


changelog		
conftest.py		
empire.py		
poetry.lock		
ps-empire		
pyproject.toml		
pytest.ini		

README

BSD-3-Clause license



Donate

Sponsor

Wiki

Docs

chat

343 online

Blog

Read me

follow @BCSecurity

follow @EmpireC2Project

views

20k

Linkedin

Empire

Empire is a post-exploitation and adversary emulation framework that is used to aid Red Teams and Penetration Testers. The Empire server is written in Python 3 and is modular to allow operator flexibility. Empire comes built-in with a client that can be used remotely to access the server. There is also a GUI available for remotely accessing the Empire server, [Starkiller](#).



BC-SECURITY BC Security

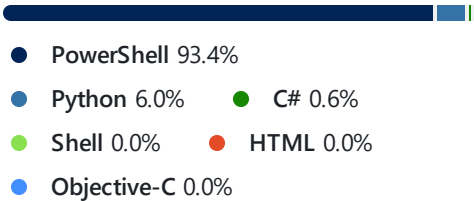
Sponsor

[Learn more about GitHub Sponsors](#)

Packages

No packages published

Languages



Features

- Server/Client Architecture for Multiplayer Support
- Supports GUI & CLI Clients
- Fully encrypted communications
- HTTP/S, Malleable HTTP, OneDrive, Dropbox, and PHP Listeners
- Massive library (400+) of supported tools in PowerShell, C#, & Python
- Donut Integration for shellcode generation
- Modular plugin interface for custom server features
- Flexible module interface for adding new tools
- Integrated obfuscation using [ConfuserEx 2](#) & [Invoke-Obfuscation](#)
- In-memory .NET assembly execution
- Customizable Bypasses
- JA3/S and JARM Evasion
- MITRE ATT&CK Integration
- Integrated Roslyn compiler (Thanks to [Covenant](#))
- Docker, Kali, ParrotOS, Ubuntu 20.04/22.04, and Debian 10/11/12 Install Support

Agents

- PowerShell
- Python 3
- C#
- IronPython 3

Modules

- [Assembly Execution](#)
- [BOF Execution](#)
- [Mimikatz](#)
- [Seatbelt](#)

- [Rubeus](#)
- [SharpSploit](#)
- [Certify](#)
- [ProcessInjection](#)
- And Many More

Sponsors



Release Notes

Please see our [Releases](#) or [Changelog](#) page for detailed release notes.

Quickstart

When cloning this repository, you will need to recurse submodules.

```
git clone --recursive https://github.com/BC-SECURITY/Empire
```



Check out the [Installation Page](#) for install instructions.

Note: The `main` branch is a reflection of the latest changes and may not always be stable. After cloning the repo, you can checkout the latest stable release by running the `setup/checkout-latest-tag.sh` script.

```
git clone --recursive https://github.com/BC-SECURITY/Empire
cd Empire
./setup/checkout-latest-tag.sh
./ps-empire install -y
```

If you are using the sponsors version of Empire, it will pull the sponsors version of Starkiller. Because these are private repositories, you need to have ssh credentials configured for GitHub. Instructions can be found [here](#).

Server

```
# Start Server
./ps-empire server

# Help
./ps-empire server -h
```

Client

```
# Start Client
./ps-empire client

# Help
./ps-empire client -h
```

Check out the [Empire Docs](#) for more instructions on installing and using with Empire. For a complete list of changes, see the [changelog](#).

Starkiller



[Starkiller](#) is a web application GUI for PowerShell Empire that interfaces remotely with Empire via its API. Starkiller can be ran as a replacement for the Empire client or in a mixed environment with Starkiller and Empire clients. As of 5.0, Starkiller is packaged in Empire as a git submodule and doesn't require any additional setup.

Contribution Rules

See [Contributing](#)

Contributors

A special thanks to the following contributors for their help with Empire:

[@harmj0y](#) [@sixdub](#) [@enigma0x3](#) [@rvrsh3ll](#) [@killswitch_gui](#)
[@xorrior](#) [@Cx01N](#) [@Hubbl3](#) [@Vinnybod](#)

Official Discord Channel

Join us in [our Discord](#) with any comments, questions, concerns, or problems!



[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.