PwnPlug Lite Module: User Account Discovery

PwnPlug Lite Module: User Account Discovery
Author: Jeremy Shane Butts (CyberGeekJSB)
Platforms: Windows (WMI/pywin32), Linux (pwd/grp)
Version: 2.0

Purpose
Enumerate local user accounts and privileged group membership to support:
- identity discovery
- audit/compliance checks
- lateral movement mapping
- detection of unexpected privileged accounts

Windows capabilities
- Enumerate local users via `Win32_UserAccount`
- Enumerate local Administrators group members via `Win32_GroupUser`
- Collect: SID, disabled/lockout state, password flags, description

Linux capabilities
- Enumerate local users via `pwd`
- Enumerate groups/members via `grp`
- Enumerate `sudo` (or `wheel`) members via `getent group`

Outputs
PwnPlug module log
`/opt/pwnplug/logs/user_discovery.json` (JSON Lines)

Standalone tools
- Python prints JSON to stdout
- PowerShell prints JSON to stdout

Execution
Windows (Python)
```powershell
python .\UserDiscovery.py
```

Windows (PowerShell)
```powershell
powershell -ExecutionPolicy Bypass -File .\UserDiscovery.ps1
```

Linux
```bash
python3 ./user_discovery_linux.py
```

GUI panel
`pwnplug/web/panels/user_discovery.html` calls:

- `GET /api/user_discovery`

Notes
- Windows Python requires `pywin32` (`pip install pywin32`)
- Admin group query assumes the group name is `Administrators`