windows local enum

1.- System Enumeration

Get system information

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

Checking installed updates

```
wmic qfe get Caption, Description
```

Check how many drivers are in the machine

```
wmic logicaldisk get Caption
```

2.- User enumeration

Check current user

```
whoami
```

Check current user privileges

```
whoami /priv
```

Groups were current user is involved

```
whoami /groups
```

View all users

```
net users
```

View user information

```
net users <username>
#Example
net users daronwolff
```

List the user groups

```
net localgroup
```

View members of a group

```
net localgroup Administrators
```

3.- Network Enumeration

Ip address configuration (default gateway, subnet, dns, domain controller)

```
ipconfig /all
```

ARP table

```
arp -a
```

Routing table

```
route print
```

Network status

```
net stat
```

4.- Password Enumeration

Search the word "password" in text files

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

Searching passwords in the registry

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

Passwords in *unattend* 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
```

5.- Firewall and AV Enumeration

Check Windows defender

```
sc query windefend
```

View all services running on the machine

```
sc queryex type= service
```

sc = service control

Firewall settings

```
netsh advfirewall firewall dump
```

```
netsh firewall show state
```

Show firewall config

```
netsh firewall show config
```