**8: SIMULATE a Privilege Escalation Attempt**

We will

* Creating a new user
* Adding that user to the Administrators group
* Enabling dangerous privileges
* Modifying a service for privilege escalation

✅ Step 1: Create a New User

1. Open Command Prompt as Administrator (cmd.exe → Right-click → Run as Administrator).
2. Run the following:
3. net user attacker Password123! /add

✅ This creates a new user named attacker.

✅ Step 2: Add That User to the Administrators Group

net localgroup Administrators attacker /add

✅ Now attacker has admin privileges.

✅ Step 3: Modify a Service

Let’s modify a harmless service to run cmd.exe with SYSTEM privileges:

sc config wuauserv binPath= "cmd.exe /k"

✅ This changes the Windows Update service to run cmd.exe instead.

Then start the service:

net start wuauserv

This will open a command prompt with SYSTEM privileges if successful.

✅ Step 4: Enable Dangerous Privileges (Check Available Privileges)

whoami /priv

✅ See if privileges like SeDebugPrivilege or SeImpersonatePrivilege are enabled.

DETECT Privilege Escalation Attempts

Now, we detect what you just simulated using logs and tools.

🔹 Step 1: Check Windows Event Logs for New Admin User

1. Open Event Viewer → Go to:
2. Windows Logs → Security
3. Search for:
   * Event ID 4720 → A new user was created
   * Event ID 4728 → A user was added to a privileged group

You should see attacker created and added to Administrators.

### Use Sysmon

Install Sysmon with this config:

cmd

CopyEdit

Sysmon.exe -accepteula -i sysmonconfig.xml

It logs:

* Registry events (ID 13)
* Service changes
* Process creations