PE Enumeration

Windows

Find system info

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

Find all running processes

```
tasklist /SVC
```

Review Network Configuration

```
ipconfig /all
```

Routing table

```
route print
```

View all active connection

```
netstat -ano
```

Firewall Ruls

```
netsh advfirewall show currentprofile
netsh advfirewall firewall show rule name=all
```

Scheduled Task

```
schtasks /query /fo LIST /v
```

Installed Applications

```
wmic product get name, version, vendor
```

System wide updates/patches

```
wmic qfe get Caption, Description, HotFixID, InstalledOn
```

Finding writable and readable files

> All executable files

```
accesschk.exe -uws "Everyone" "C:\Program Files"
```

```
Get-ChildItem "C:\Program Files" -Recurse | Get-ACL | ?{$_.AccessToStrung -match "Everyone\sAllow\s\sModify"}
```

Finding Unmounted Disk

```
mountvol
```

Finding Kernal modules and drivers

```
driverquery.exe /v /fo csv | ConvertFrom-CSV | Select-Object 'Display Name' , 'Start Mode', Path

Get-WmiObject Win32_PnPSignedDriver | Select-Object DeviceName, DriverVersion, Manufacturer | Where-Object {$_.DeviceName -like "*NAME*"}
```

Finding binarys to elevate

```
reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
reg query HKEY_CURRENT_MACHINE\Software\Policies\Microsoft\Windows\Installer
```

Automated Enumeration

> Windows Privesc Check

linux

Find System info

```
uname -a
```

Find all running processes

```
ps aux
```

Review Network Configuration

```
ip a
```

Routing table

```
/sbin/route
```

```
/sbin/routel
```

View all active connections

```
ss -anp
```

Firewall ruls

```
grep -Hs iptables /etc/*
cat /etc/iptable-backup
```

Scheduled Task

```
cat /etc/crontab
```

Installed Applicatons

```
dpkg -l
```

Finding writable and readable files

> ALl writable Directrys

```
find / -writable -type d 2>/dev/null
```

Finding Unmounted Disk

```
mount
cat /etc/fstab
/bin/lsblk
```

Finding Kernal modules and drivers

```
lsmod
/sbin/modinfo NAME
```

SUID - Finding binarys to elevate

```
find / -pern -u=s -type f 2>/dev/null
```