Domain 04 Demo 07

Using Event Viewer to Implement Logging and Forensic Analysis

Objective: To implement logging and forensic analysis using Event Viewer for maintaining a secure and well-monitored network environment

Tools required: Windows Server 2022

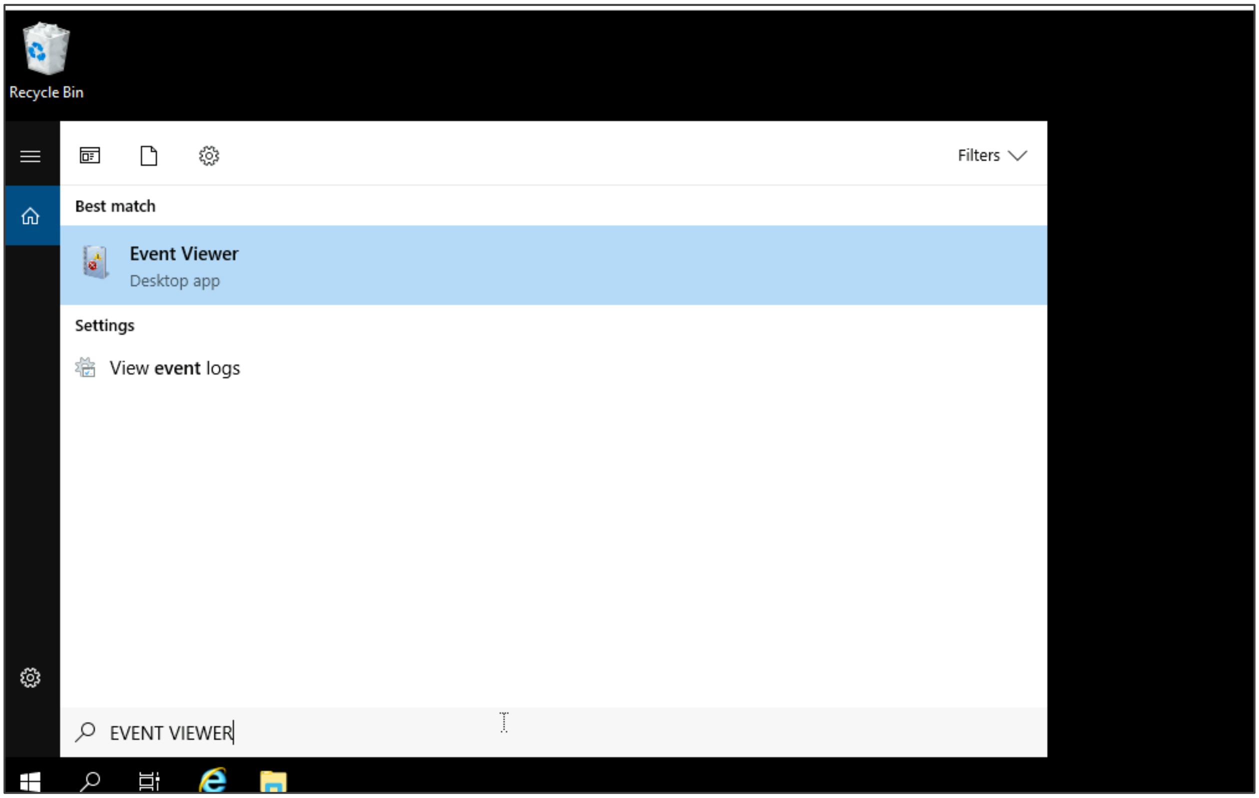
Prerequisites: None

Steps to be followed:

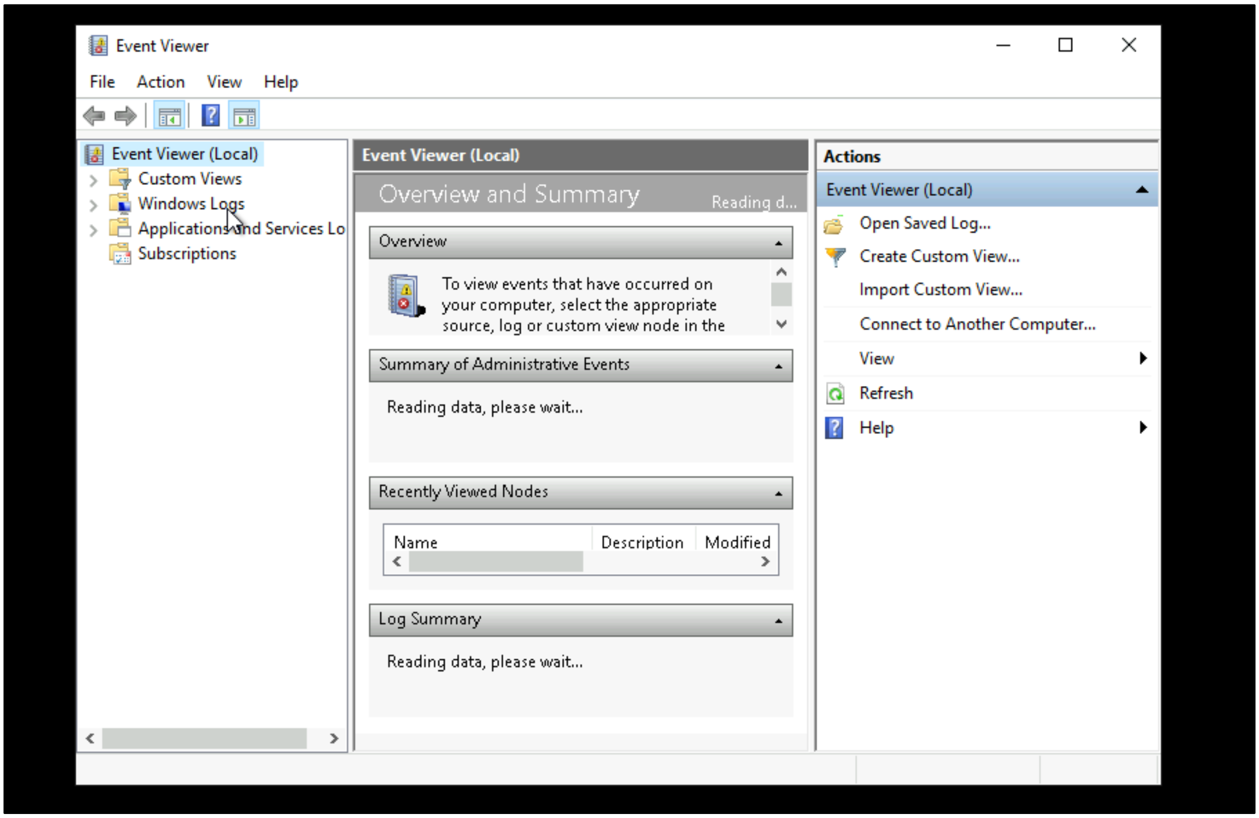
1. Use Event Viewer to view successful and failed login
2. Set up a group policy to log the failed login attempts
3. Create a user and add it to the administrator group
4. View the port status and name resolution using netstat and nslookup

Step 1: Use Event Viewer to view successful and failed login

1.1 Search for and select **Event Viewer** on Windows



1.2 On the **Event Viewer** page, click on **Windows Logs** from the left navigation pane

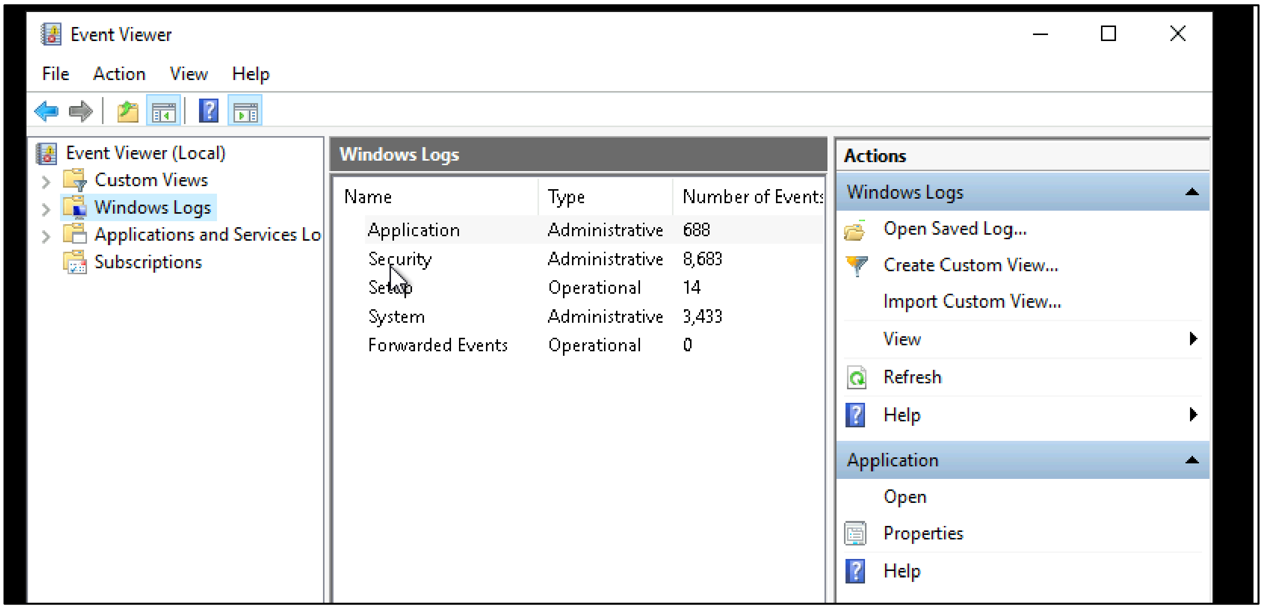


To view events that have occurred on your computer, select the appropriate source, log or custom view node in the

Reading data, please wait...

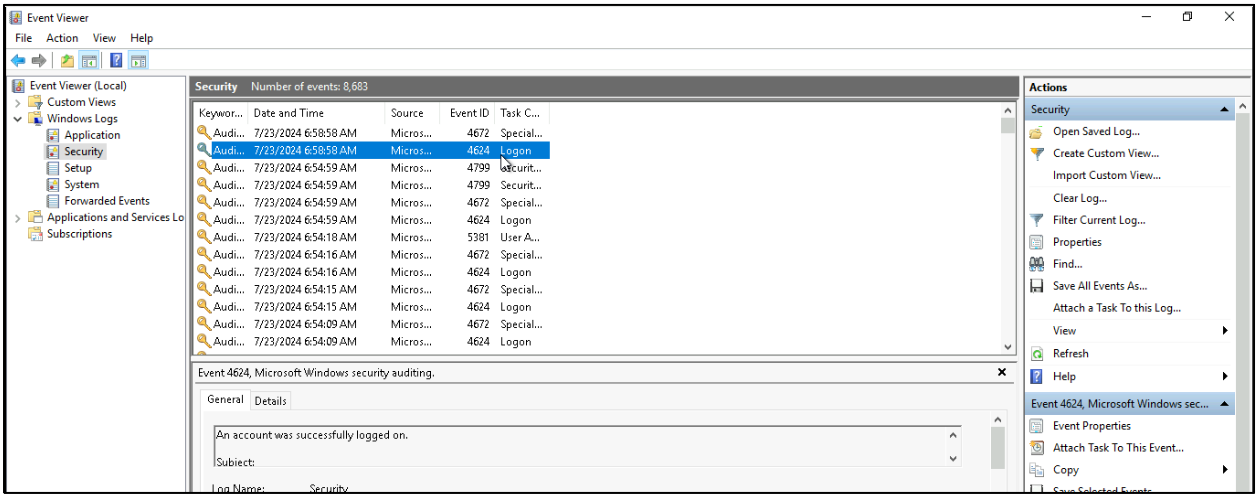
Reading data, please wait...

1.3 Now, click on **Security**



Name	Type	Number of Events
Application	Administrative	688
Security	Administrative	8,683
Setup	Operational	14
System	Administrative	3,433
Forwarded Events	Operational	0

1.4 Click on the specific log as shown in the below screenshot:



Security Number of events: 8,683

Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	7/23/2024 6:58:58 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:58:58 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:59 AM	Micros...	4799	Securit...
Audi...	7/23/2024 6:54:59 AM	Micros...	4799	Securit...
Audi...	7/23/2024 6:54:59 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:54:59 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:18 AM	Micros...	5381	User A...
Audi...	7/23/2024 6:54:16 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:54:16 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:15 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:54:15 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:09 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:54:09 AM	Micros...	4624	Logon

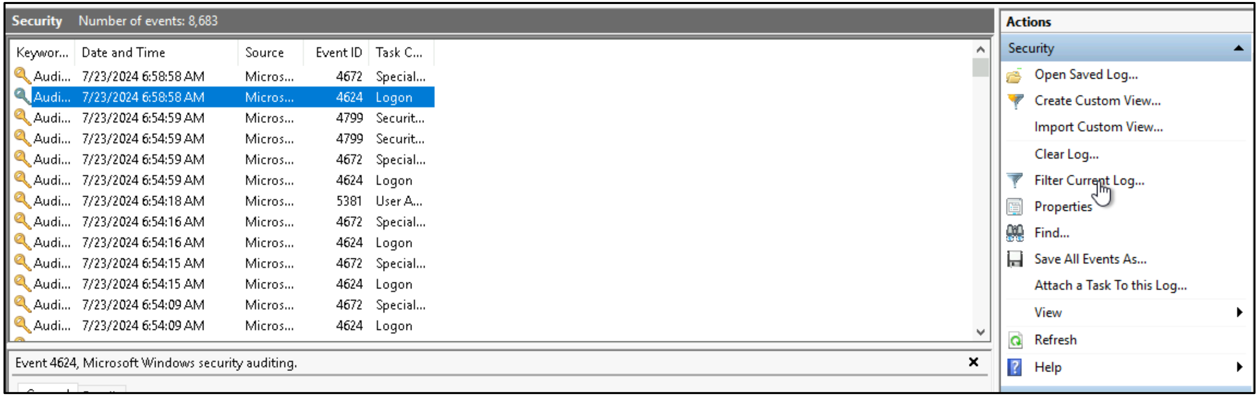
Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:

Log Name: Security

1.5 Now, click on **Filter Current Log** to filter the logs

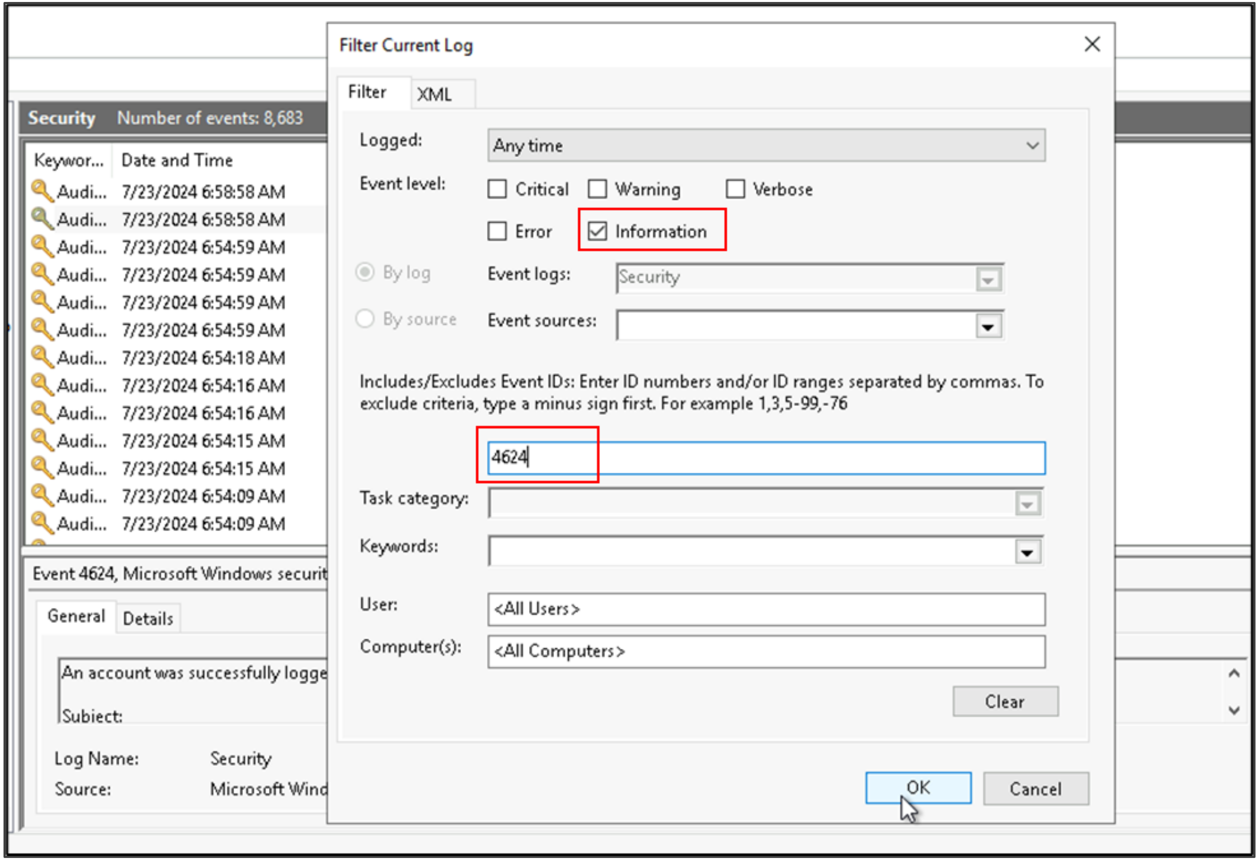


Security Number of events: 8,683

Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	7/23/2024 6:58:58 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:58:58 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:59 AM	Micros...	4799	Securit...
Audi...	7/23/2024 6:54:59 AM	Micros...	4799	Securit...
Audi...	7/23/2024 6:54:59 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:54:59 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:18 AM	Micros...	5381	User A...
Audi...	7/23/2024 6:54:16 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:54:16 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:15 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:54:15 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:09 AM	Micros...	4672	Special...
Audi...	7/23/2024 6:54:09 AM	Micros...	4624	Logon

Event 4624, Microsoft Windows security auditing.

1.6 Select **Information** as the Event level, add the Event ID, and then click on **OK**



Security   Number of events: 8,683

Keywor...	Date and Time
Audi...	7/23/2024 6:58:58 AM
Audi...	7/23/2024 6:58:58 AM
Audi...	7/23/2024 6:54:59 AM
Audi...	7/23/2024 6:54:59 AM
Audi...	7/23/2024 6:54:59 AM
Audi...	7/23/2024 6:54:59 AM
Audi...	7/23/2024 6:54:18 AM
Audi...	7/23/2024 6:54:16 AM
Audi...	7/23/2024 6:54:16 AM
Audi...	7/23/2024 6:54:15 AM
Audi...	7/23/2024 6:54:15 AM
Audi...	7/23/2024 6:54:09 AM
Audi...	7/23/2024 6:54:09 AM

Event 4624, Microsoft Windows securit

General   Details

An account was successfully logge

Subject:

Log Name: Security

Source: Microsoft Wind

Filter Current Log

Filter   XML

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error ☑ Information

○ By log   Event logs: Security

○ By source   Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4624

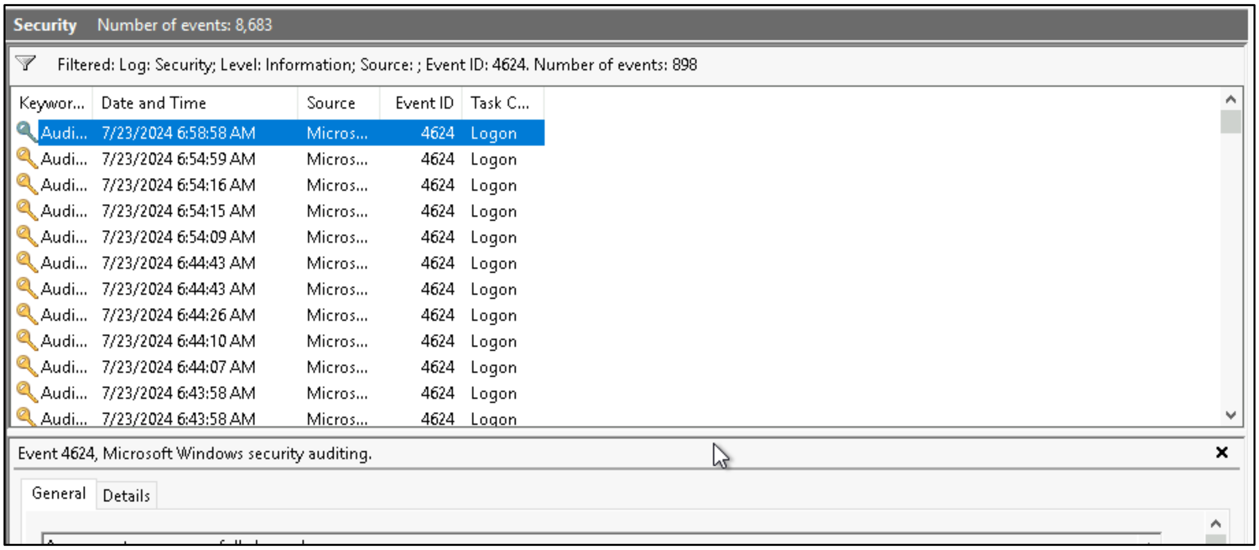
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

All the events with successful logins are displayed.



Security   Number of events: 8,683

Filtered: Log: Security; Level: Information; Source: ; Event ID: 4624. Number of events: 898

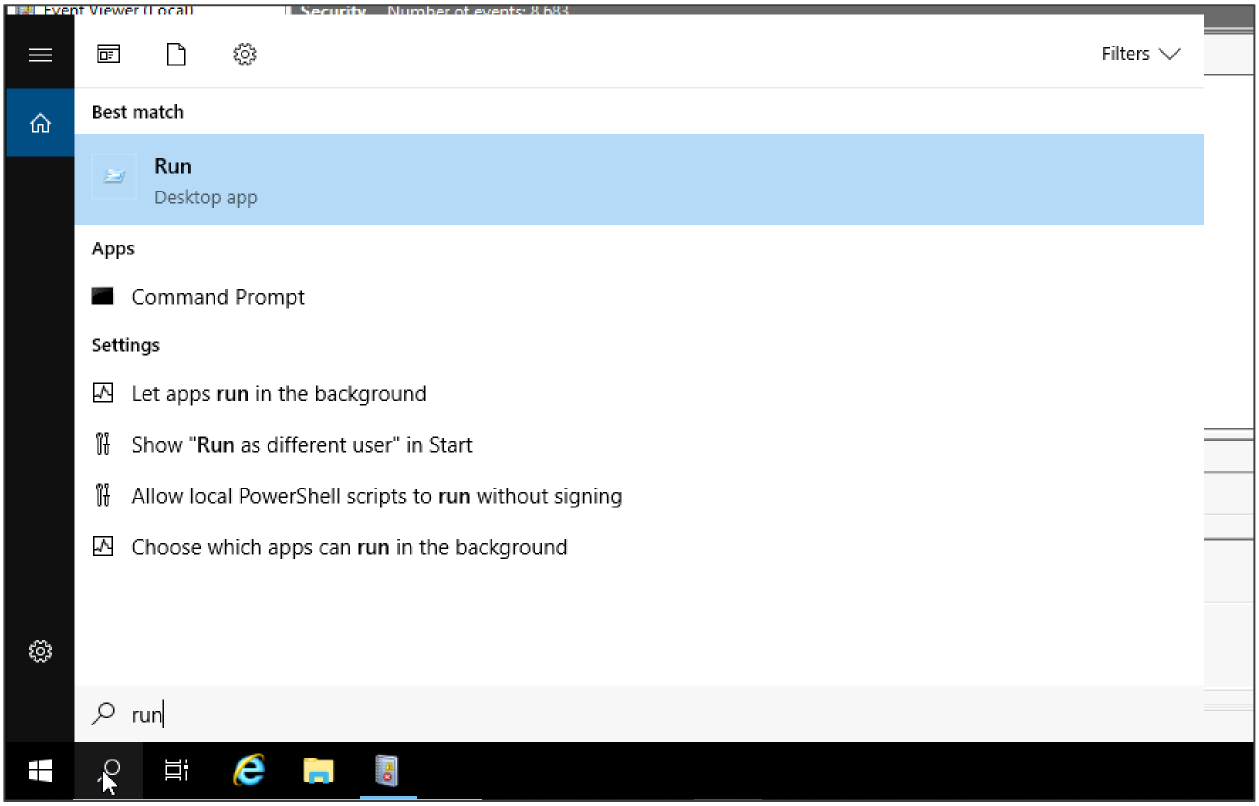
Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	7/23/2024 6:58:58 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:59 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:16 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:15 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:54:09 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:44:43 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:44:43 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:44:26 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:44:10 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:44:07 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:43:58 AM	Micros...	4624	Logon
Audi...	7/23/2024 6:43:58 AM	Micros...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General   Details

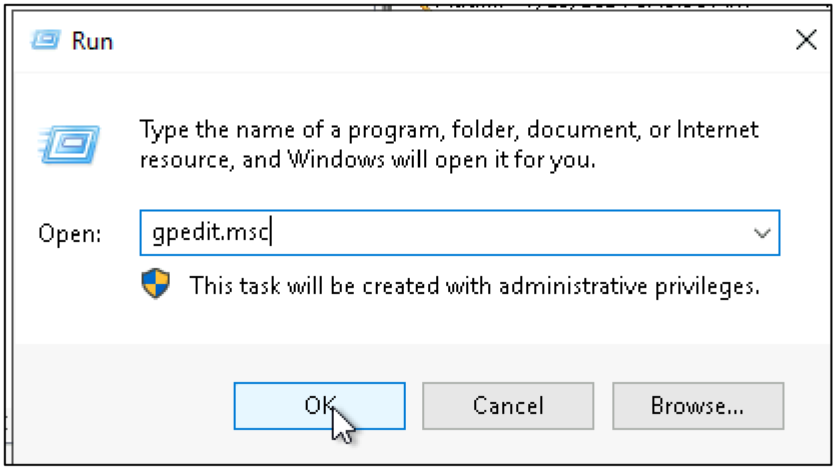
Step 2: Set up a group policy to log the failed login attempts

2.1 Search for and select **Run** on Windows


Event Viewer (Local)
Security Number of events: 8,683
Filters
Best match
Run
Desktop app
Apps
Command Prompt
Settings
Let apps run in the background
Show "Run as different user" in Start
Allow local PowerShell scripts to run without signing
Choose which apps can run in the background

run

2.2 Enter **gpedit.msc** in the **Open** field and click on **OK**

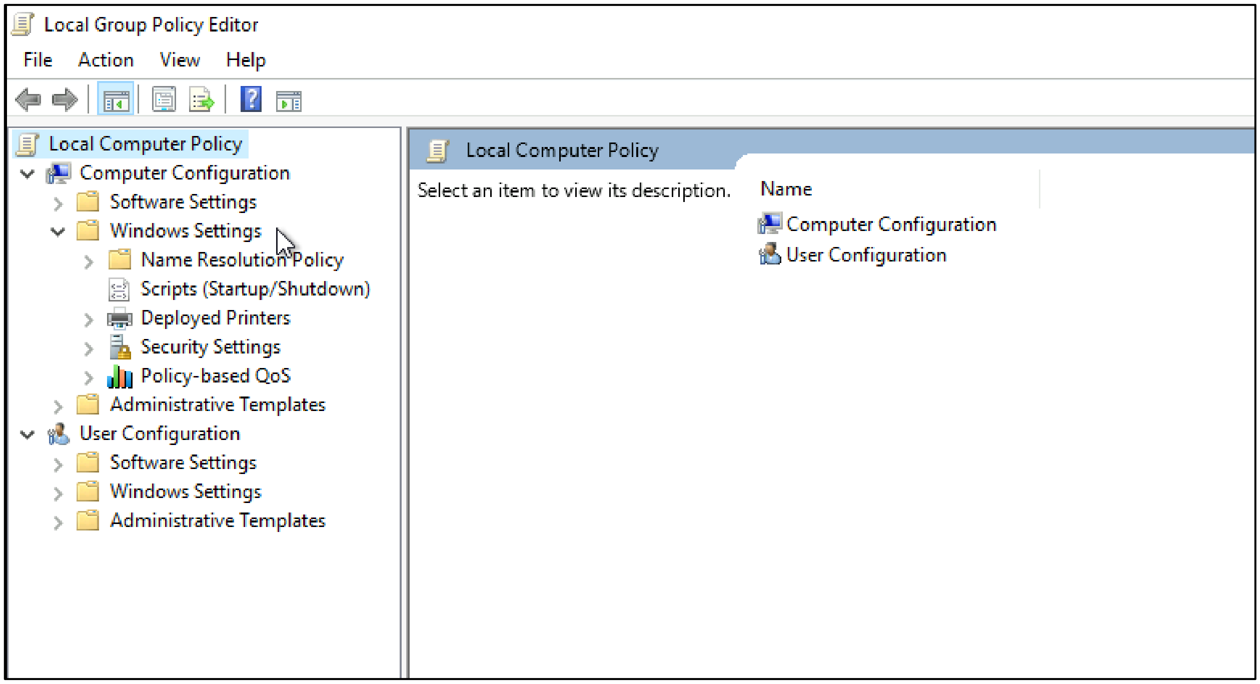


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

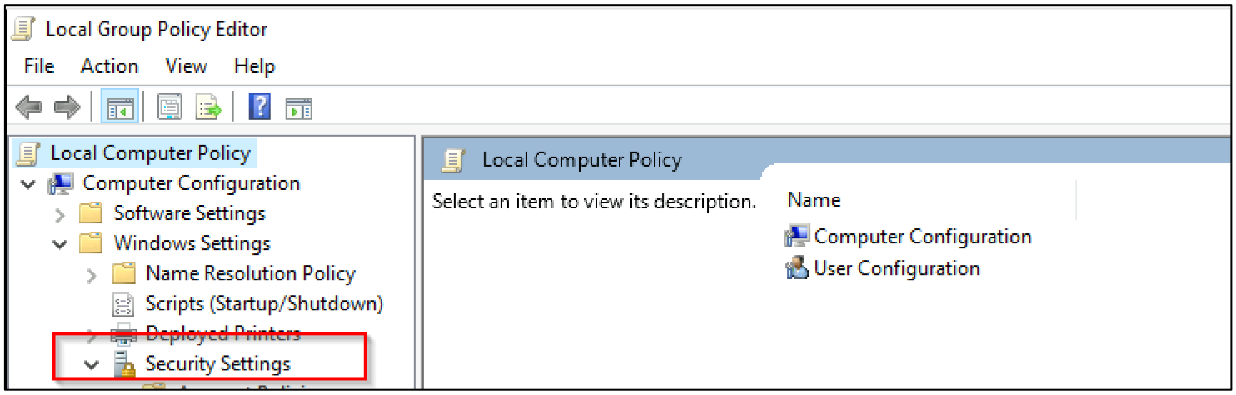
Open: gpedit.msc

This task will be created with administrative privileges.

2.3 On the **Local Computer Policy** page, expand the **Windows Settings** folder in the left navigation pane, and then click on **Security Settings**

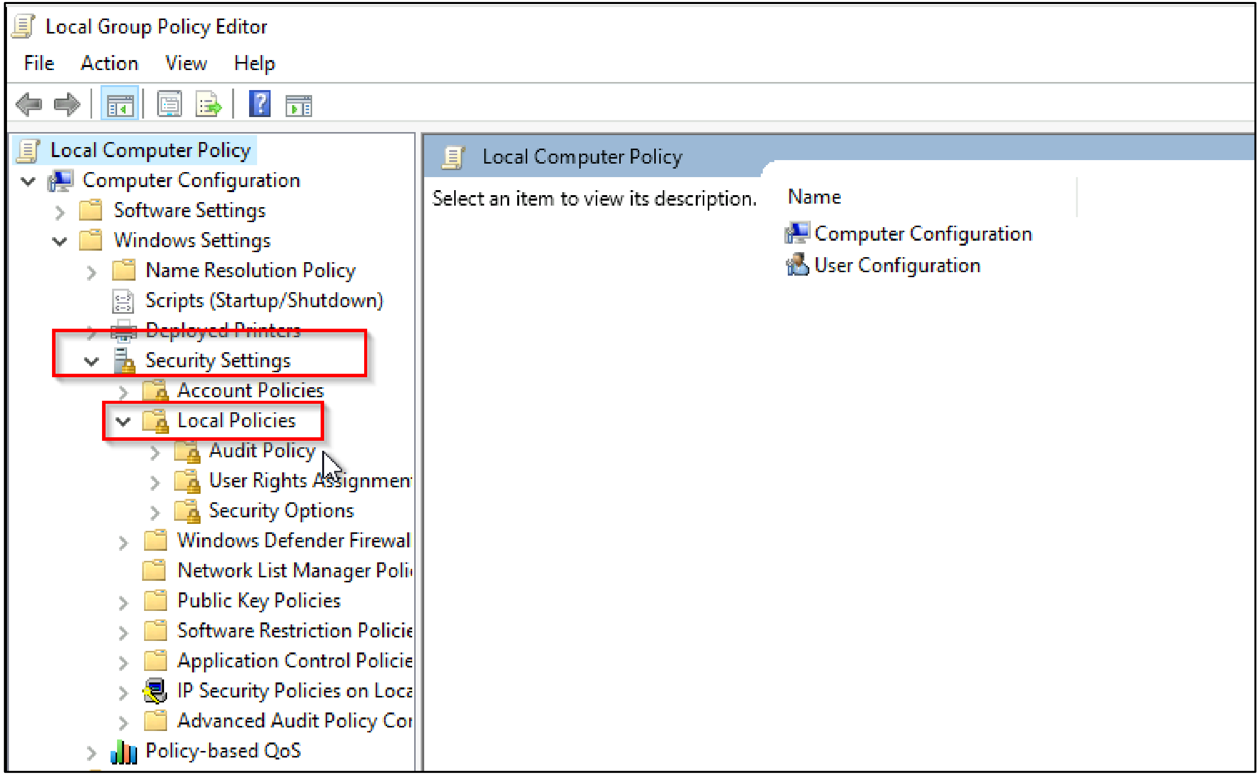


Select an item to view its description.

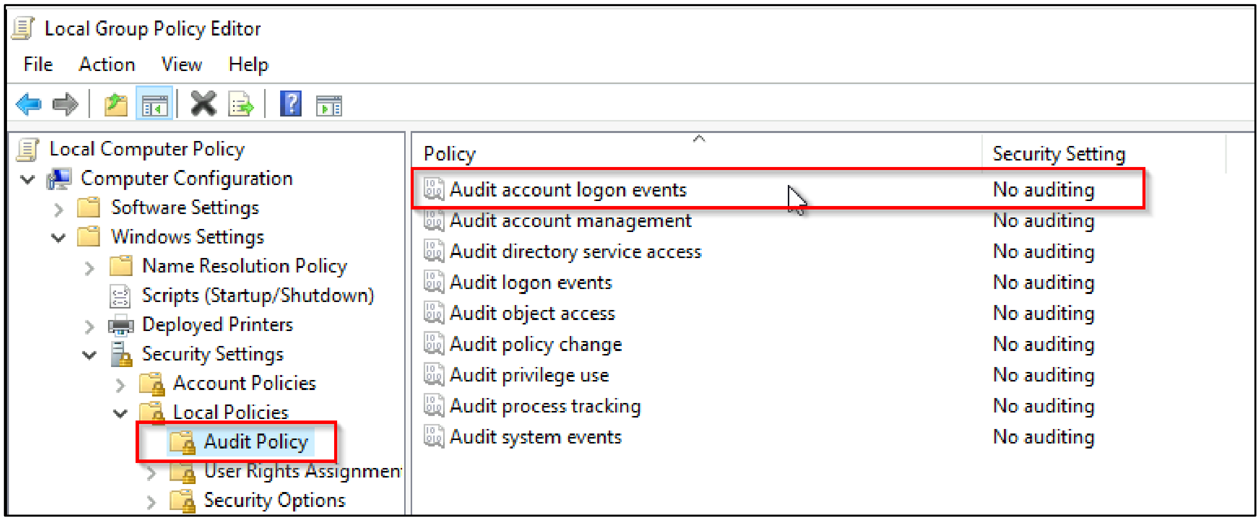


Select an item to view its description.

2.4 Now, expand the **Security Settings** folder and then click on **Local Policies**

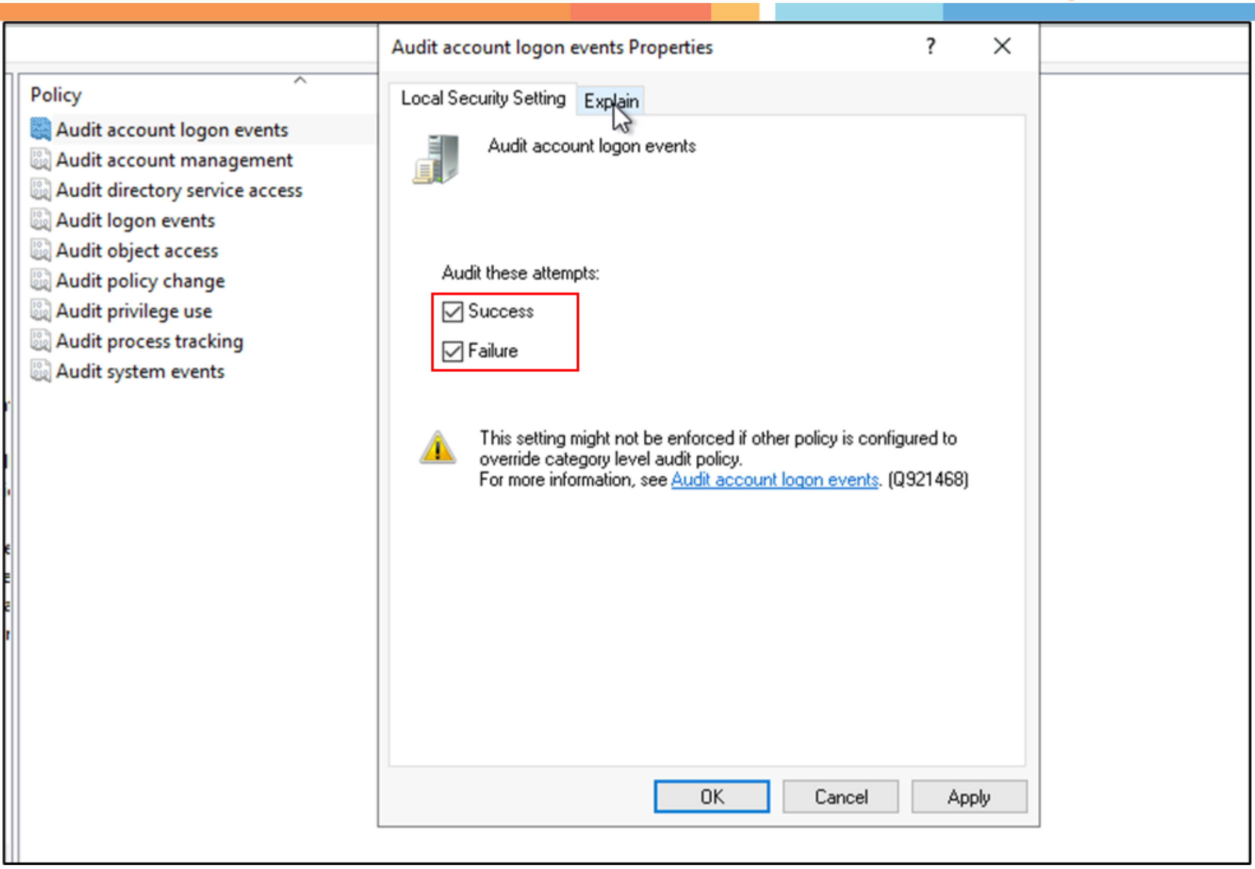


2.5 Click on **Audit Policy** under **Local Policies** and then select **Audit account logon events**



Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

2.6 Mark the checkboxes and then click on **OK**



Audit account logon events Properties

Local Security Setting | Explain

Audit account logon events

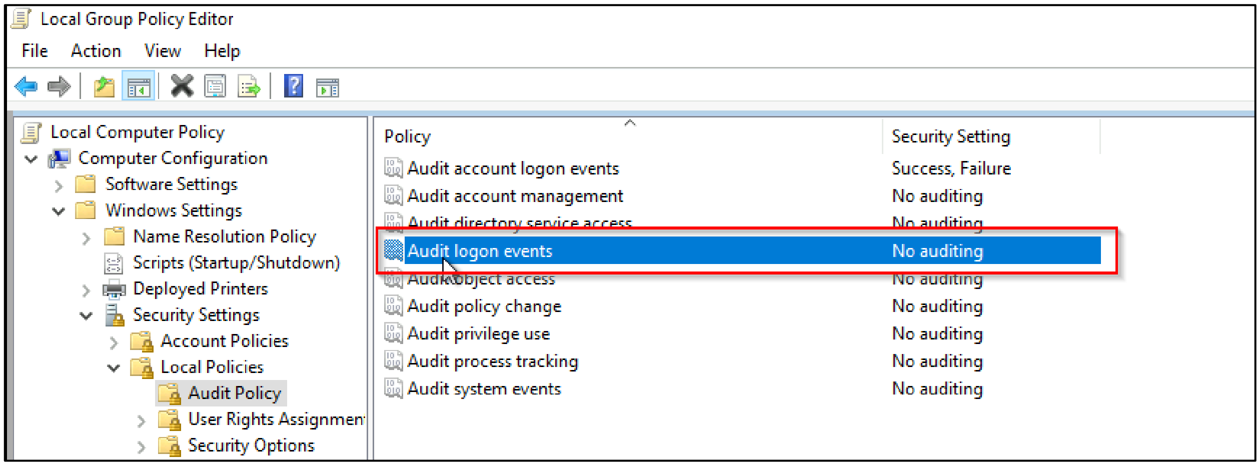
Audit these attempts:

☑ Success

☑ Failure

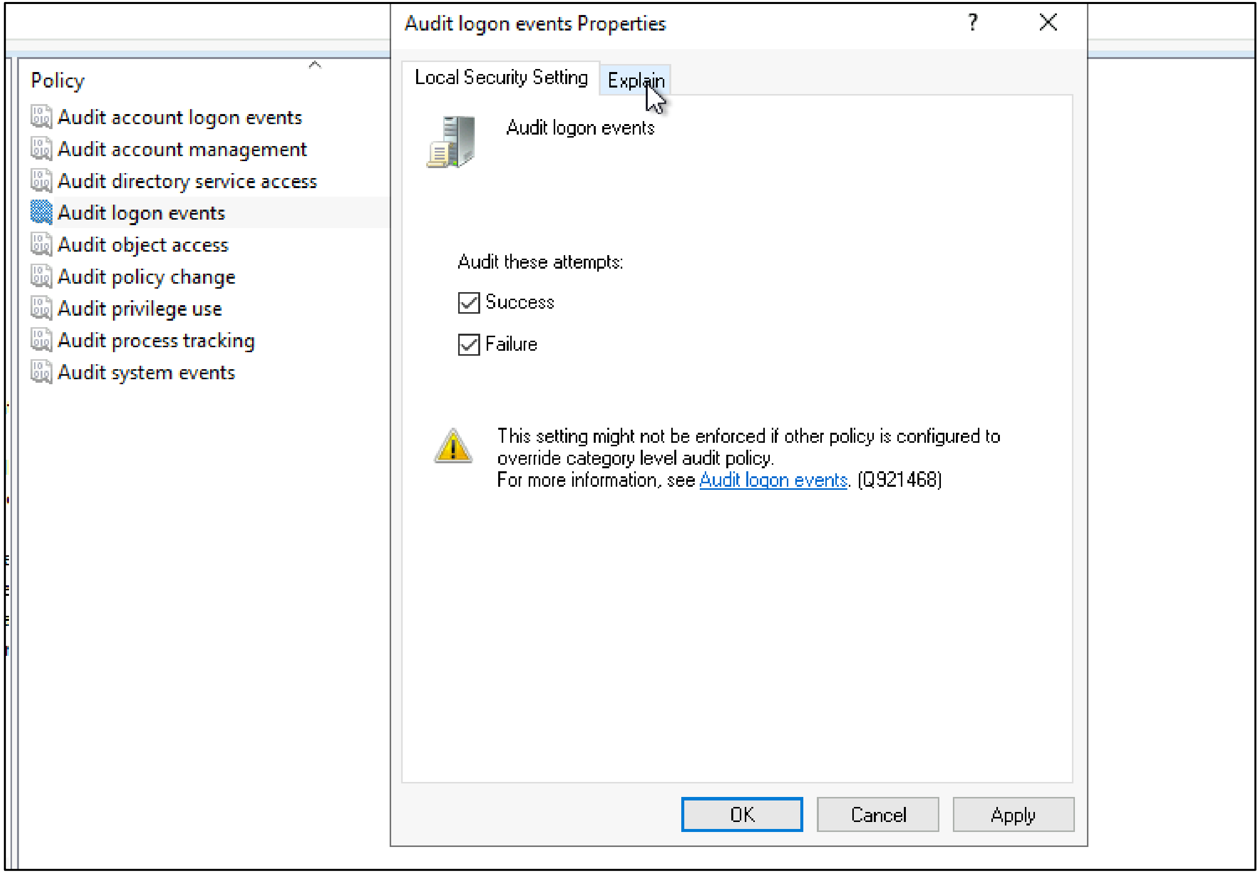
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)

2.7 Now, select the **Audit logon events**, mark the checkboxes, and then click on **OK**



Local Group Policy Editor

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing



Audit logon events Properties

Audit logon events

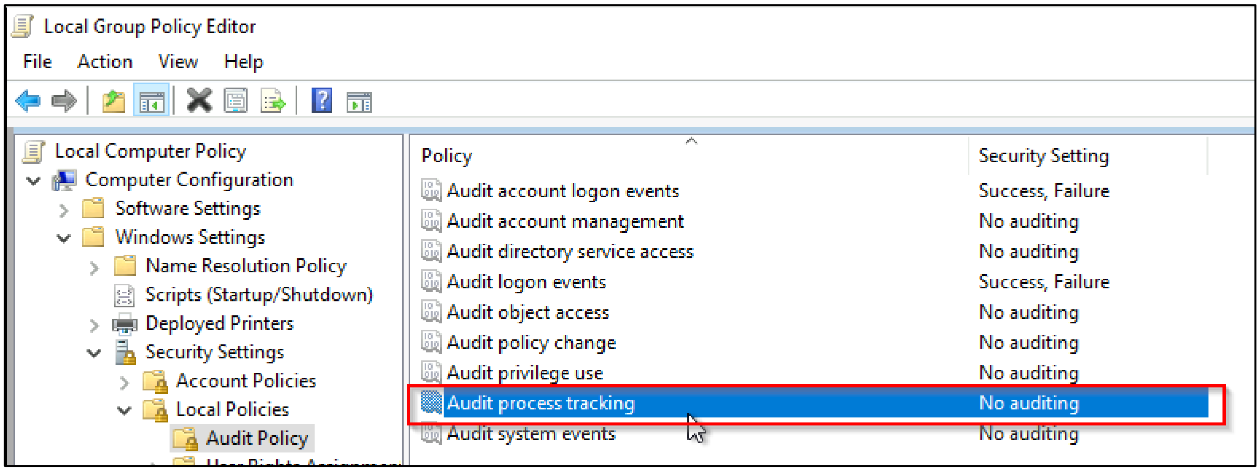
Audit these attempts:

☑ Success

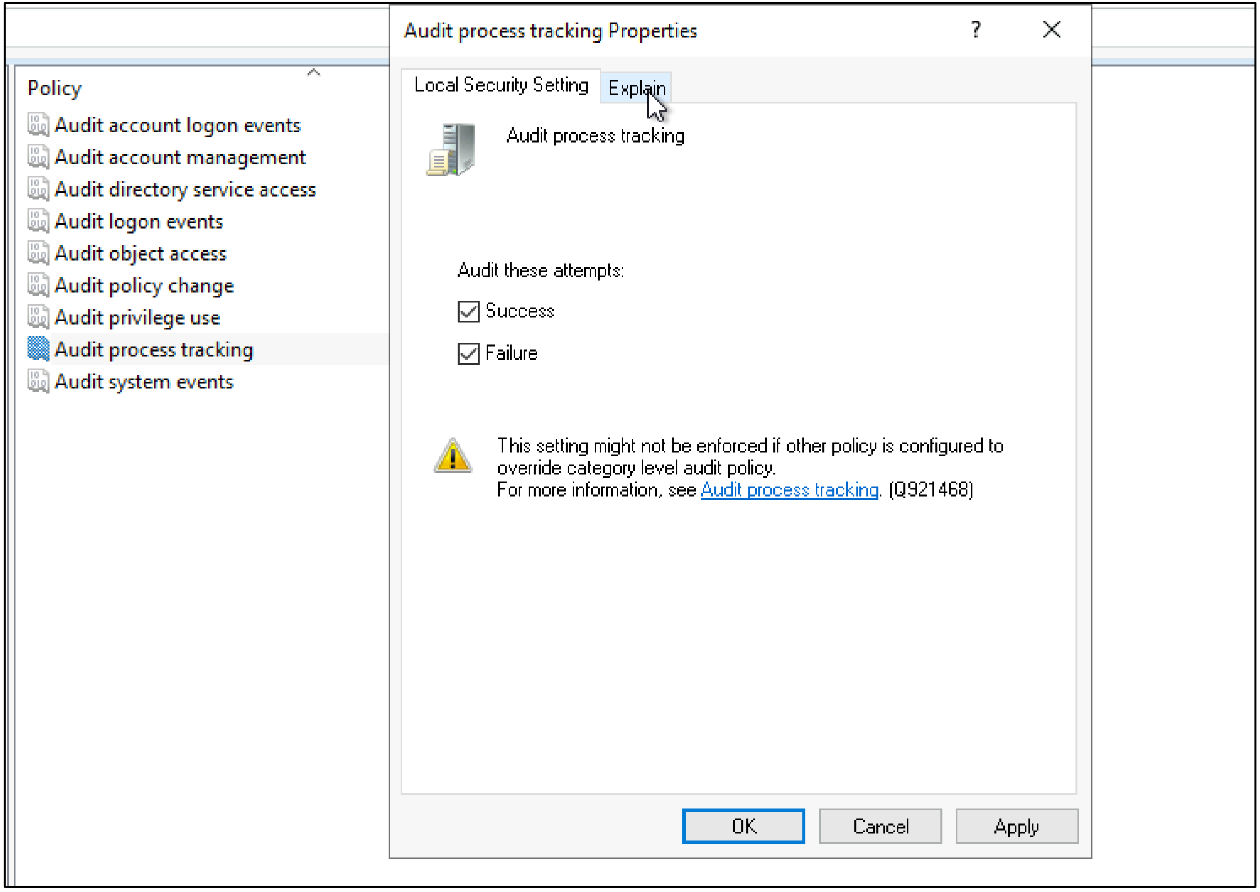
☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit logon events. (Q921468)

2.8 Now, select **Audit process tracking**, mark the checkboxes, and then click on **OK**



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing



Audit process tracking Properties

Local Security Setting | Explain

Audit process tracking

Audit these attempts:

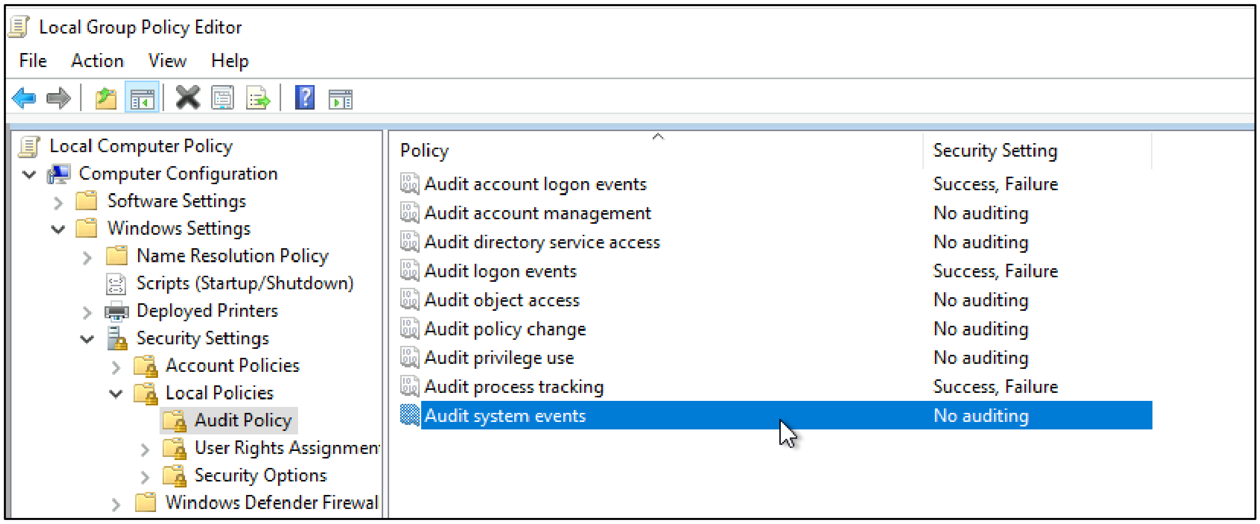
☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit process tracking. (Q921468)

Policy
Audit account logon events
Audit account management
Audit directory service access
Audit logon events
Audit object access
Audit policy change
Audit privilege use
Audit process tracking
Audit system events

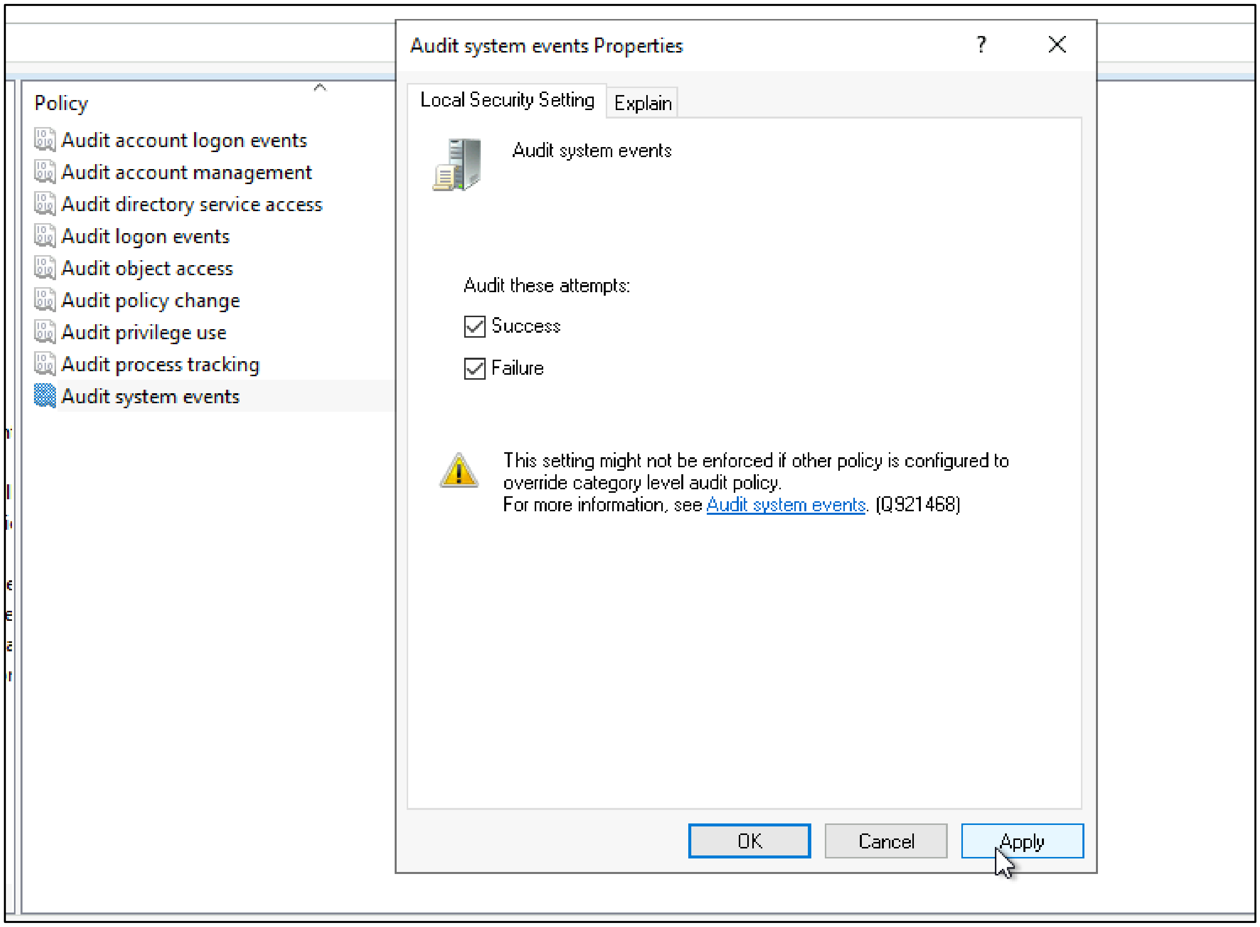
2.9 Finally, select **Audit system events**, mark the checkboxes, and then click on **OK**



Local Group Policy Editor

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignmen
          - Security Options
        - Windows Defender Firewal

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	Success, Failure
Audit system events	No auditing



Audit system events Properties

Policy
- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

Audit system events

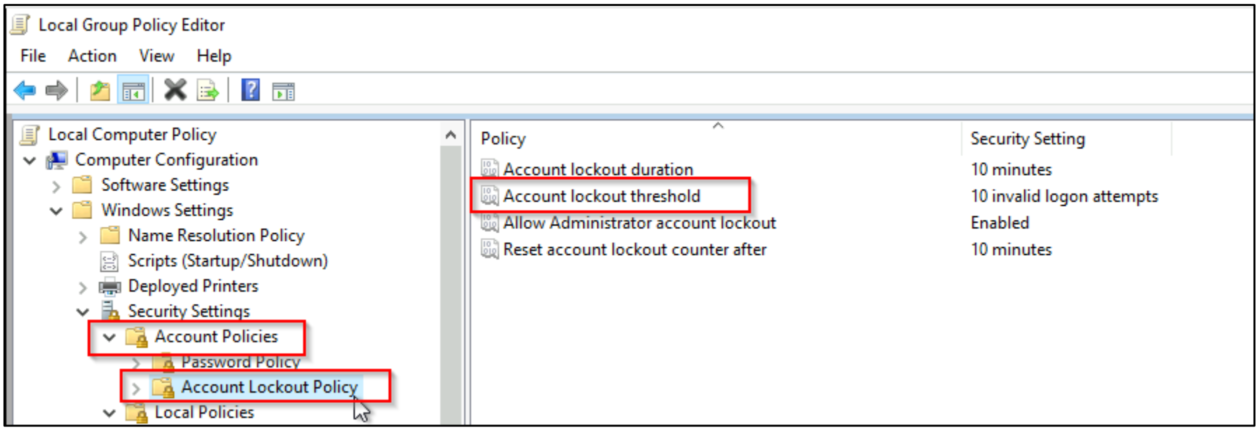
Audit these attempts:

☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit system events. (Q921468)

2.10 Now, expand the **Account Policies** folder from the left navigation pane, click on **Account Lockout Policy**, and then select **Account lockout threshold**

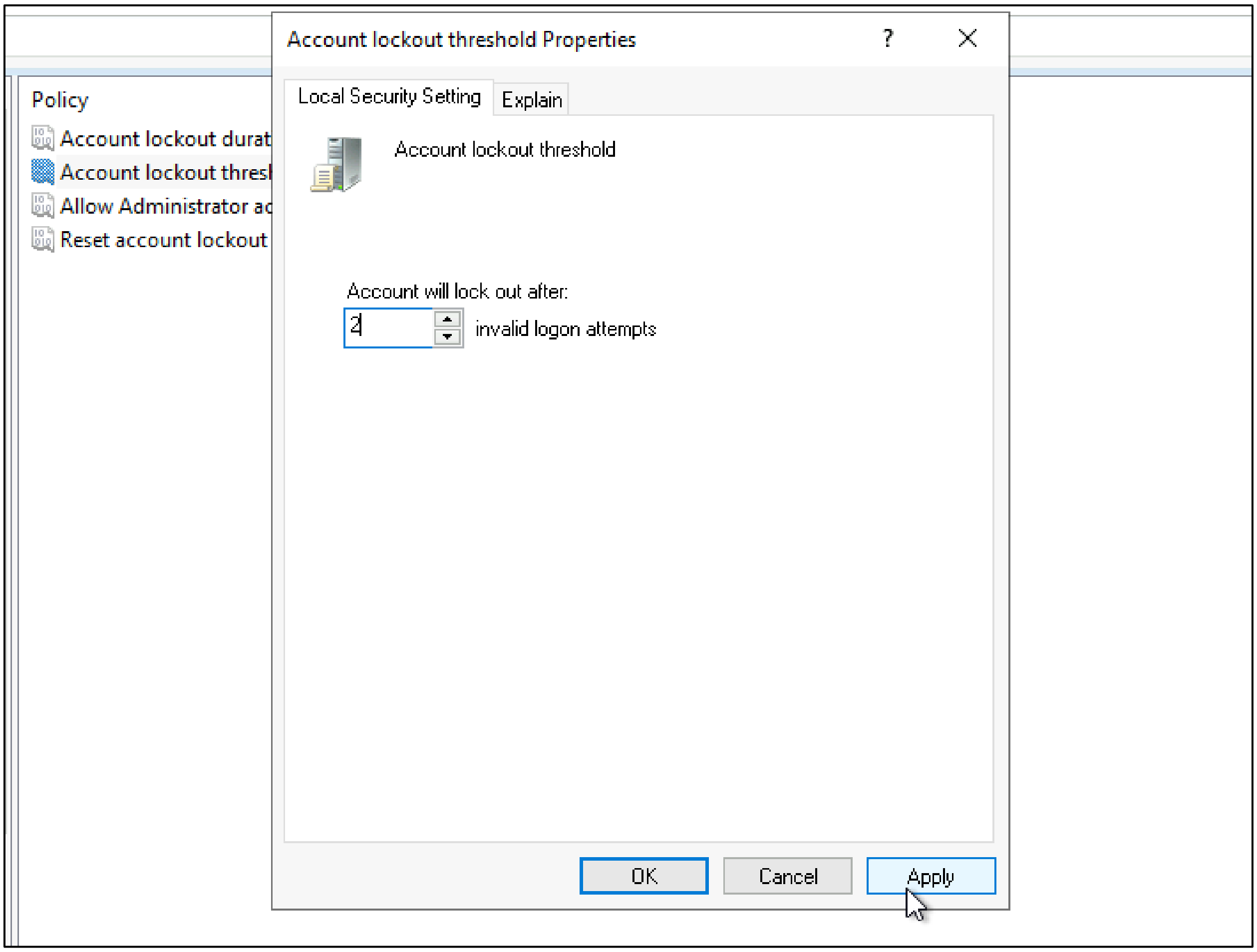


Local Group Policy Editor

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
        - Local Policies

Policy	Security Setting
Account lockout duration	10 minutes
Account lockout threshold	10 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

2.11 Set the lockout threshold to 2 and click on **Apply**

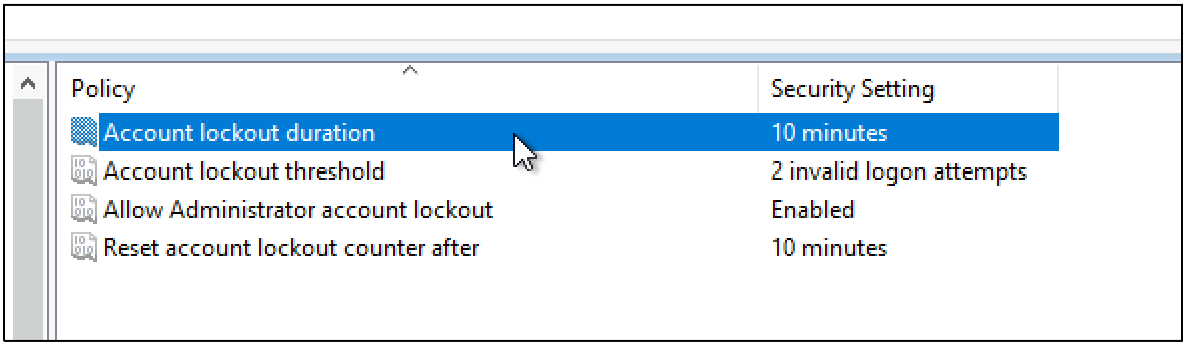

Account lockout threshold Properties

Account lockout threshold

Account will lock out after:

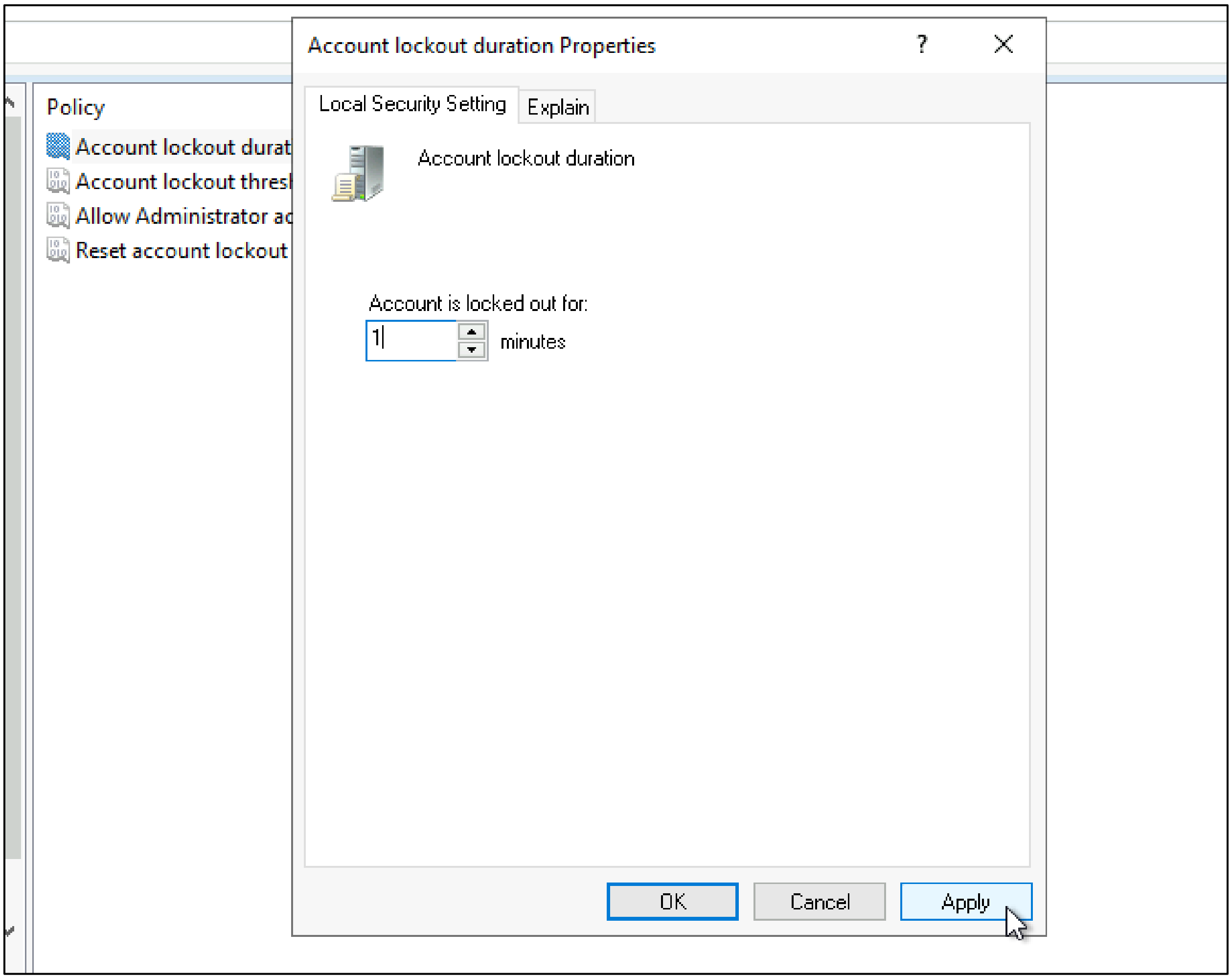
2 invalid logon attempts

2.12 Now, click on **Account lockout duration**



Policy	Security Setting
Account lockout duration	10 minutes
Account lockout threshold	2 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

2.13 Set the duration as 1 minute and click on **Apply**

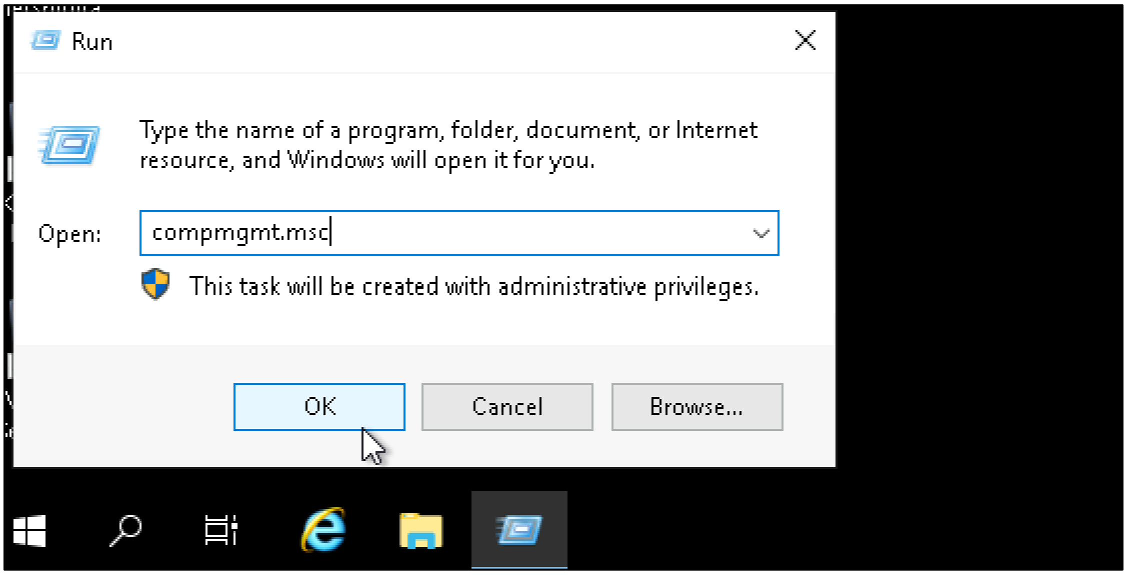


Account lockout duration

Account is locked out for:
1 minutes

Step 3: Create a user and add it to the administrator group

3.1 Navigate back to Run, enter **compmgmt.msc** in the **Open** field, and then click **OK**

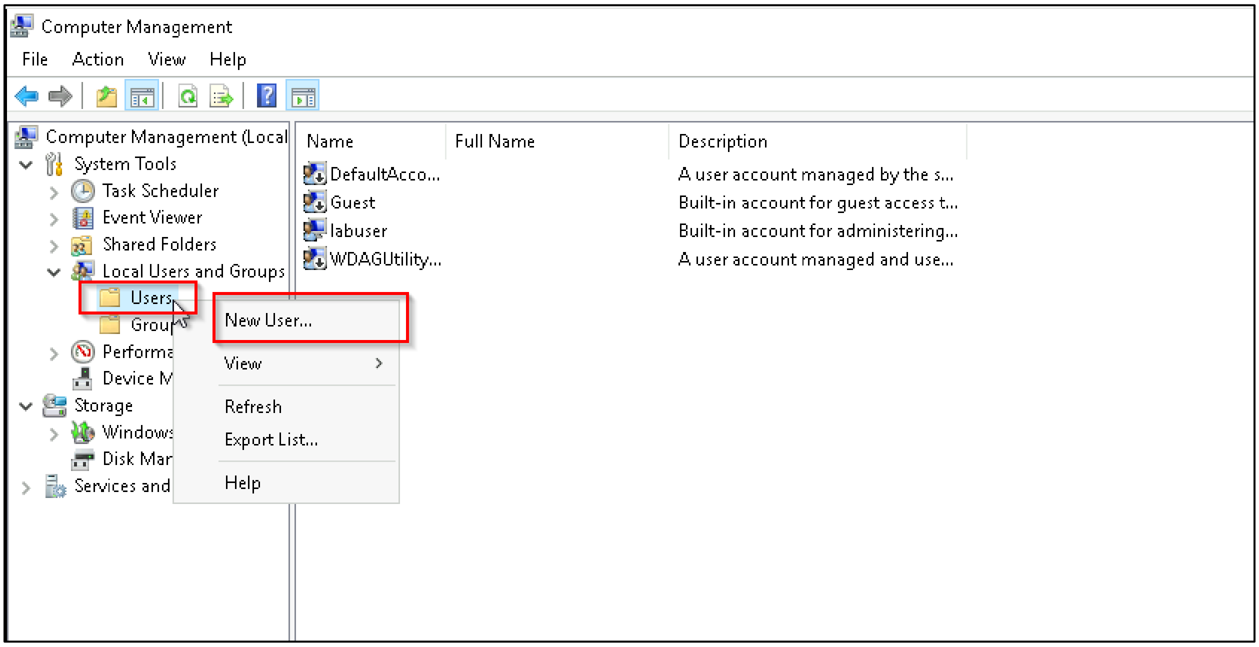


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: compmgmt.msc

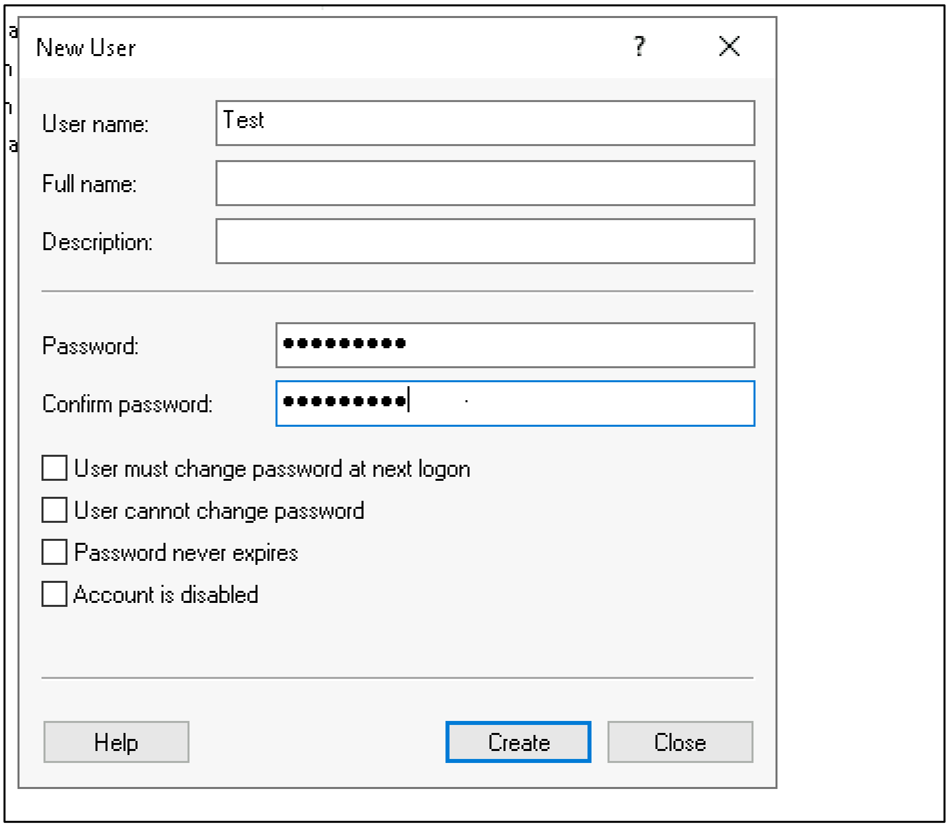
This task will be created with administrative privileges.

3.2 On the Computer Management page, click on **Local Users and Groups**, right-click on **Users**, and then select **New User**



Name	Full Name	Description
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
labuser		Built-in account for administering...
WDAGUtility...		A user account managed and use...

3.3 Provide the username, set its password, and then click on **Create**



User name: Test

Full name:

Description:

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

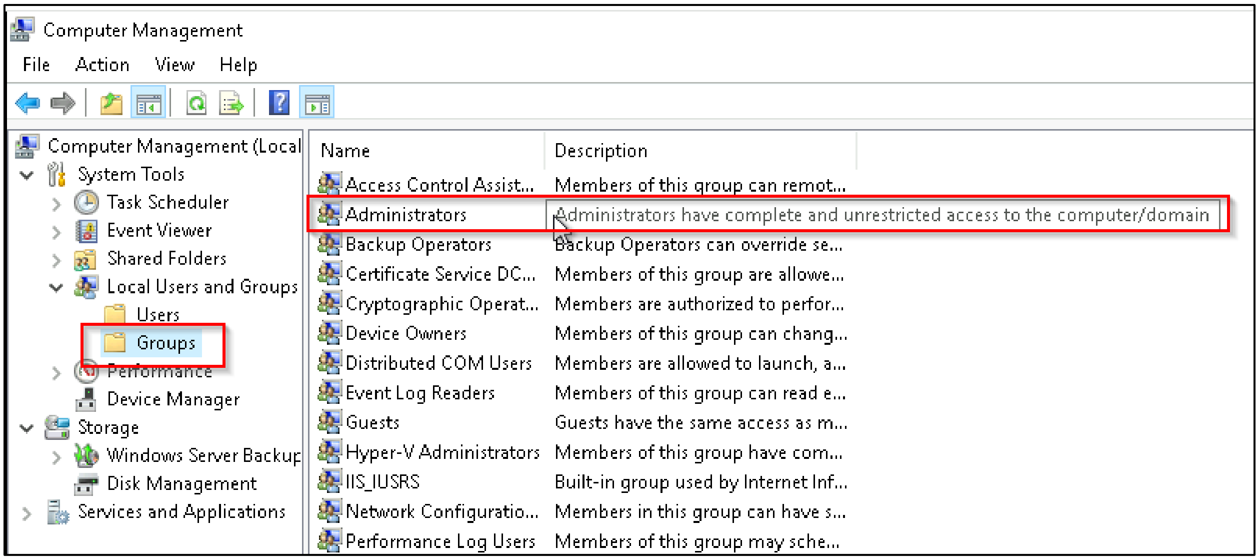
□ User must change password at next logon

□ User cannot change password

□ Password never expires

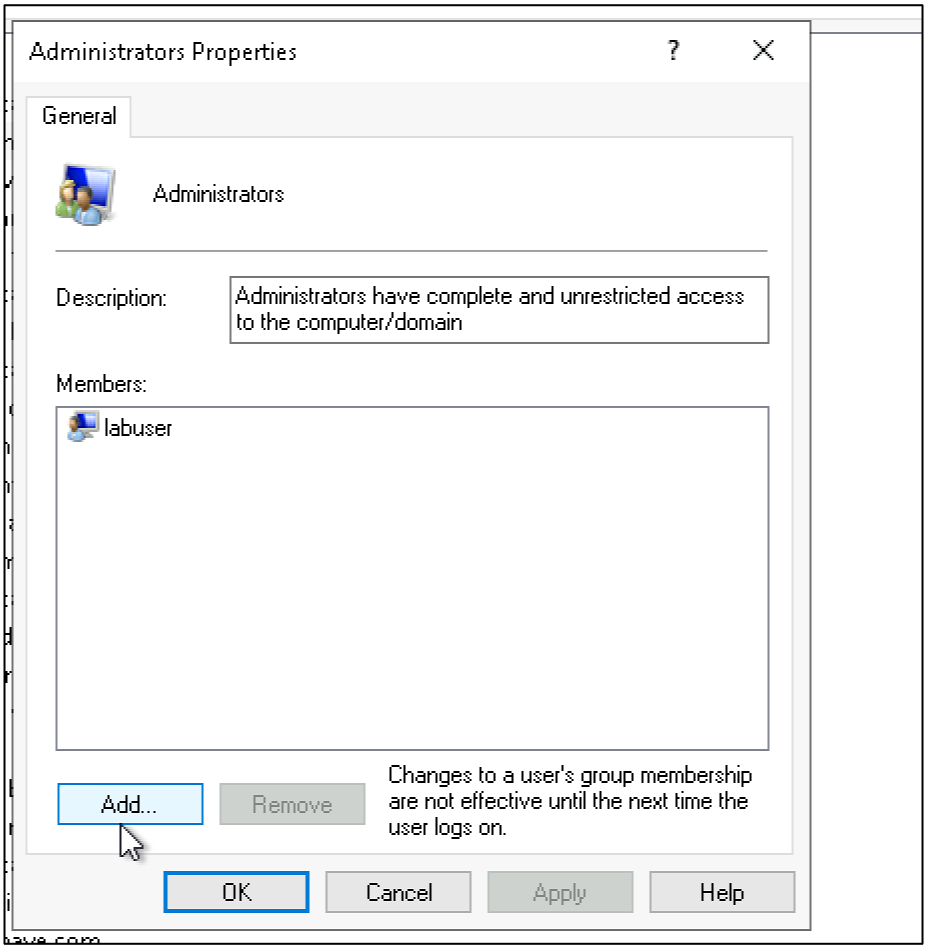
□ Account is disabled

3.4 Now, click on **Groups** and then select **Administrators**



Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override se...
Certificate Service DC...	Members of this group are allowe...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...

3.5 On the **Administrators** page, click on **Add**, search for the username, click on **Check Names**, and then click on **OK**



Administrators Properties

General

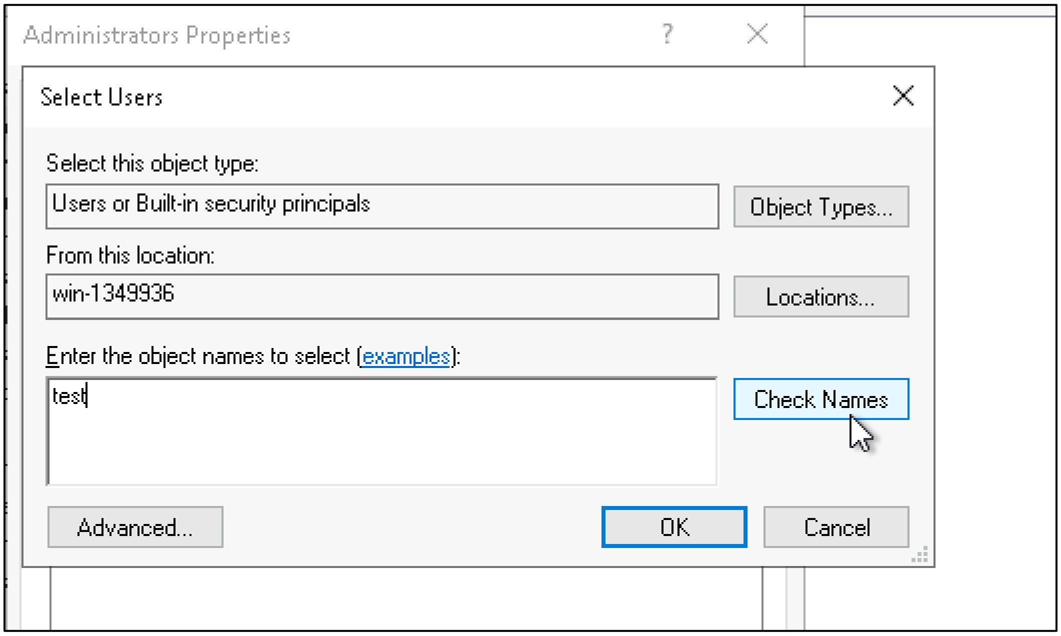
Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

labuser

Changes to a user's group membership are not effective until the next time the user logs on.



Select this object type:

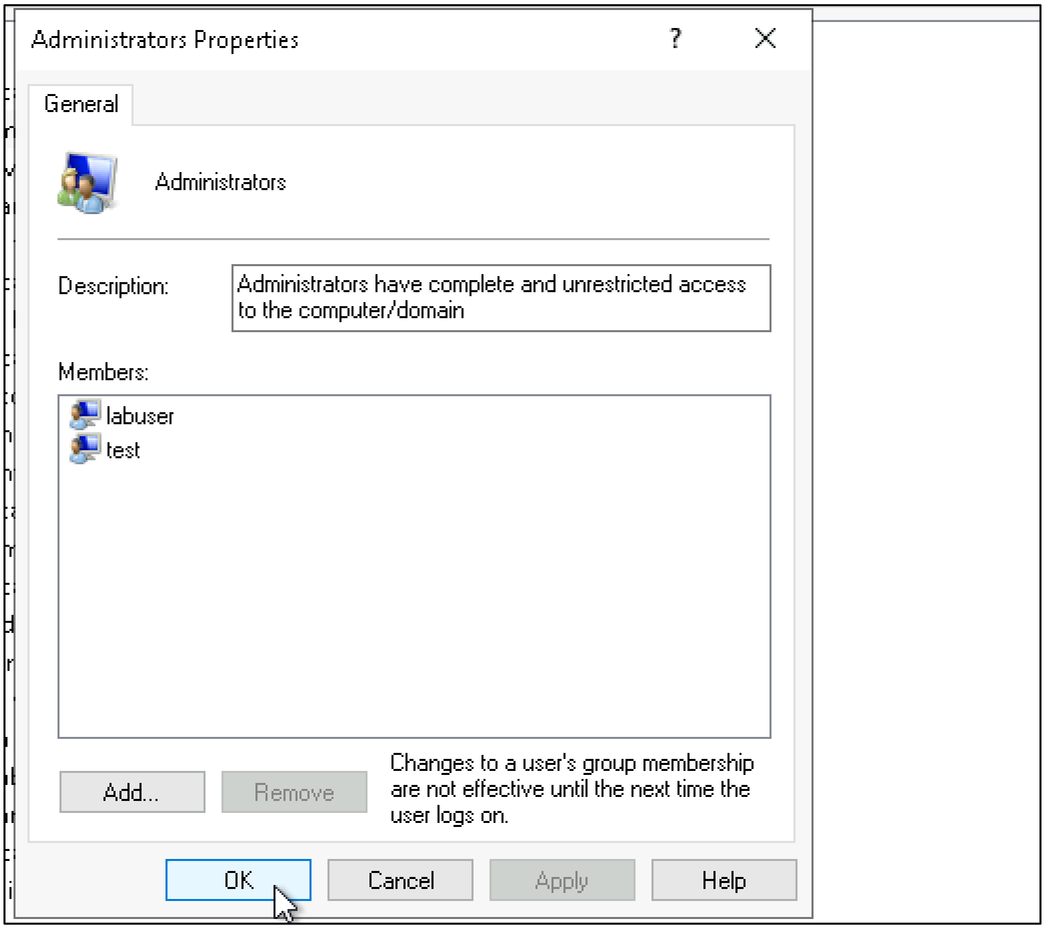
Users or Built-in security principals

From this location:

win-1349936

Enter the object names to select (examples):

test



Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

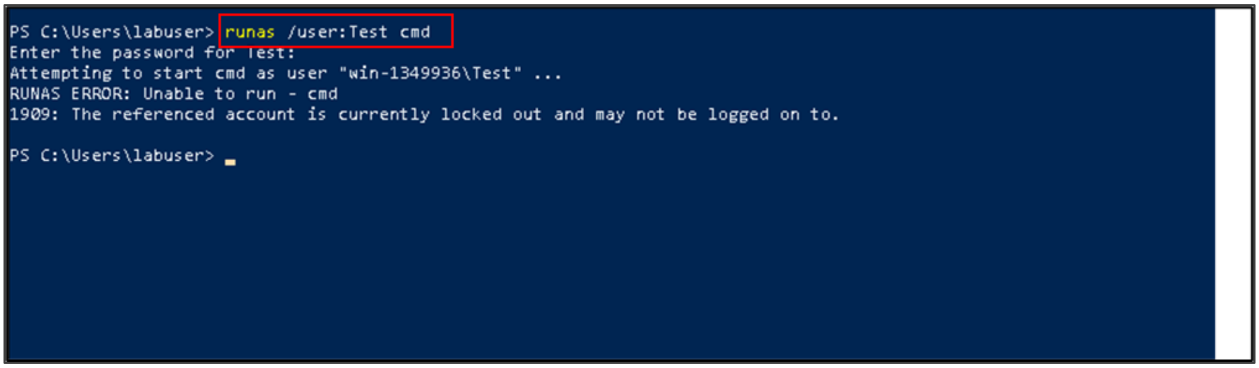
Members:

labuser
test

Changes to a user's group membership are not effective until the next time the user logs on.

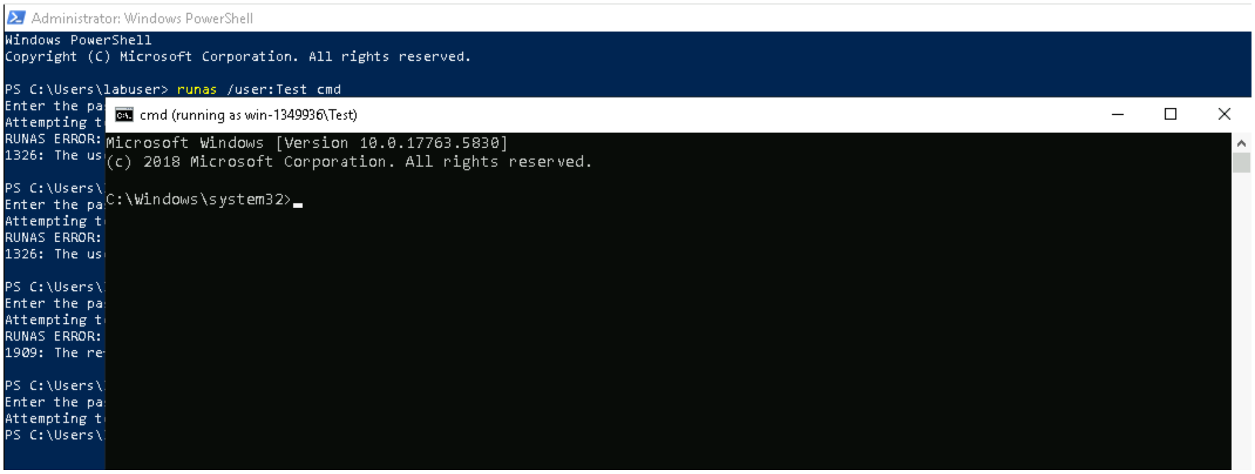
You can see that the user is added.

3.6 Now, open **Windows PowerShell**, and then run the command **runas /user:Test cmd**, and then enter its password



```
PS C:\Users\labuser> runas /user:Test cmd
Enter the password for Test:
Attempting to start cmd as user "win-1349936\Test" ...
RUNAS ERROR: Unable to run - cmd
1909: The referenced account is currently locked out and may not be logged on to.

PS C:\Users\labuser> _
```

You can see that the command prompt starts with the privileges of the test user.



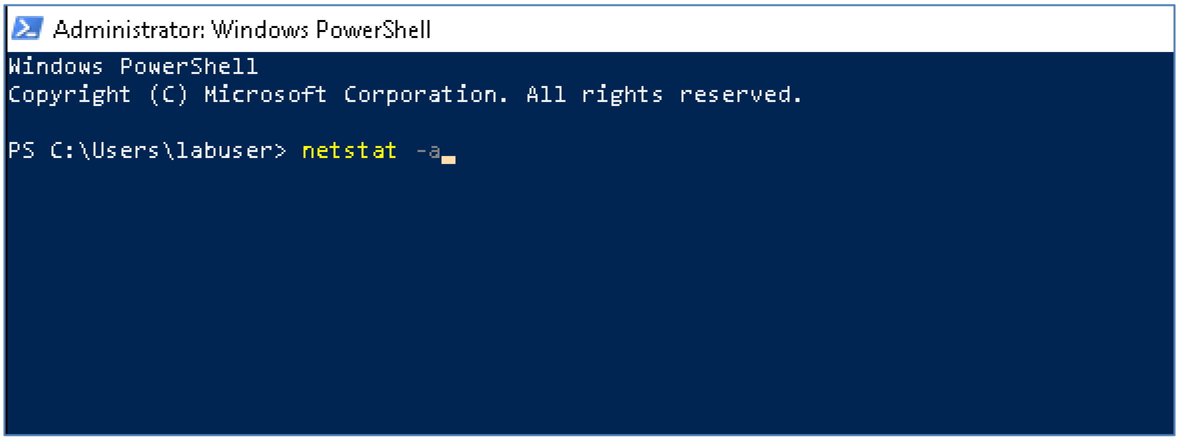
Administrator: Windows PowerShell
cmd (running as win-1349936\Test)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\labuser> runas /user:Test cmd
Enter the pa
Attempting t
RUNAS ERROR:
1326: The us

PS C:\Users\
Enter the pa
Attempting t
RUNAS ERROR:
1326: The us

PS C:\Users\
Enter the pa
Attempting t
RUNAS ERROR:
1909: The re

PS C:\Users\
Enter the pa
Attempting t
PS C:\Users\
```

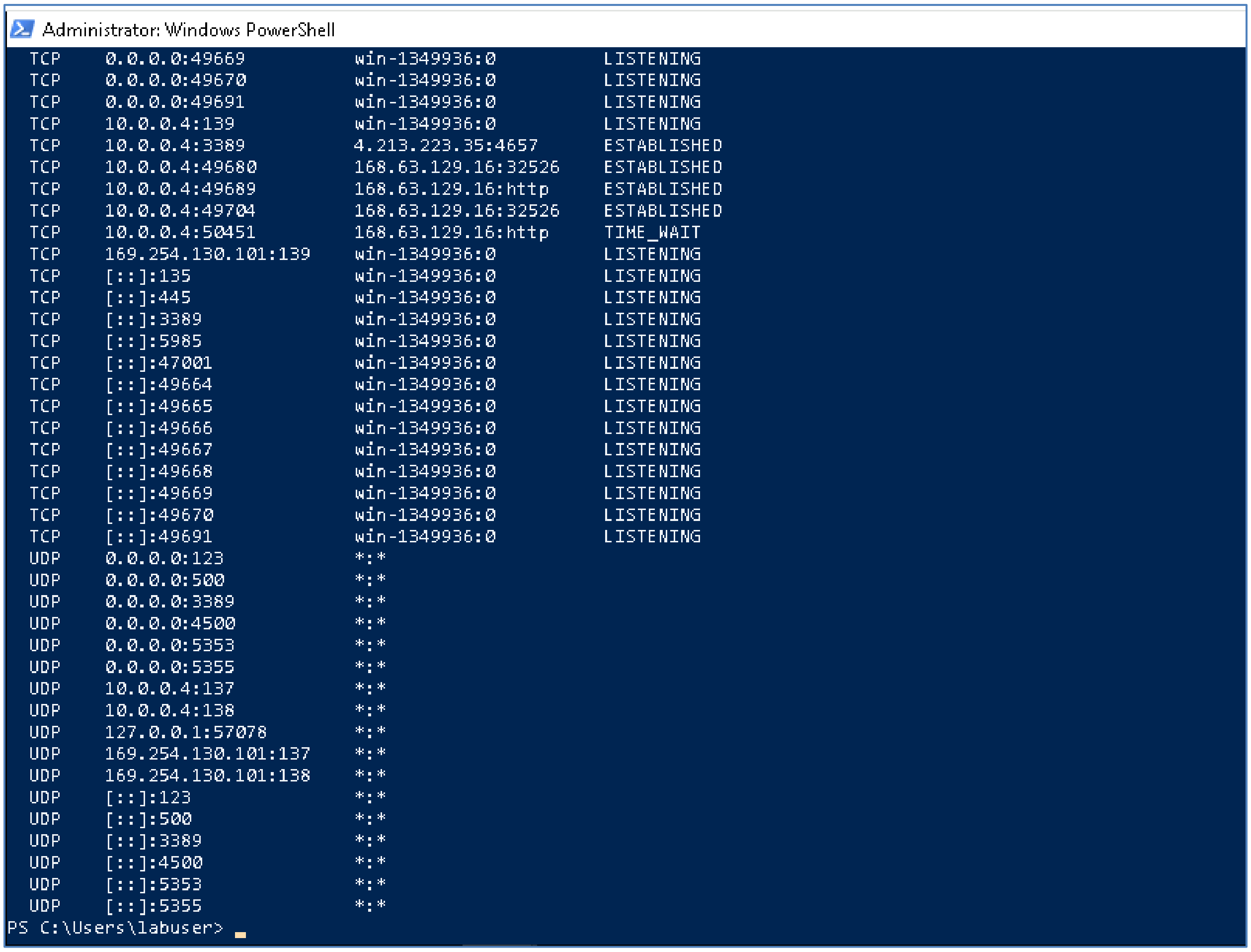
```
Microsoft Windows [Version 10.0.17763.5830]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>_
```

Step 4: View the port status and name resolution using netstat and nslookup

4.1 Open the Windows PowerShell and run the command **netstat -a**

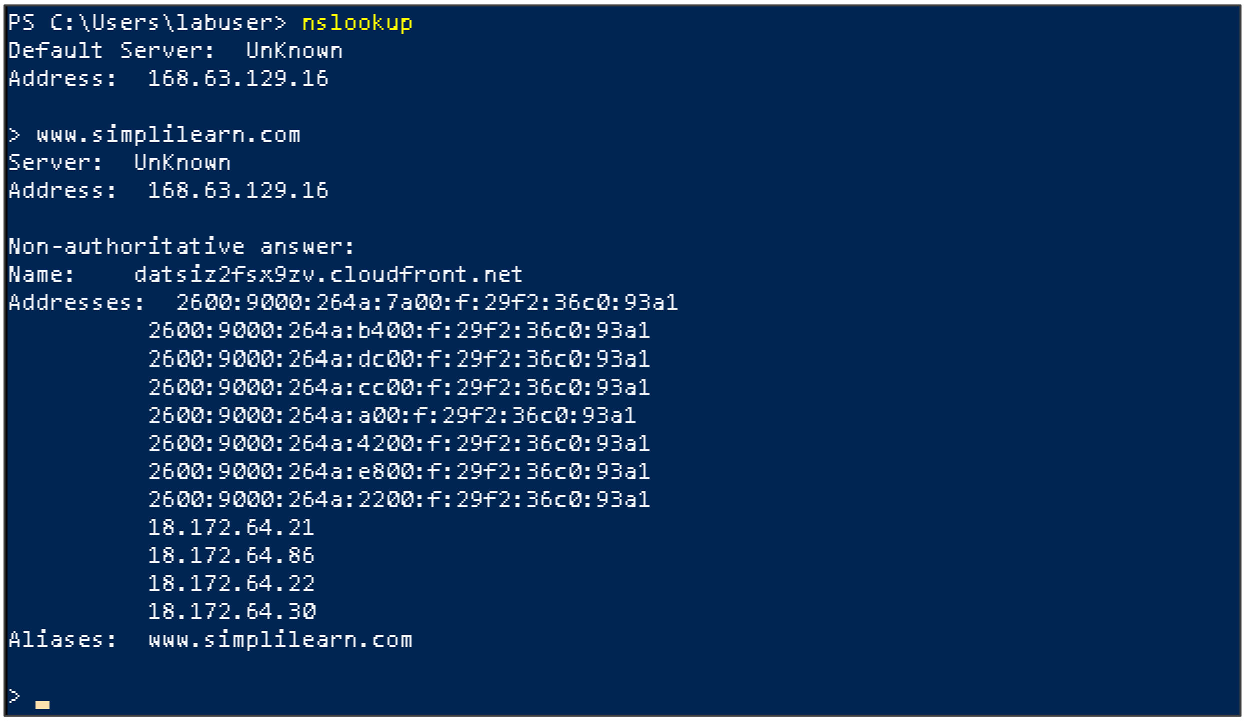


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\labuser> netstat -a
```



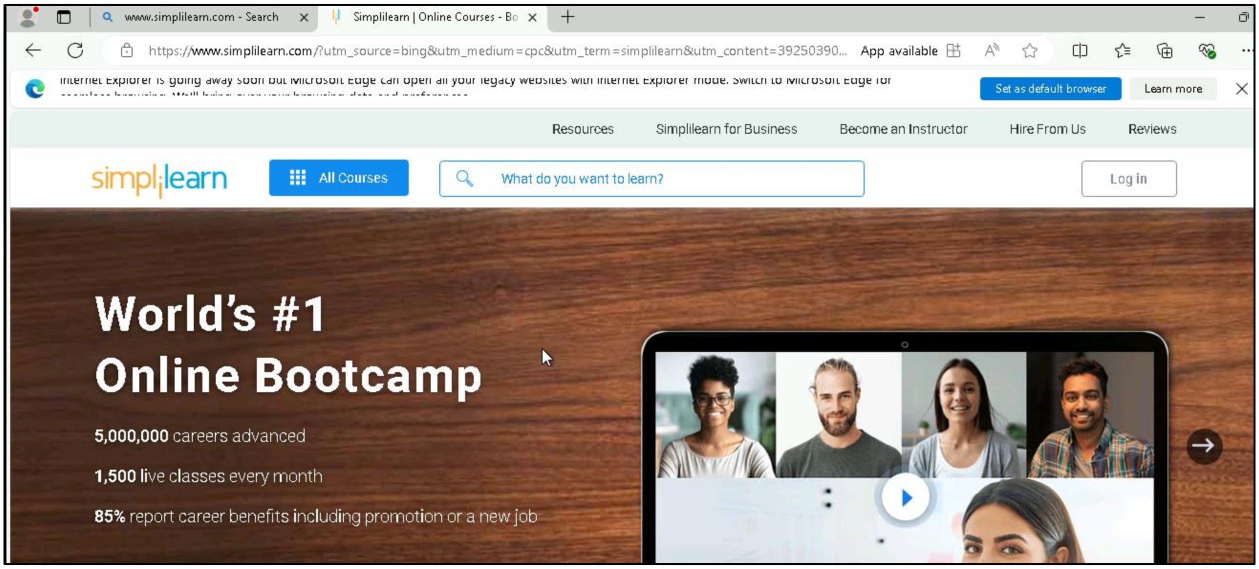
```
  TCP    0.0.0.0:49669          win-1349936:0          LISTENING
  TCP    0.0.0.0:49670          win-1349936:0          LISTENING
  TCP    0.0.0.0:49691          win-1349936:0          LISTENING
  TCP    10.0.0.4:139           win-1349936:0          LISTENING
  TCP    10.0.0.4:3389          4.213.223.35:4657      ESTABLISHED
  TCP    10.0.0.4:49680         168.63.129.16:32526    ESTABLISHED
  TCP    10.0.0.4:49689         168.63.129.16:http     ESTABLISHED
  TCP    10.0.0.4:49704         168.63.129.16:32526    ESTABLISHED
  TCP    10.0.0.4:50451         168.63.129.16:http     TIME_WAIT
  TCP    169.254.130.101:139    win-1349936:0          LISTENING
  TCP    [::]:135               win-1349936:0          LISTENING
  TCP    [::]:445               win-1349936:0          LISTENING
  TCP    [::]:3389              win-1349936:0          LISTENING
  TCP    [::]:5985              win-1349936:0          LISTENING
  TCP    [::]:47001             win-1349936:0          LISTENING
  TCP    [::]:49664             win-1349936:0          LISTENING
  TCP    [::]:49665             win-1349936:0          LISTENING
  TCP    [::]:49666             win-1349936:0          LISTENING
  TCP    [::]:49667             win-1349936:0          LISTENING
  TCP    [::]:49668             win-1349936:0          LISTENING
  TCP    [::]:49669             win-1349936:0          LISTENING
  TCP    [::]:49670             win-1349936:0          LISTENING
  TCP    [::]:49691             win-1349936:0          LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3389           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    10.0.0.4:137           *:*
  UDP    10.0.0.4:138           *:*
  UDP    127.0.0.1:57078        *:*
  UDP    169.254.130.101:137    *:*
  UDP    169.254.130.101:138    *:*
  UDP    [::]:123               *:*
  UDP    [::]:500               *:*
  UDP    [::]:3389              *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
PS C:\Users\labuser>
```

4.2 Now, run the command **nslookup**, and then type **www.simplilearn.com**



```
PS C:\Users\labuser> nslookup
Default Server:  UnKnown
Address:  168.63.129.16

> www.simplilearn.com
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    datsiz2fsx9zv.cloudfront.net
Addresses:  2600:9000:264a:7a00:f:29f2:36c0:93a1
          2600:9000:264a:b400:f:29f2:36c0:93a1
          2600:9000:264a:dc00:f:29f2:36c0:93a1
          2600:9000:264a:cc00:f:29f2:36c0:93a1
          2600:9000:264a:a00:f:29f2:36c0:93a1
          2600:9000:264a:4200:f:29f2:36c0:93a1
          2600:9000:264a:e800:f:29f2:36c0:93a1
          2600:9000:264a:2200:f:29f2:36c0:93a1
          18.172.64.21
          18.172.64.86
          18.172.64.22
          18.172.64.30
Aliases:  www.simplilearn.com

>
```

4.3 Open the browser and navigate to **www.simplilearn.com**

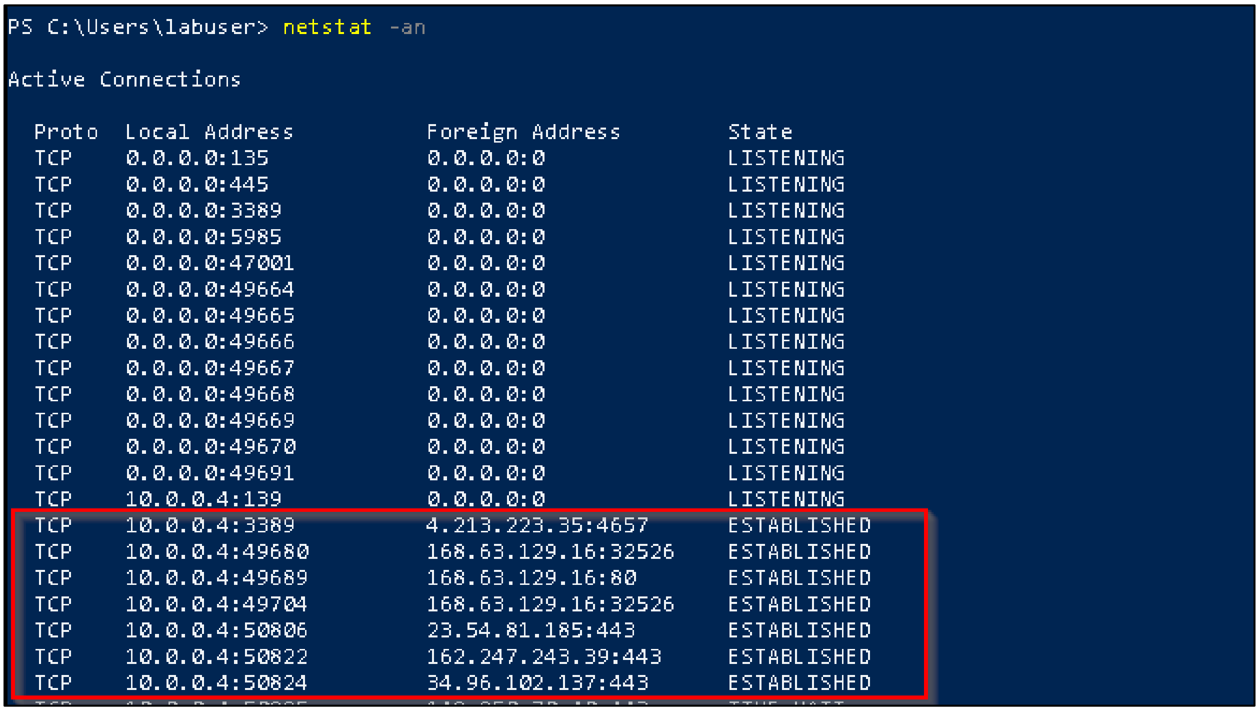


https://www.simplilearn.com/?utm_source=bing&utm_medium=cpc&utm_term=simplilearn&utm_content=39250390...

Internet Explorer is going away soon but Microsoft Edge can open all your legacy websites with Internet Explorer mode. Switch to Microsoft Edge for

www.simplilearn.com - Search
Simplilearn | Online Courses - Bo
App available
Set as default browser
Learn more
Resources
Simplilearn for Business
Become an Instructor
Hire From Us
Reviews
simplilearn
All Courses
What do you want to learn?
Log in
World's #1
Online Bootcamp
5,000,000 careers advanced
1,500 live classes every month
85% report career benefits including promotion or a new job

4.4 Now, navigate back to PowerShell, and run the command **netstat -an**



```
PS C:\Users\labuser> netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49691          0.0.0.0:0              LISTENING
  TCP    10.0.0.4:139           0.0.0.0:0              LISTENING
  TCP    10.0.0.4:3389          4.213.223.35:4657      ESTABLISHED
  TCP    10.0.0.4:49680         168.63.129.16:32526    ESTABLISHED
  TCP    10.0.0.4:49689         168.63.129.16:80       ESTABLISHED
  TCP    10.0.0.4:49704         168.63.129.16:32526    ESTABLISHED
  TCP    10.0.0.4:50806         23.54.81.185:443       ESTABLISHED
  TCP    10.0.0.4:50822         162.247.243.39:443     ESTABLISHED
  TCP    10.0.0.4:50824         34.96.102.137:443      ESTABLISHED
```

You can see that the state is established successfully.

By following these steps, you have successfully implemented logging and forensic analysis using Event Viewer to maintain a secure and well-monitored network. environment