**Enumeration Simulation: Listing User Accounts on a Windows Computer**

**Objective:**

To perform **user enumeration** using Command Prompt on a Windows system and analyze the security implications of exposing user account information.

**Step-by-Step Experiment:**

**Step 1: Open Command Prompt**

1. Press **Win + R**, type **cmd**, and press **Enter**.
2. Ensure that the Command Prompt is **run as administrator** (Right-click > "Run as administrator").

**Step 2: Enumerate Local User Accounts**

**Method 1: Using net user Command**

* Type the following command to list all user accounts:

cmd

CopyEdit

net user

* This will display all local user accounts on the system.

**Method 2: Viewing Detailed User Information**

* To get details of a specific user, use:

cmd

CopyEdit

net user <username>

Example:

cmd

CopyEdit

net user Administrator

* This provides information such as:
  + Account creation date
  + Password policies
  + Group memberships

**Method 3: Enumerating Domain Users (For Networked Systems)**

* If the computer is part of a **domain**, use:

c

CopyEdit

net group "Domain Users" /domain

or

cmd

CopyEdit

net user /domain

* This retrieves all domain user accounts (Requires proper permissions).

**Step 3: Security Implications & Countermeasures**

💡 **Risk:** Unauthorized users can list accounts and attempt brute-force attacks.  
✅ **Countermeasures:**

* Disable the built-in **Administrator** account if not in use.
* Use **strong passwords & multi-factor authentication**.
* Restrict enumeration using **Group Policy (gpedit.msc)**:
  + Local Security Policy > Security Settings > Local Policies > Security Options
  + **Set "Accounts: Administrator account status" to Disabled**

**Deliverables:**

🔹 **Screenshots** of enumeration commands and results.  
🔹 **Analysis Report** on findings and security risks.  
🔹 **Defense Strategy Recommendations** to prevent unauthorized enumeration.

Would you like to expand this with PowerShell-based enumeration or automation? 🚀