



PowerShell

From zero to hero

VulnStrike Research Initiative



01

Crash Course

Blaze through basics of
PowerShell in minutes

Cmdlet Naming Convention

Verb-Noun

(e.g. Write-Host, Invoke-WebRequest)

Alias

- Some commands have aliases using the Verb-Noun convention.
 - o `Invoke-WebRequest` -> `iwr`
 - o `Get-Variable` -> `gv`
 - o `Get-ChildItem` -> `gci`, `ls`, `dir`

Basic Scripting

```
PS> Write-Host "Hello World!"  
Hello World!
```

Case Insensitive

```
PS> Write-Host "Hello World!"  
Hello World!
```

Escape Character

```
PS> Write-Host "Hell`o W`orld`!"  
Hello World!
```

Call .NET Assemblies

```
PS> (New-Object System.Net.WebClient).DownloadString("https://stillu.cc/.well-known/pubkey.asc")  
Contact: mailto:business@stillu.cc  
GPG Key: https://stillu.cc/.well-known/pubkey.asc  
Preferred-Languages: en
```


Ability to Ingest Encoded Commands

```
$scriptBlock = {Write-Host "Hello World!"}  
$baseOut = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($scriptBlock))  
# VwByAGkAdABlAC0ASABvAHMAAdAAgACIASABlAGwAbABvACAAV  
wBvAHIAbABkACEAIgA=  
> powershell -enc $baseOut  
Hello World!
```

Combine Language “Features”

```
(NEw-ObjEct
io.coMpRESsIOn.deflAtEstREam( [io.MeMoRystream] [sYSteM.C
OnVERT]::fROMbASE64stRING('09NQqjasrTaorTaqVdJNU0/V9cgvVt
dRDy/KLAFSJeqaCkoeqTk5+Qrh+UU5KYpKAA=='),[sysTeM.io.coMpr
ESSIOn.coMpresSiOnM0dE]::dEcoMpreSS) |%{ NEw-
ObjEct Io.sTreamrEaDer( $_,[TexT.ENcodiNg]::aSCiI ) } |
%{$_.rEaDtoend()}) |&((gV '*mdR*').NaMe[3,11,2]-Join'')
# Output: Hello World!
```

Comb

ures”

```
(NEw-ObJect  
io.coMprESSIO  
OnVERT]::fROM  
dRDy/KLAFSJeq  
ESSION.coMpre  
ObJect Io.sT  
%{$_.rEadtoen  
# Output: Hel
```



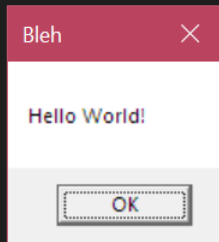
```
eam] [sYSteM.C  
/dJNU0/V9cgvVt  
ysTeM.io.cOMpr  
v-  
:aScii ) } |  
l,2]-Join'' )
```

Dynamic Compilation

- Compile and execute C# code in memory
 - o Win32 API calls
 - o In-memory execution
- See
 - o itm4n/PrivescCheck
 - o PowerSploit/PowerUp

```
C:\Users\34146\Downloads> temp.ps1 > ...
```

```
1 $CSharpSource = @'  
2 [DllImport("user32.dll", SetLastError=true)]  
3 public static extern int MessageBox(IntPtr hWnd, string lpText, string lpCaption, uint uType);  
4 '@  
5 try {  
6     [Util.Win32] | out-null  
7 }  
8 catch {  
9     $CompilerParameters = New-Object -TypeName System.CodeDom.Compiler.CompilerParameters  
10    $CompilerParameters.GenerateInMemory = $True  
11    $CompilerParameters.GenerateExecutable = $False  
12    Add-Type -MemberDefinition $CSharpSource -Name 'Win32' -Namespace 'Util' -Language CSharp -CompilerParameters $CompilerParameters  
13 }  
14 [Util.Win32]::MessageBox(0, "Hello World!", "Bleh", 0)
```



The background features a dark blue central area with wavy, organic shapes in shades of pink and light blue extending to the edges. A central circle with diagonal hatching contains the number '02' in pink.

02

Threats

Malware Execution Platform

PowerShell as a parent process

- Difficult to identify and inspect running code
- .NET assembly execution

Reverse shell

- .NET TcpClient class

Easy obfuscation

- Case insensitivity, Get-Command stringing, universal environment variables, etc.

Existing Mitigations/Defenses

- Anti-Malware Scan Interface (AMSI) + Windows Defender
 - o PowerShell analysis
 - Obfuscation analysis
 - Static analysis
 - Dynamic analysis


Existing Mitigations/Defenses

```
PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\34146> invoke-mimikatz
At line:1 char:1
+ invoke-mimikatz
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\34146> |
```



Existing Mitigations/Defenses

- Trivial to bypass with some work
 - o Invoke-Obfuscation
 - o AMSITrigger
 - o cobbr/PSAmsi
 - o tokyoneon/Chimera
 - o Manual labor

The background features a vibrant color palette of deep blue, purple, and magenta. Large, fluid, wavy shapes in these colors overlap and flow across the frame. Interspersed among these organic forms are various geometric patterns: a section of diagonal lines in the upper left, a circular hatched pattern in the lower right, and several small, faint circles scattered throughout. The overall aesthetic is modern and dynamic.

Live Demo

THANKS

Still Hsu

- <https://stillu.cc>
- @StillAzureH

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon and infographics & images by Freepik