**5.Privilege Escalation Simulation**

What Happens When You Add a User to the Administrators Group?

When you add a user to a group on a Windows system, security logs capture this as a privilege change event. The relevant Event IDs to look for are:

* 4728 — A member was added to a security-enabled global group
* 4732 — A member was added to a security-enabled local group (including Administrators group on local machine)

Since the Administrators group is a local security group, Event ID 4732 is the typical event you’ll see.

How to Create a User and Add to Administrators Group (for simulation)

Run these commands as admin in PowerShell or CMD:

# Create a local user

net user TestUser P@ssw0rd! /add

# Add the user to the local Administrators group

net localgroup Administrators TestUser /add

What to Look for in the Event Logs

1. Open Event Viewer → Windows Logs → Security
2. Filter by Event ID 4728 or 4732
3. Analyze the event details:

* The event will show:
  + Subject: Who made the change (the admin or process)
  + Group Name: The group affected (e.g., Administrators)
  + Member: The user added (e.g., TestUser)
  + Group SID and Member SID
* The log will indicate that a member was added to a privileged group.

Detection Tip: Compare Group Memberships Before/After

* Before adding the user, query the current members of the Administrators group:
* net localgroup Administrators
* After adding the user, run it again.
* Detect anomalous or unexpected additions to privileged groups by cross-referencing:
  + Security Event Logs (4728/4732)
  + Current group membership

|  |  |  |
| --- | --- | --- |
| Event ID | Description | Group Type |
| 4728 | Member added to global group | Global Security Group |
| 4732 | Member added to local group | Local Security Group (e.g. Administrators) |