CobaltStrike插件开发官方指南 Part4

CoolCat / 2019-09-05 08:59:00 / 浏览数 3487 渗透测试 渗透测试 顶(0) 踩(0)

翻译+实践

原文地址：

https://www.cobaltstrike.com/agscript-script/index.html

0x07 日志/计数器/窗口

事件日志

Cobalt Strike的运算符和脚本均将全局事件传递给共享事件日志，AgScripts也可以会对这些日志进行操作。

事件日志事件均以event_开头，使用event_notify可列出全局通知：

```
on event_notify {
   println("I see: $1");
}
```

如需将消息输出到共享事件日志可使用say函数。

```
say("Hello World");
```

要发布重大事件或通知（不一定是聊天），请使用elog函数，如出现冲突信息服务器将自动为此信息添加时间戳并存储（比如登陆一个已登陆的账号），此类信息也将显示
Strike的活动报告中。

```
elog("system shutdown initiated");
```

计时器

利用AgScript可中的heartbeat_X可实现定期执行任务，其中X的值可以是1s，5s，10s，15s，30s，1m，5m，10m，15m，20m，30m或60m

```
on heartbeat_10s {
   println("I happen every 10 seconds");
}
```

对话框

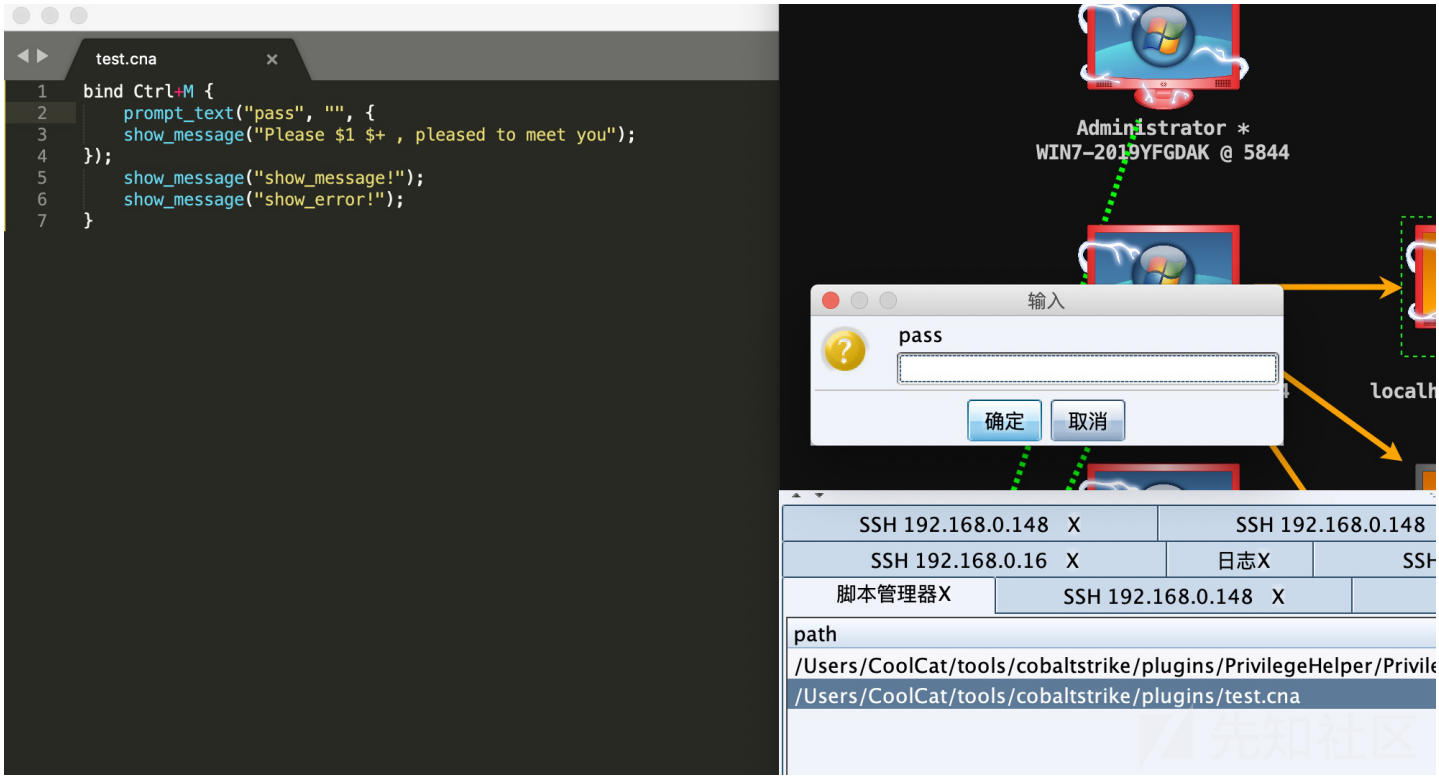
使用show_message可向用户提示信息，使用show_error可向用户提示错误信息。

```
bind Ctrl+M {
   show_message("show_message!");
   show_message("show_error!");
}
```

使用prompt_text函数可提示输入框：

```
prompt_text("What is your name?", "Joe Smith", {
   show_message("Please $1 $+ , pleased to meet you");
});
```

确认框可以使用prompt_confirm，和prompt_text函数相似度极高。

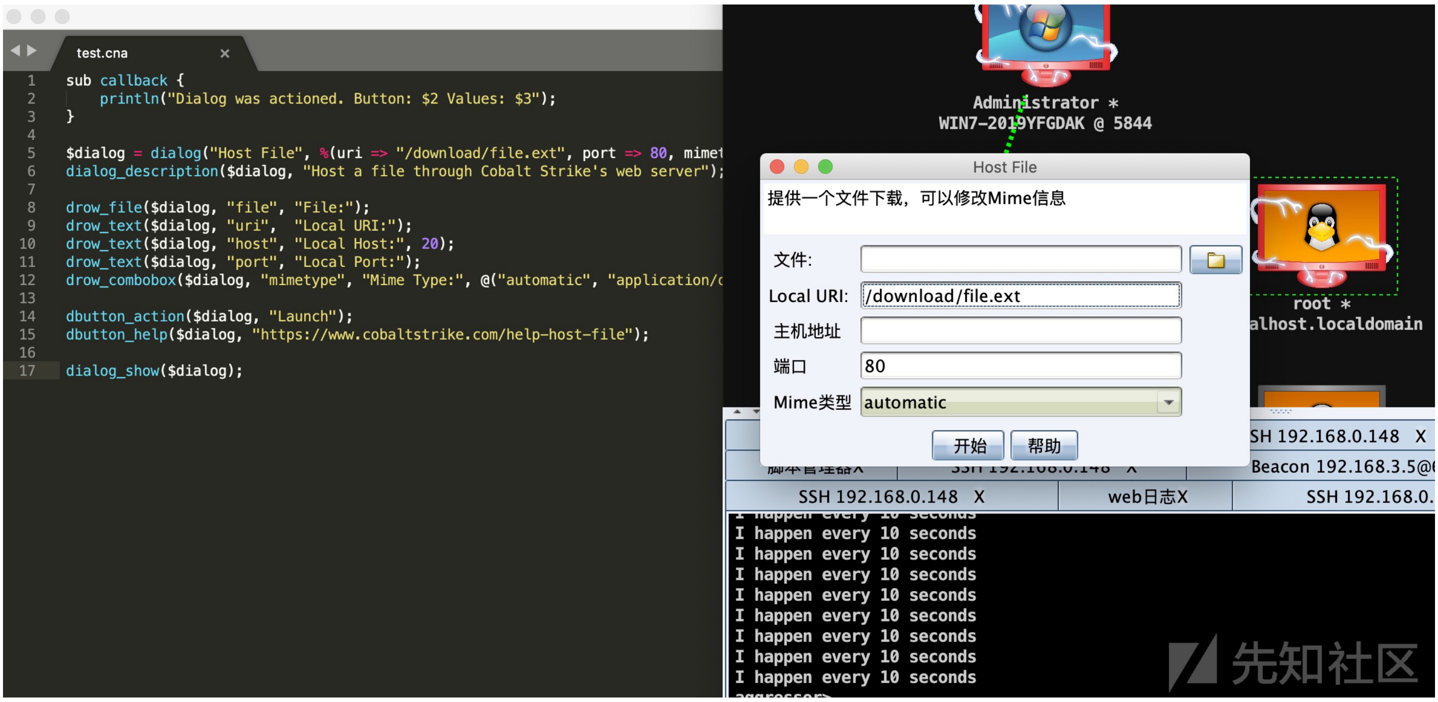


自定义对话框

AgScript有一个API可用于构建自定义对话框。
dialog函数用于创建一个对话框，对话框主要由行和按钮组成，其中行包含了标签，行名称，要输入的GUI组件，可能还有用于设置输入的帮助程序。
关闭按钮对话框并触发回调函数。
回调函数的参数类型是一个字典，将每行的名称映射到对应的GUI组件中的输入值。最后再使用dialog_show函数将对话框展示出来即可。demo：

```
sub callback {
   println("Dialog was actioned. Button: $2 Values: $3");
}

$dialog = dialog("Host File", %(uri => "/download/file.ext", port => 80, mimetype => "automatic"), &callback);
dialog_description($dialog, "Host a file through Cobalt Strike's web server");

drow_file($dialog, "file", "File:");
drow_text($dialog, "uri",  "Local URI:");
drow_text($dialog, "host", "Local Host:", 20);
drow_text($dialog, "port", "Local Port:");
drow_combobox($dialog, "mimetype", "Mime Type:", @("automatic", "application/octet-stream", "text/html", "text/plain"));

dbutton_action($dialog, "Launch");
dbutton_help($dialog, "https://www.cobaltstrike.com/help-host-file");

dialog_show($dialog);
```

(该窗口在Attacks -> Web Drive-by -> Host File中触发打开)



跟进这个绘制对话框的流程

```
line1-3 ■■callback■■
line5 dialog■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
line6 ■■■■■■■
line8 ■■■■■■■■■
line9-11 ■■■■■
line12 ■■■■■
line14 ■■■■■■■■
line15 ■■■■■■(■■■■■■)
line17 ■■■■
```

0x08 自定义报告

报告处理

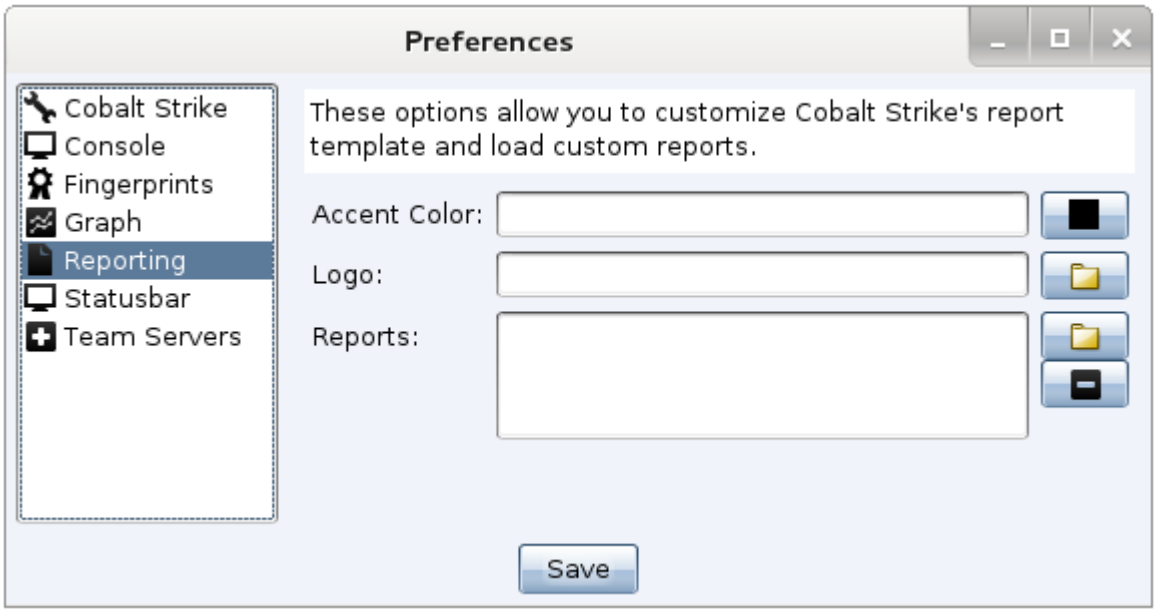
Cobalt Strike使用特定领域的语言来定义其报告，该语言类似于AgScript，但其大多数API均无法访问，报告生成过与AgScript脚本引擎无关。

处理报告的脚本引擎可以访问数据聚合API和一些基元，用以指定Cobalt Strike报告的结构。

default.rpt文件定义了Cobalt Strike中的默认报告的样式。

报告加载

在Cobalt Strike -> Preferences -> Reports中可看到如下窗口



选择完logo文件以及.rpt文件并保存即可在Reporting功能中看到自定义的报告。

错误报告

如果到处报告的过程中发生了未知错误，可在 View -> Script Console中查看错误详情

报告demo

如下demo中的报告并未获取什么实质性内容，仅作为自定义报告的一个demo而已：

```
# default description of our report [the user can change this].
describe("Hello Report", "This is a test report.");

# define the Hello Report
report "Hello Report" {
   # the first page is the cover page of our report.
   page "first" {
       # title heading
       h1($1['long']);

       # today's date/time in an italicized format
       ts();

       # a paragraph [could be the default...
       p($1['description']);
   }

   # this is the rest of the report
   page "rest" {
       # hello world paragraph
       p("Hello World!");
   }
}
```

其中h1函数是输出标题,ts函数输出报告的日期/时间戳,p函数输出段落。详情可参考报告相关的函数

数据聚合API

Cobalt
Strike的报告依赖于数据聚合API来获取其信息，该API为您提供了客户当前连接到的所有团队服务器的数据的合并视图,并提供了评估活动的综合报告，处理报告的这些函数以

总结：

对于大部分开发者而言，摸清楚agScript的基本语法后只需在函数库里面翻翻自己需要的函数就可以轻松写出需要的插件了。

函数库：

```
https://www.cobaltstrike.com/aggressor-script/functions.html
```

点击收藏 | 0 关注 | 1

上一篇：绕过CSRF防御 下一篇：oauth重定向之账号劫持（acc...

1. 0 条回复

- 动动手指，沙发就是你的了！