Windows Privilege Escalation

Introduction to the Windows Shells

Leonardo Tamiano

Contents

1 Windows is Not Open-Source

`Linux` is an open-source operating system initially developed by Linus Torvalds around `1991` and currently developed by the open-source community. To this day it is still maintained by Torvalds.

For more information on the linux kernel developmeng you can check the respective mailing list

- https://lkml.org/

`Windows` is a proprietary operating system developed by `Microsoft`. This means that we have less knowledge about the internal functioning of Windows.

It also means that the `kernel` of the operating system and the external `user-space` programs cannot be taken apart. For example in linux you have different user-space programs using the same kernel, and this has given rise to the concept of `linux distribution`, such as

- ArchLinux
- Ubuntu
- Debian

Since in windows it is not possible to separate the user-space programs from the internal kernel code, the concept of a windows distribution does not exist.

2 Some History

Before `Microsoft Windows` there was `Microsoft DOS`, a non-graphical, command line operating system created for IBM compatible computers.

```
DOS -> Disk Operating System
```

Microsoft DOS History

Date	Version
1981	MS-DOS 1.0
1982	MS-DOS 1.2
1983	MS-DOS 2.0
1984	MS-DOS 3.0
1986	MS-DOS 3.2
1987	MS-DOS 3.3
1988	MS-DOS 4.0
1991	MS-DOS 5.0
1993	MS-DOS 6.0
1993	MS-DOS 6.2
1994	MS-DOS 6.21
1994	MS-DOS 6.22

Microsoft Windows History

Date	Version
1985	Windows 1.0
1990	Windows 3.0
1993	Windows NT
1995	Windows 95
2001	Windows XP
2006	Windows Vista
2009	Windows 7
2012	Windows 8
2014	Windows 10
2021	Windows 11

3 Windows Setup

Using `quickemu`

```
quickget windows 11
quickemu --vm windows-11.conf --display spice
```

4 CMD.exe

4.1 Basic Commands

operating system, version and architecture

```
systeminfo
```

username

```
whoami
```

working directory

```
cd
```

get env variables

```
set
```

print specific env variable value

```
echo %PATH%
```

find path of executables

```
where <EXE NAME>
```

get documentation

```
help dir
```

clear screen

```
cls
```

4.2 File System Commands

print current directory

```
cd
```

list files in current directory

```
dir
dir /A
```

create directory

```
mkdir test
```

create new file

```
type NUL > test.txt
echo "hello" > test.txt
```

read file's content

```
type test.txt
```

4.3 Permissions Commands

current user

```
whoami
```

list my groups

```
whoami /groups
```

privileges of current user

```
whoami /priv
```

account policy for current user

```
net accounts
```

list users in the system

```
net user
```

list user detail

```
net user <USERNAME>
```

get permissions of file

```
icacls <FILE>
```

4.4 Networking Commands

list all network interfaces

```
ipconfig /all
```

display routing table

```
route print
```

display network information

```
netstat -ao
```

5 Powershell.exe

5.1 Basic Commands

list local users

```
Get-LocalUser
```

list local groups

```
Get-LocalGroup
```

gets members from a local group

```
Get-LocalGroupMember <GROUP-NAME>
```

get env variables

```
dir env:
```

search files recursively

```
Get-ChildItem -Path C:\Users\ -Include *.kdbx -File -Recurse -ErrorAction SilentlyContinue
Get-ChildItem -Path C:\Users\ -Include *.txt -File -Recurse -ErrorAction SilentlyContinue
```

5.2 Process Commands

running processes

```
Get-Process
```

installed apps (32 bit)

```
Get-ItemProperty "HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*"
      | select displayname
```

installed apps (64 bit)

```
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*" | select
    displayname
```

5.3 Services Comands

get service info

```
Get-Service * | Select-Object Displayname,Status,ServiceName,Can*
Get-CimInstance -ClassName win32_service | Select Name,State,PathName | Where-Object {$_.
    State -like 'Running'}
```

6 References

- https://github.com/quickemu-project/quickemu
- https://users.dimi.uniud.it/~antonio.dangelo/LabOS/2008/lessons/helper/history/msdosHistory.html
- https://en.wikipedia.org/wiki/Microsoft_Windows
- https://www.computerhope.com/msdos.htm