SCENARIO 1: PRIVILEGE ESCALATION ATTEMPT

1. Create a New User (Backdoor Account)
    a. net user backdoor Passw0rd! /add
2. Add the User to Administrators Group
    a. net localgroup administrators backdoor /add
3. Log in as Backdoor to Confirm
    a. runas /user:backdoor cmd
    b. whoami
    c. net session

now I am in admin access.

4. Open Event Viewer to See Logs
    a. I can see 4720, 4728, 4672 all the event

🔍 Search for Event IDs:

- `4720` – User Account Created
- `4728` – Added to Administrators Group
- `4672` – Privileged login