

Cobaltstrike插件 | CrossC2踩坑记录

原创sp4ce HACK学习呀

2021-01-08原文

前言

CrossC2面向企业自身及红队人员的安全评估框架，支持CobaltStrike对其他平台(Linux/MacOS/...)的安全评估，支持自定义模块，及包含一些常用的渗透模块。

使用

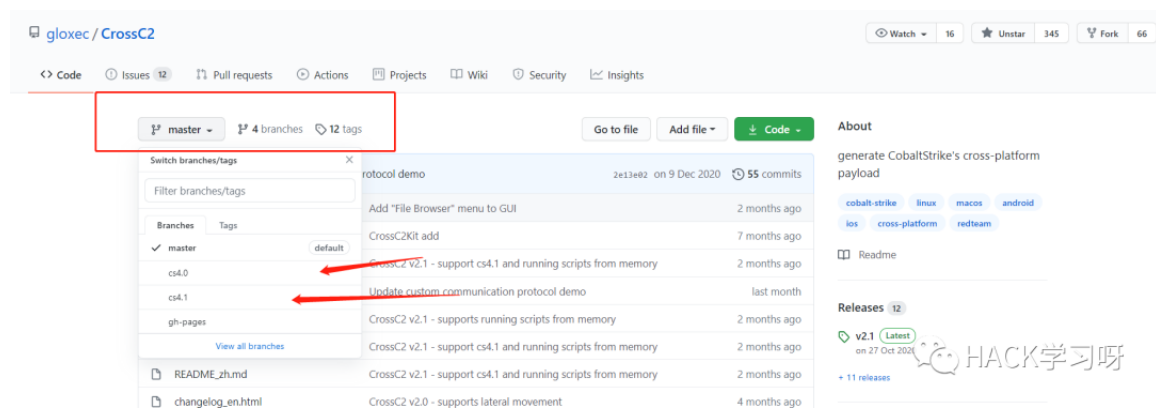
直接下载<https://github.com/gloxec/CrossC2/releases>中的最新版即可，导入CNA后即可使用

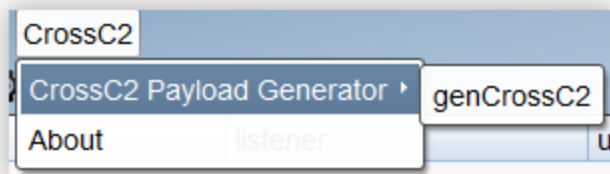
4.0需要下载4.0分支

4.1需要下载4.1分支

分支查看

地址: <https://github.com/gloxec/CrossC2>





HACK学习呀

CrossC2 Payload Generator

Export CrossC2 Payload
<https://github.com/alexer/CrossC2>

URI Path: /a

Web Delivery Port: 55413

Choose: default `./cobaltstrike.beacon_keys` `./cobaltstrike.beacon_keys`

Choose: `rebind_dynamic_lib` `null`

System: Linux

Listener: (reverse_https) Listener: ...

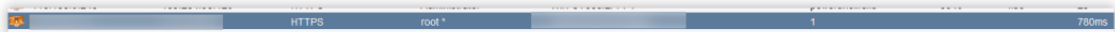
Arch: x64

Payload_Type: Stageless

OutputFileName: CrossC2-test

Build

HACK学习呀

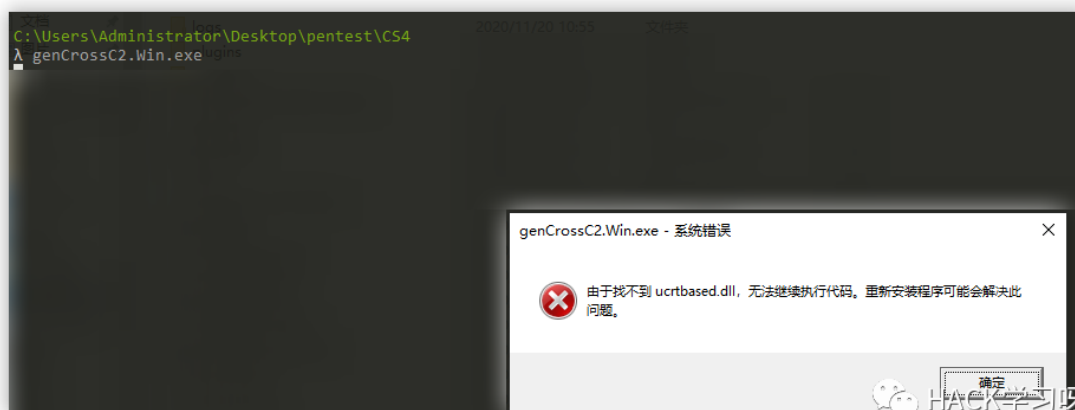


踩坑

由于本机是win10，会出现以下2个问题：

1、丢失 `ucrtbased.dll` 问题

在直接运行genCrossC2.Win.exe时会报错，提示丢失ucrtbased.dll。



解决方案：安装VS2017或VS2019即可解决，文章后面会提供32位的dll下载，下载后移入C:\Windows\System32即可使用

2、windows下无法通过CNA中生成Linux beacon

这个坑浪费了一下午去解决，直接丢解决过程

定位问题

cna插件中的第3、4行需要替换为相应的路径

```
C: > Users > Administrator > Desktop > pentest > CS4 > CrossC2.cna
1  menubar("CrossC2", "generator", 2);
2
3  $CC2_PATH = "C:\\Users\\Administrator\\Desktop\\pentest\\CS4\\"; # <----- fix
4  $CC2_BIN = "genCrossC2.Win.exe";
5
```

第115行的 `$dialog = dialog("CrossC2 Payload Generator", %(uri => "/a", lport => "55413", beaconKey => "./cobaltstrike.beacon_keys", rebind_lib => "null", listener => "Listener: ", system => "System: ", arch => "Arch: ", payload_type => "Payload_Type: ", outputFileName`

```
=> "/tmp/CrossC2-test"), &dialogCallBack);
```

需要修改，Windows中不存在/tmp目录，这里直接改为\$dialog = dialog("CrossC2 Payload Generator", %(uri => "/a", lport => "55413", beaconKey => "./cobaltstrike.beacon_keys", rebind_lib => "null", listener => "Listener: ", system => "System: ", arch => "Arch: ", payload_type => "Payload_Type: ", outputFileName => "CrossC2-test"), &dialogCallBack);，删掉/tmp/，直接生成在CS根目录下

第29行的getSystemInfo

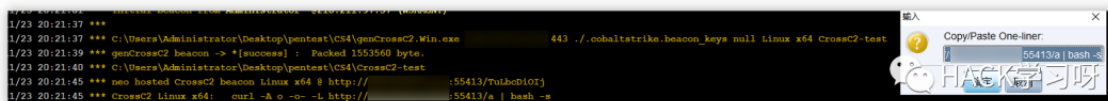
函数，由于Windows中不存在/usr/bin/uname文件，删掉该函数，同时删掉checkSpace函数并全局搜索调用该函数的变量，一并删除。（不知道作者为什么要这么写。。。）

第89行elog("genCrossC2 beacon ->

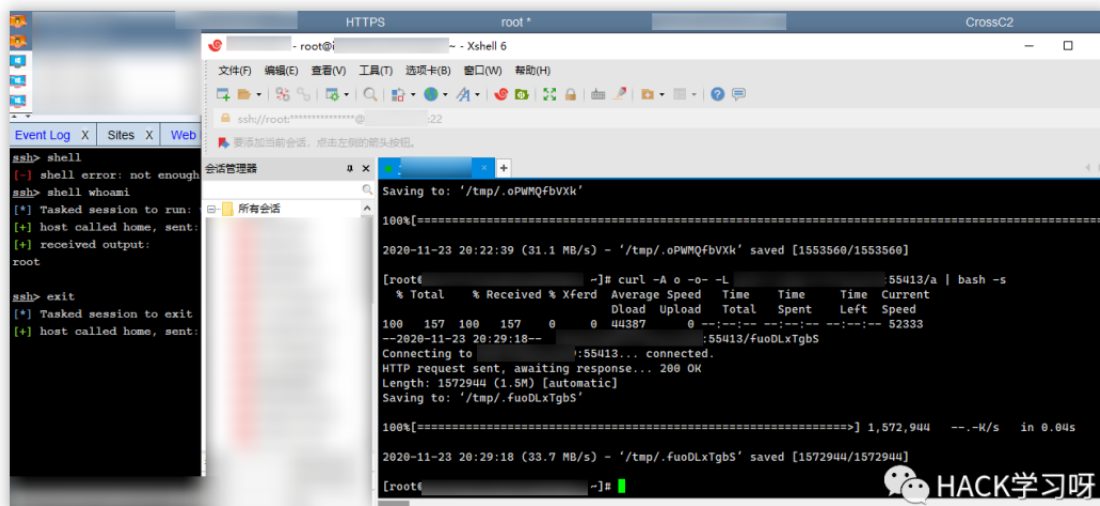
".\$data[13]);更改为elog("genCrossC2 beacon ->

".\$data[12]);，获取生成的大小

最终成果



一键上线



Ucrtbased.dll下载地址

链接:

https://pan.baidu.com/s/1MKIOccCO1ehyoD_q1uA3hg

提取码: fymc

解压密码: hacker1961

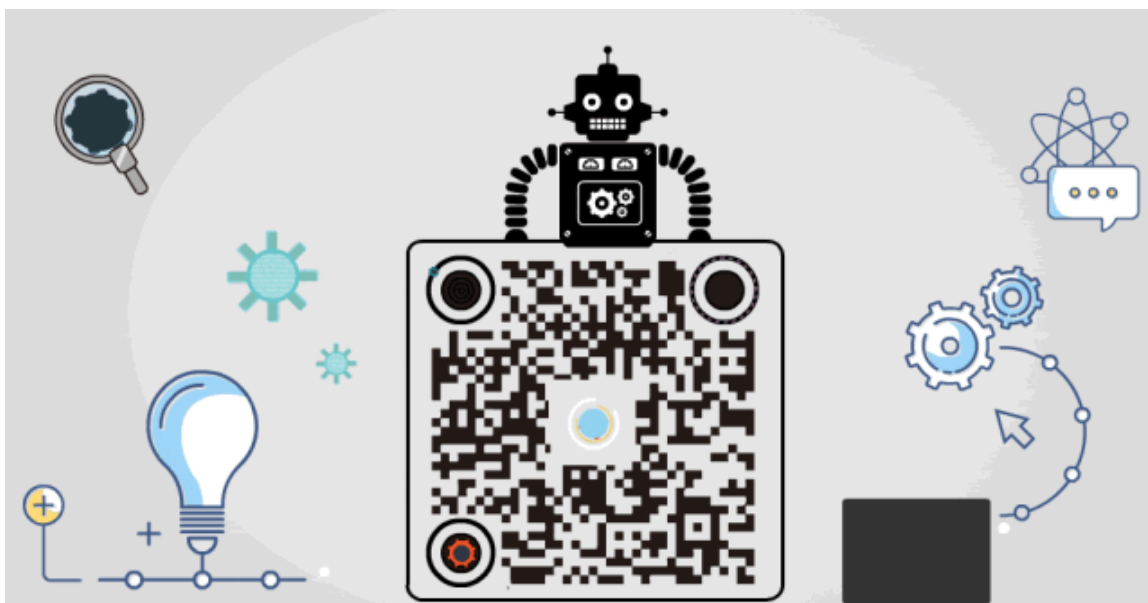


推荐阅读

CS如何配置通过CDN上线

点赞, 转发, 在看

原创投稿作者: Sp4ce



精选留言

用户设置不下载评论