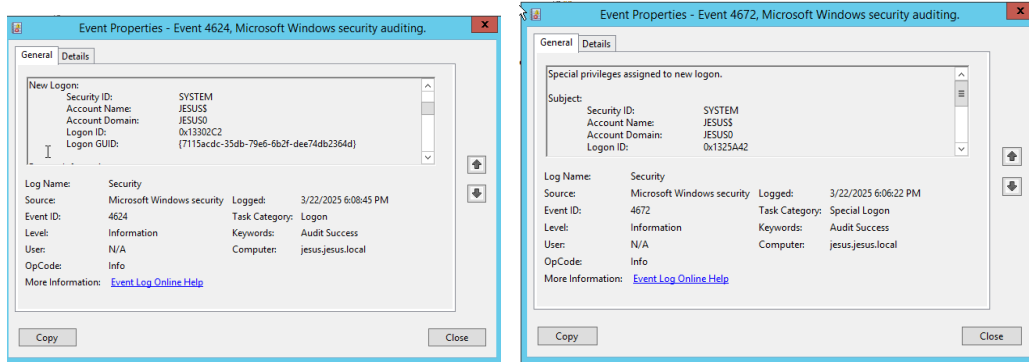
3. Review event

Now I open server manager for control user logon

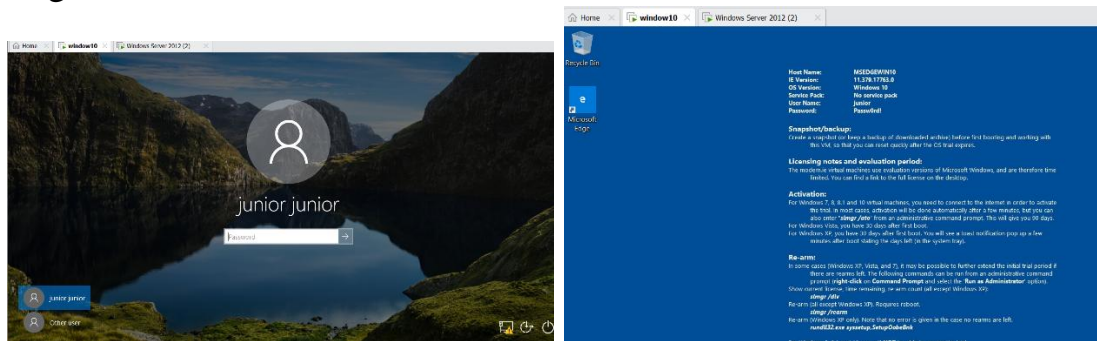
First open tools → select security → open event logon → select logon event that → has event id 4624



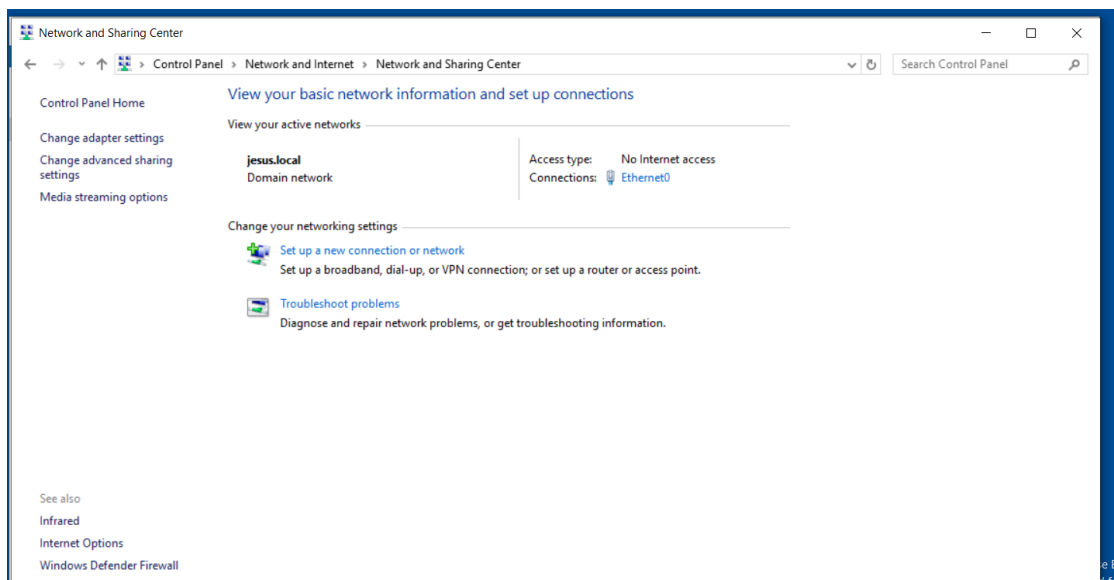
This all detail of jesus user where recording when , what and where she logon



4. Login with window 10



5. Checking when window 10 connected to server and when is connected to domain name after login using junior user to verify the domain name is available.



6. After connected to domain check permission

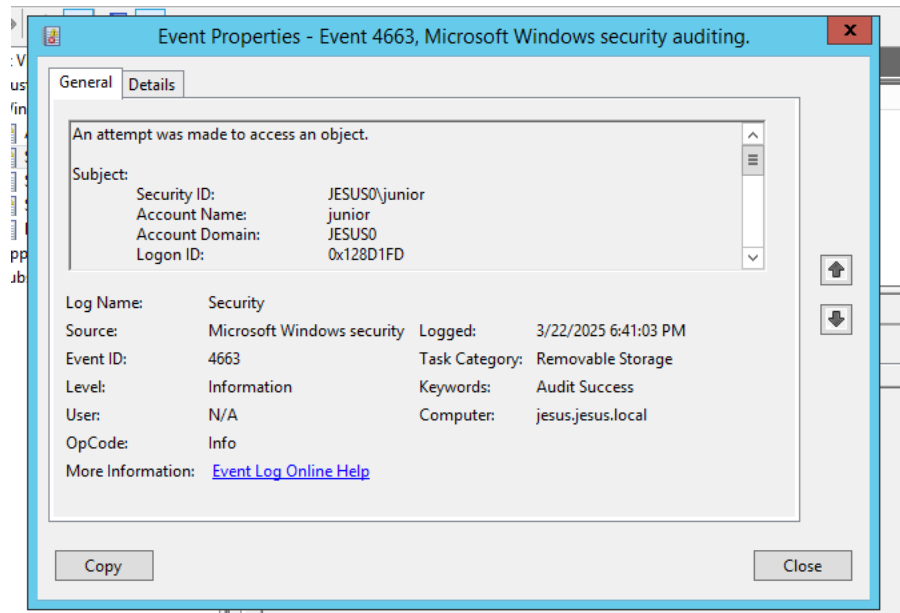


Figure 1: this a record where junion try to make login using domain name