

**DEPARTMENT: ICT**

**PROGRAM: INFORMATION TECHNOLOGY**

**RQF LEVEL: 8**

**RQF LEVEL: 8**

**MODULE: CYBERSECURITY**

**Academic: 2024-2025**

**ASSISSGNMENT 2**

**Date: 2/04/2025**

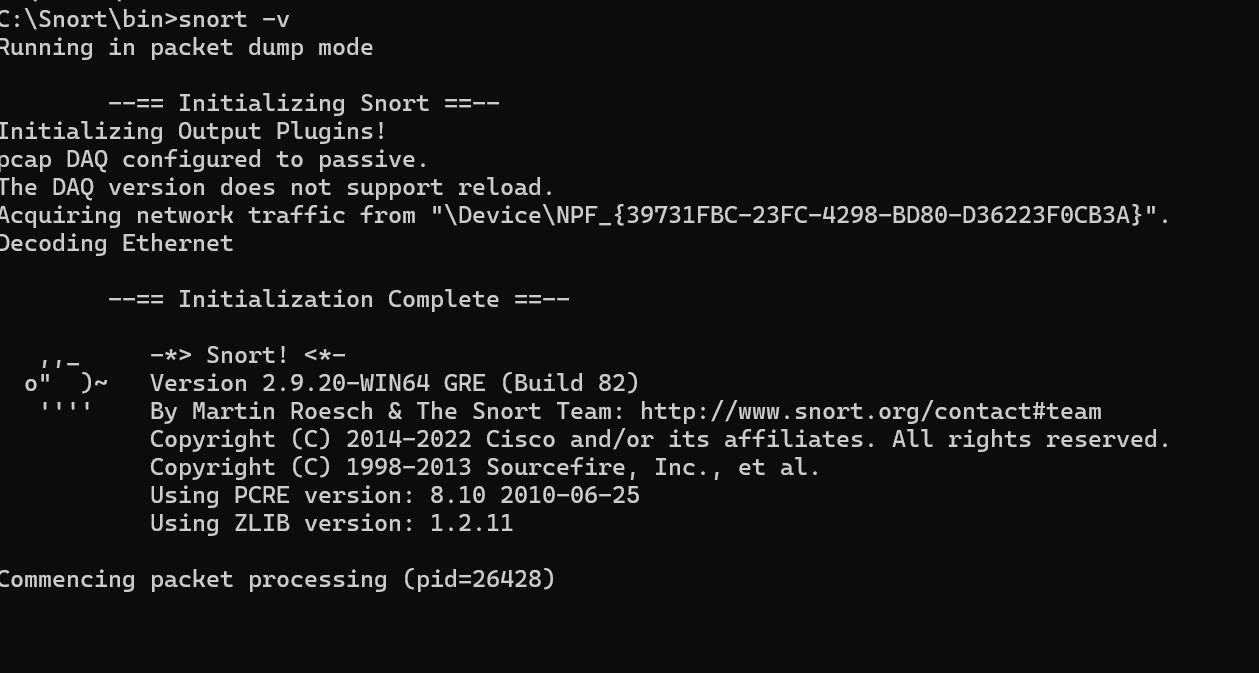
**Name: NIYIGABA Claude**

**Reg No: 24RP14647**

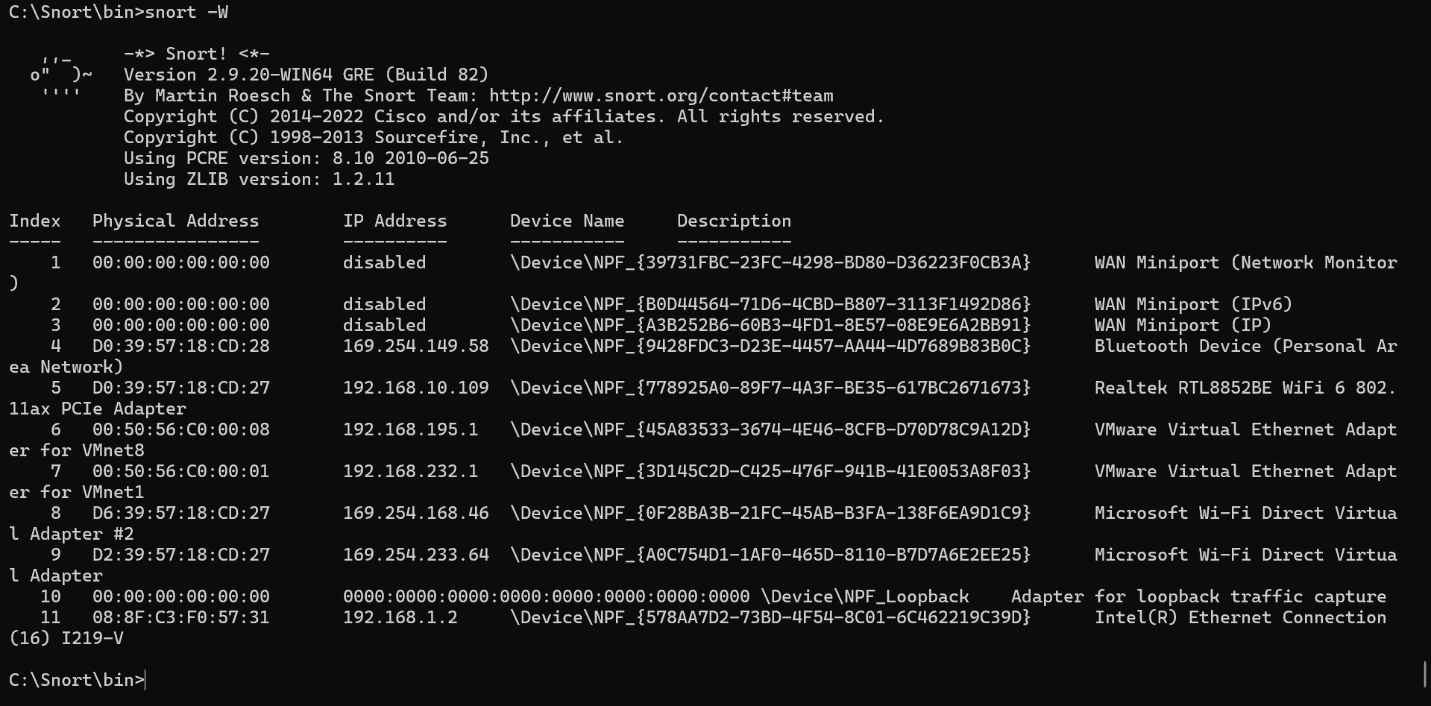
Assignment 2

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

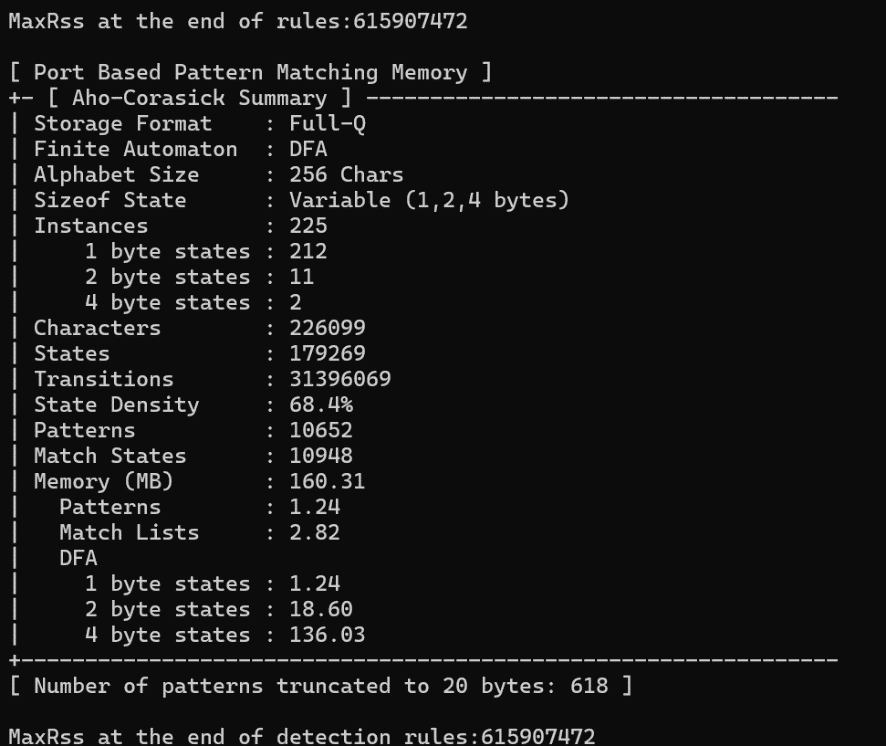
1. with examples of screenshots from snort
2. Snort –v

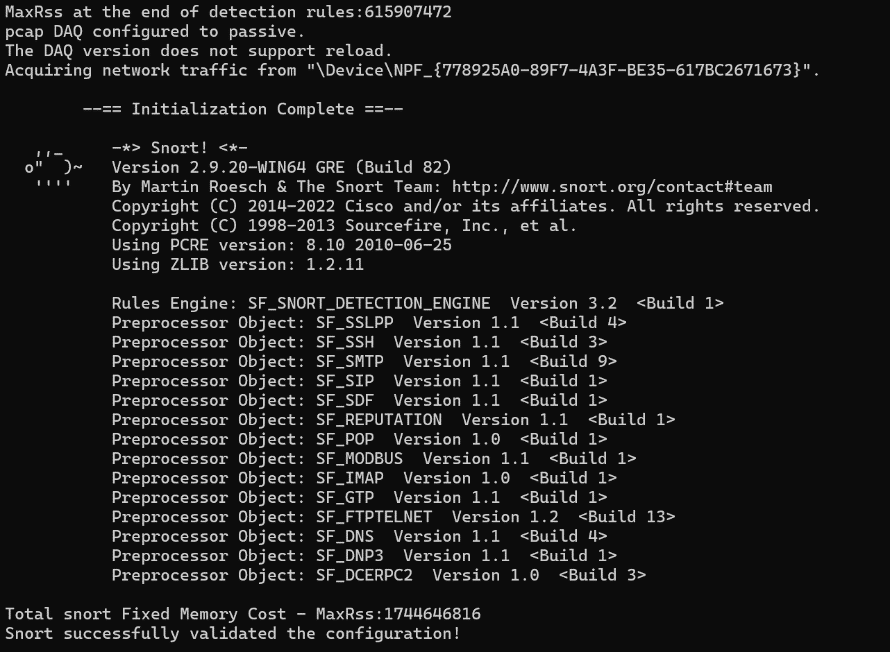


1. Cmd snort/bin > snort -W / show interfaces



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

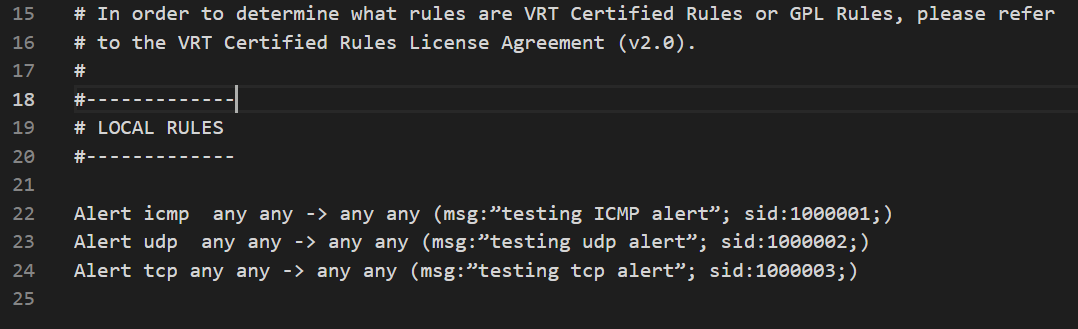




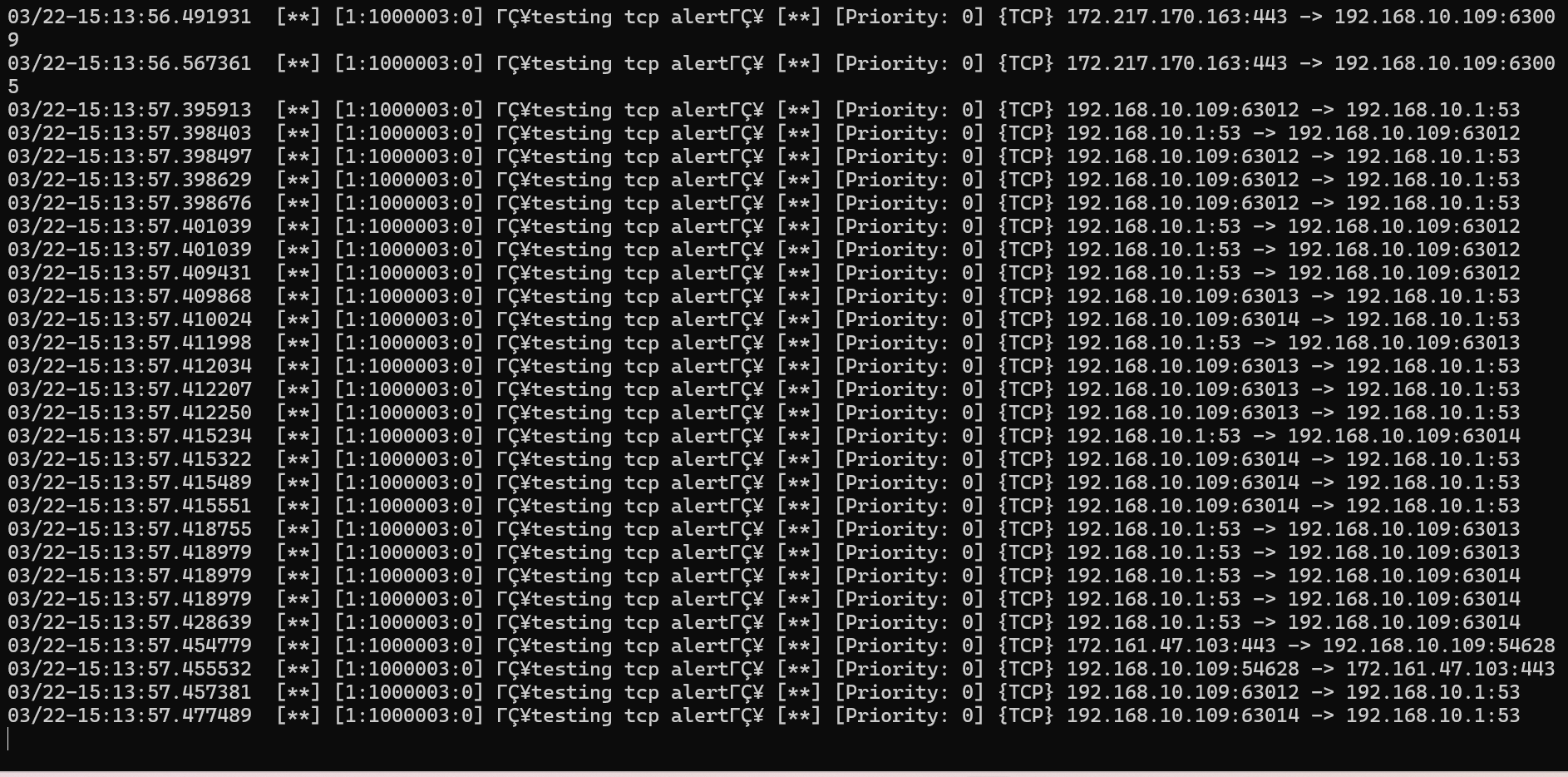
1. **Checking white.list and black.list are exit**



1. Create Local.rules file for protection

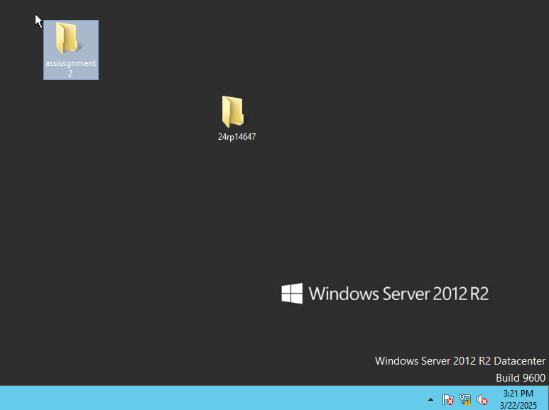
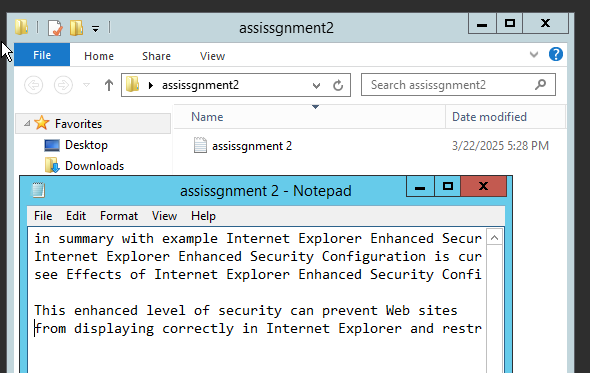


1. Snort -i 4 -c c:\snort\etc\snort.conf -A console for checking service

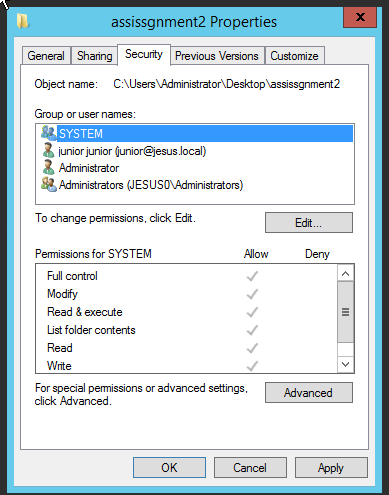
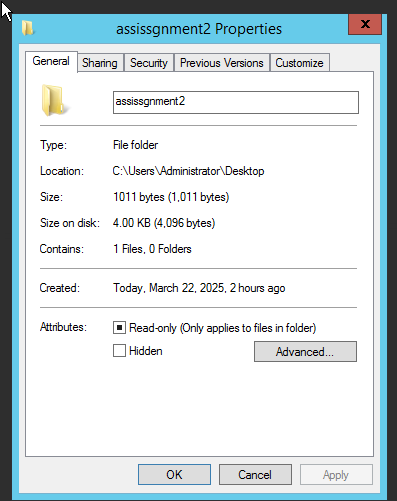


1. RBAC/window server, describe the best practices measures to implement for protection of information.
2. Create a folder and create file use to protect

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

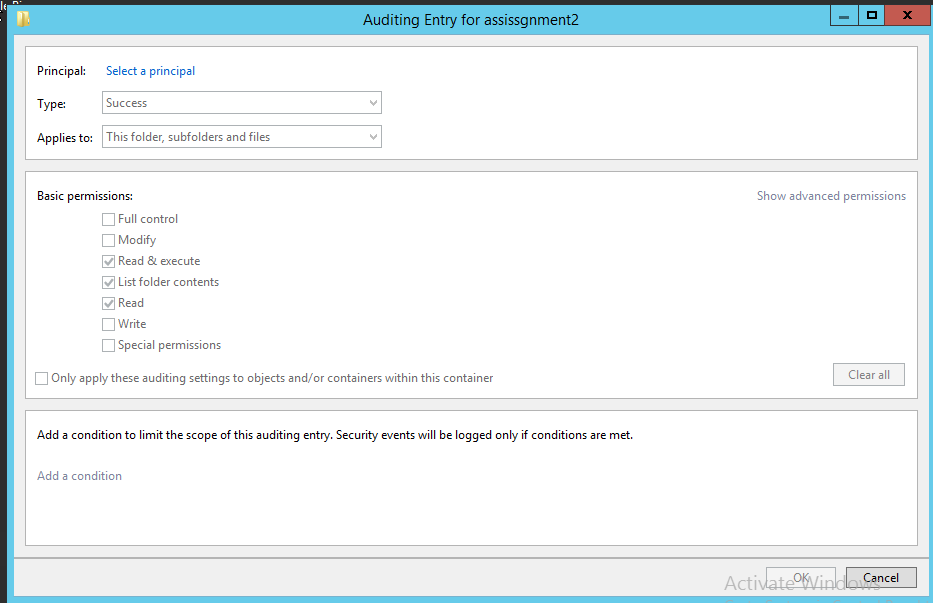
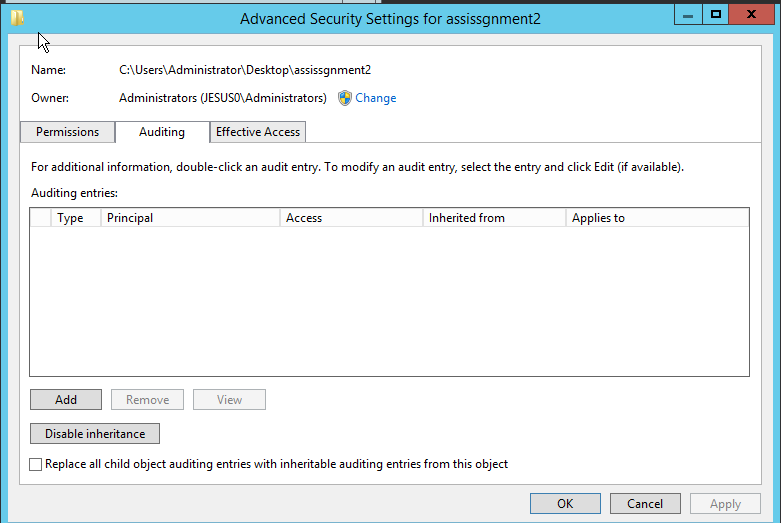
 

1. Selection on folder for security and permission to the users:
2. Now I was select assessgnment2 and make it as right click, select advance for separating user access and select security

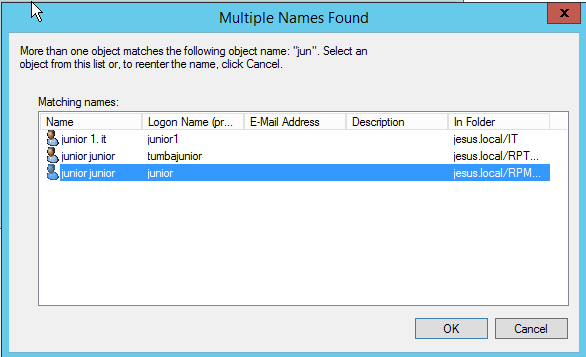
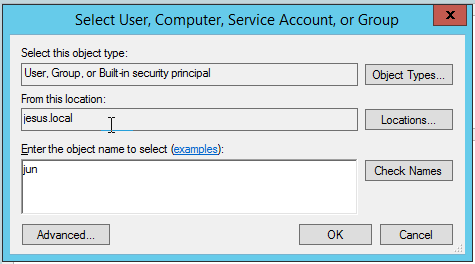


1. This a picture that show user access now select auditing and add users want toaccess and select principle

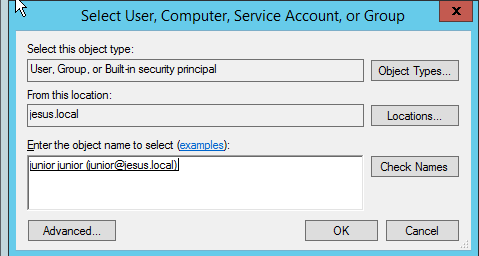
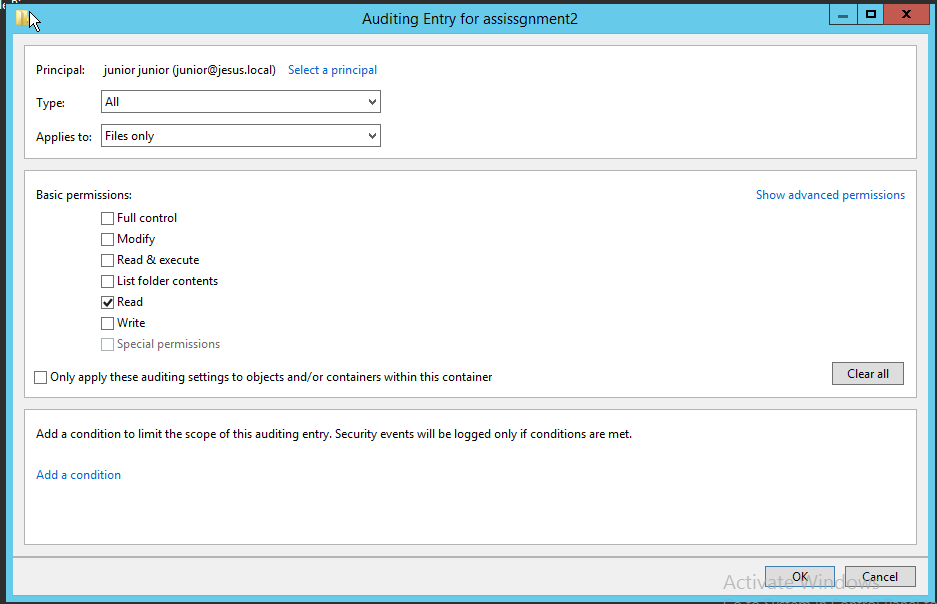
* Read
* Read and execute
* Read folder content



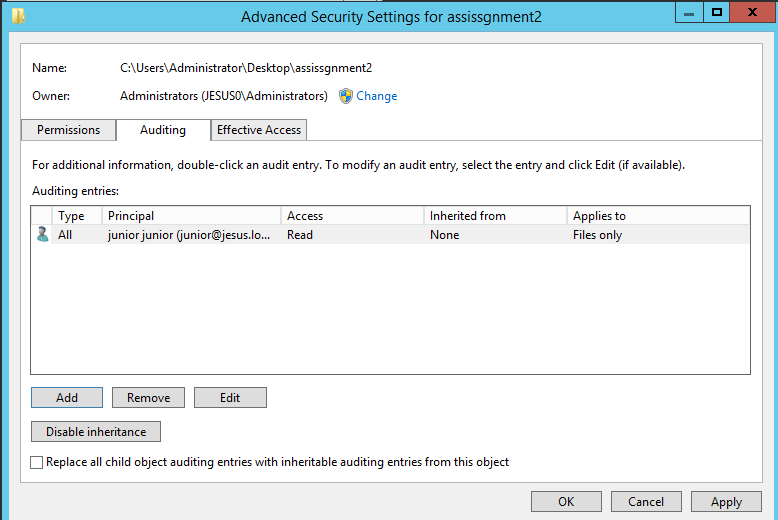
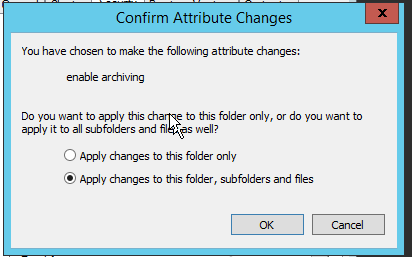
1. Example of user used as junior has select from user list



1. After select [junior@jesus.local](mailto:junior@jesus.local) now has access for read only

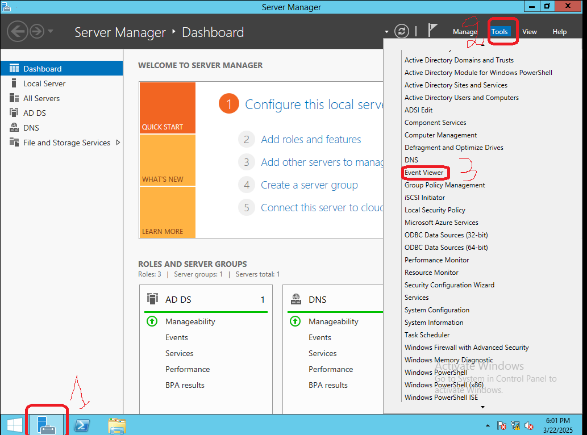
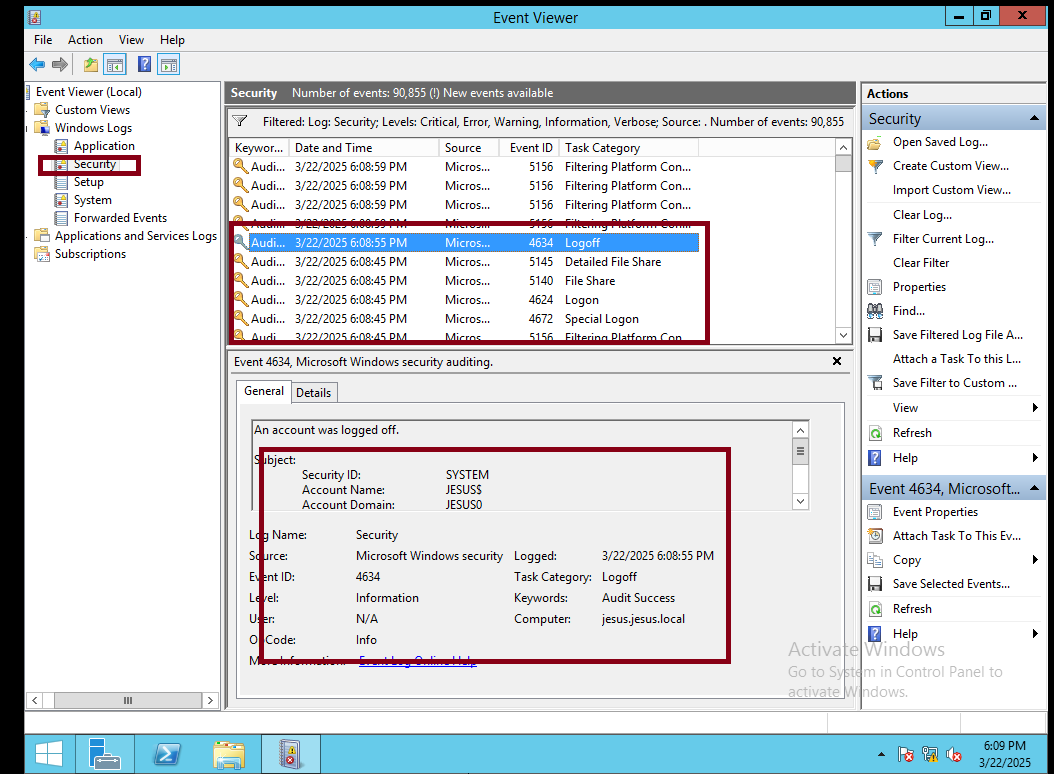
1. Conform that permission rules

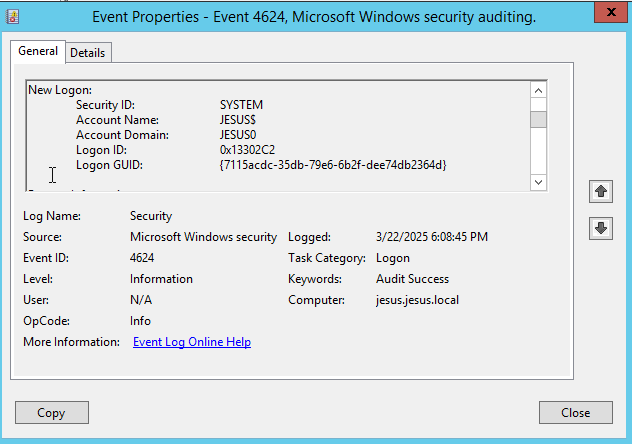
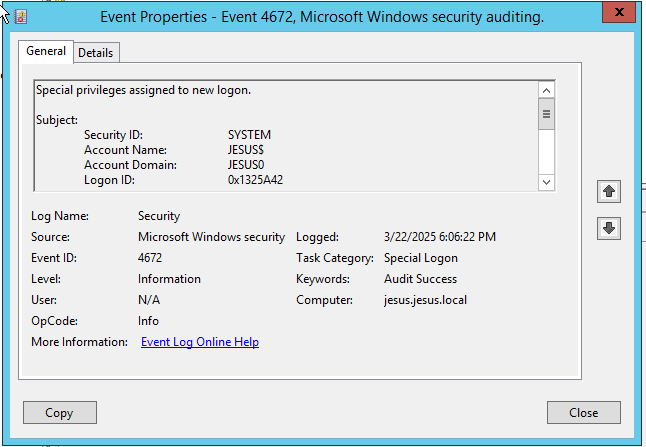
1. Review event

Now I open server manager for control user logon

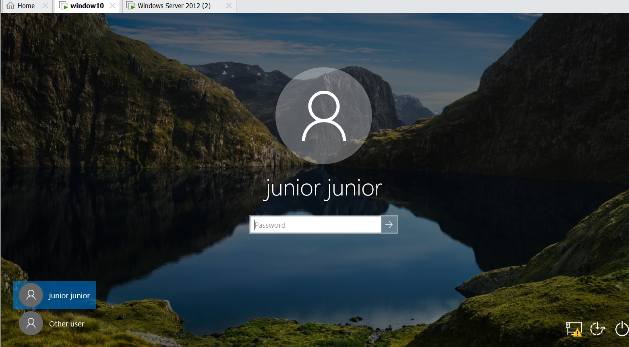
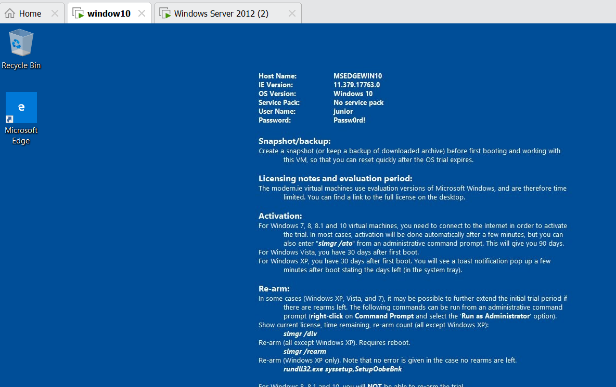
First open tools select security open event logon select logon event that has event id 4624

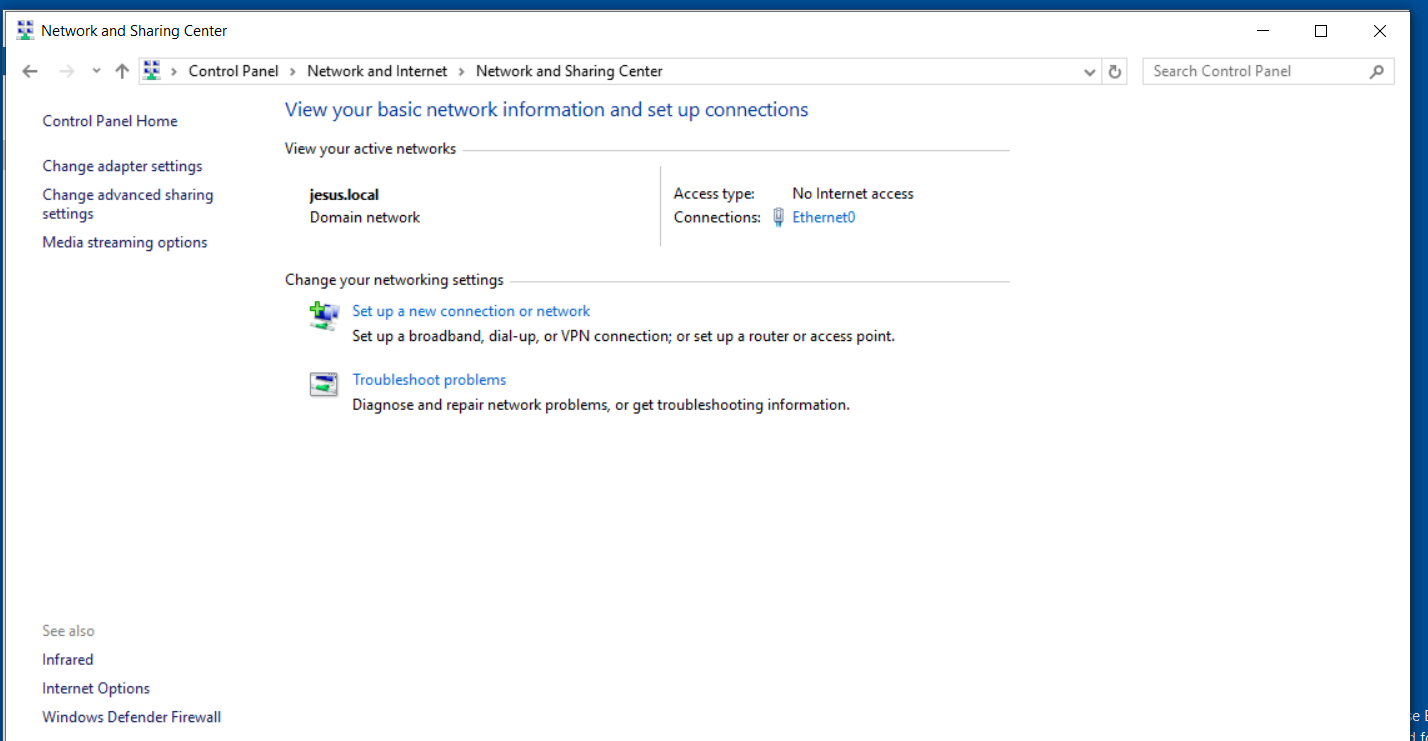
This all detail of jesus user where recording when , what and where she logon

1. Login with window 10

1. 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.



1. After connected to domain check permission

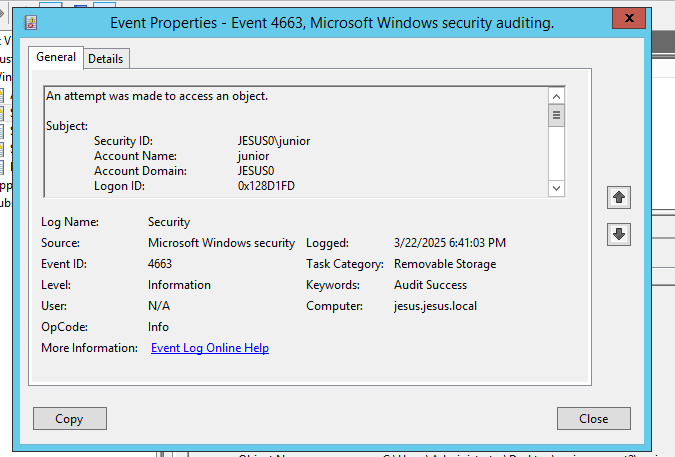


Figure 1: this a record where junion try to make login using domain name