System Enumeration

To find information about system os version & hostname

```
systeminfo
```

One liner to find os version and architecture

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

To find latest patch information

```
wmic qfe
```

To list drives

```
wmic logicaldisk
```

To get better output for logical disk

```
wmic logicaldisk get caption,description,providername
```

User Enumeration

To find out which user you are

```
whoami
```

To find out what kind of priv's your user has

```
whoami /priv
```

To find out which group your user belong's

```
whoami /groups
```

To find out User's on your computer

```
net users
```

To find out information about a specific user on the computer

```
net user username
```

To find out diiferent group's

```
net localgroup
```

To find information about a specific group

```
net localgroup groupname
```

Network Enumeration

To find the ip address of the machine , subnets etc…….

```
ipconfig /all
```

To find arp table

```
arp -a
```

To find out which port's are open and connected tcp , udp

```
netstat -ano
```

Password Hunting

```
findstr /si password *.txt *.config *.ini
```

Av Enumeration

Checking windows defender

```
sc query windefend
```

Checking other running services to look for some other antivirus

```
sc queryex type= service
```

To Checking firewall

```
netsh advfirewall firewall dump
```

or

```
netsh firewall show state
```

To Get more detailed overview of firewall to check different port's

```
netsh firewall show config
```

Automatic Enumeration

Some best tool

Winpeas https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS/winPEASexe

Windows exploit suggester https://github.com/AonCyberLabs/Windows-Exploit-Suggester

Metasploit post/multi/recon/local_exploit_suggester

Wsl

Wsl stand's for window's sub system for linux mean's you can run linux on windows system .

#update this

look for bash.exe

Impersonete Tokens

In this attack we can impersonete someone's token if we have any of these token
`SeAssignPrimaryToken`

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Wi
%20Privilege%20Escalation.md#eop—impersonation-privileges

In meterpreter u can try

```
load incognito
```

```
list_tokens -u
```

U can also use local_exploit_suggester to find exploit's

Also try exploit/windows/local/ms16_075_reflection
exploit/windows/local/ms16_075_reflection_juicy

Runas

It's a feature in a feature in windows which let's you run a program as administrator . U can abuse this feature to get root .

```
cmdkey /list
```