DNS隧道实战&&cobaltstrike利用dns隧道

前言

使用 `dns` 隧道进行 `tcp` 通信。

正文

首先配置域名

记录类型	主机记录	解析线路(isp)	记录值	MX优先级
NS	cok	默认	ns1.hac425.top	--
NS	ns10	默认	ns1.hac425.top	--
NS	ns35	默认	ns1.hac425.top	--
NS	ns34	默认	ns1.hac425.top	--
NS	tcp	默认	ns1.hac425.top	--
A	ns1	默认	45.[redacted].120	--

配置一个 `A` 记录指向我们的 `vps`, 然后配置几个 `ns` 记录，指向刚刚设置的 `A` 记录

然后在服务端安装

```
wget https://launchpad.net/ubuntu/+archive/primary/+files/dns2tcp_0.5.2.orig.tar.gz
tar xvf dns2tcp_0.5.2.orig.tar.gz
cd dns2tcp-0.5.2/
./configure
make
sudo make install
```

新建一个配置文件

```
[root@vultr dns2tcp-0.5.2]# cat my.conf
listen = 45.63.0.120
port = 53
user = nobody
chroot = /tmp
domain = ns10.hac425.top
resources = ssh:127.0.0.1:22,socks:127.0.0.1:1082,http:127.0.0.1:3128
```

然后

```
dns2tcpd -f my.conf -F -d 2
```

接着在客户端 也安装好。

```
dns2tcpc -r socks -z ns10.hac425.top vps_ip -l 8888 -d 2
```

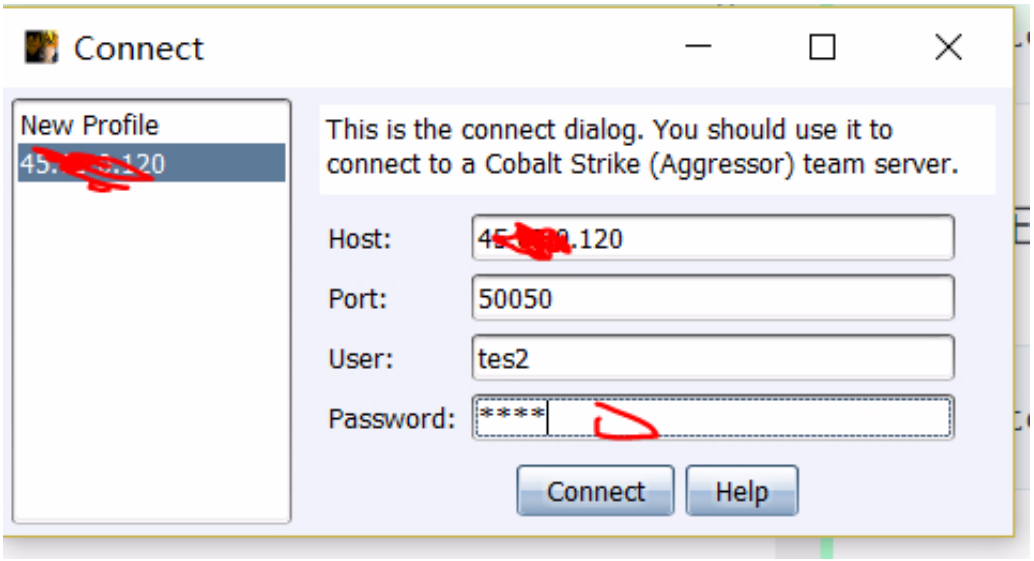
然后访问 B:8888 ---> vps_ip:1082

cobaltstrike

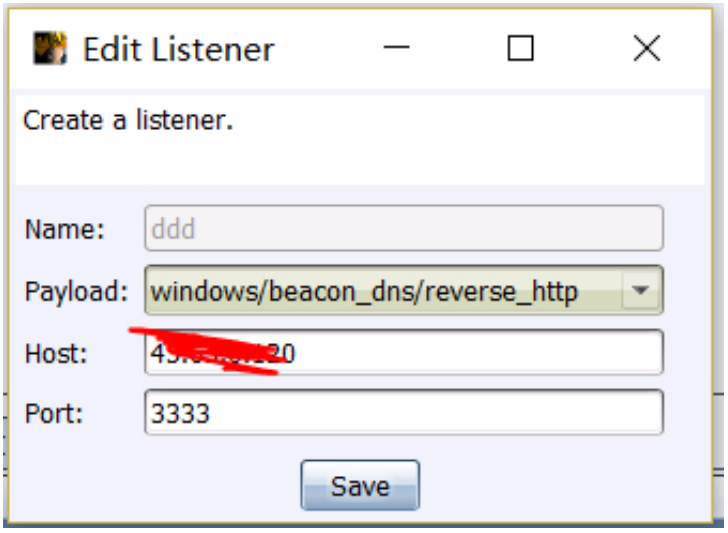
把下好的 cobaltstrike 传到 vps, 装好 jdk, 运行 ./teamserver vps_ip password

```
[root@vultr cobaltstrike]# ./teamserver 45.[redacted]20 1234
[*] Will use existing X509 certificate and keystore (for SSL)
[!] You are using an OpenJDK Java implementation. OpenJDK is not recommended for use with Cobalt Strike. Use O
implementation for the best Cobalt Strike experience.
[$] Added EICAR string to Malleable C2 profile. [This is a trial version limitation]
[+] Team server is up on 50050
[*] SHA256 hash of SSL cert is: 2875f60565051c77c6dbfac9ff42af9f5a164240c0fd190e1c26024f6a3f74b0
[$] WARNING! Beacon will not encrypt tasks or responses! [This is a trial version limitation]
[$] Disabled x86 payload stage encoding. [This is a trial version limitation]
[$] Disabled x64 payload stage encoding. [This is a trial version limitation]
[+] Listener: ddd (windows/beacon_dns/reverse_http) on port 3333 started!
```

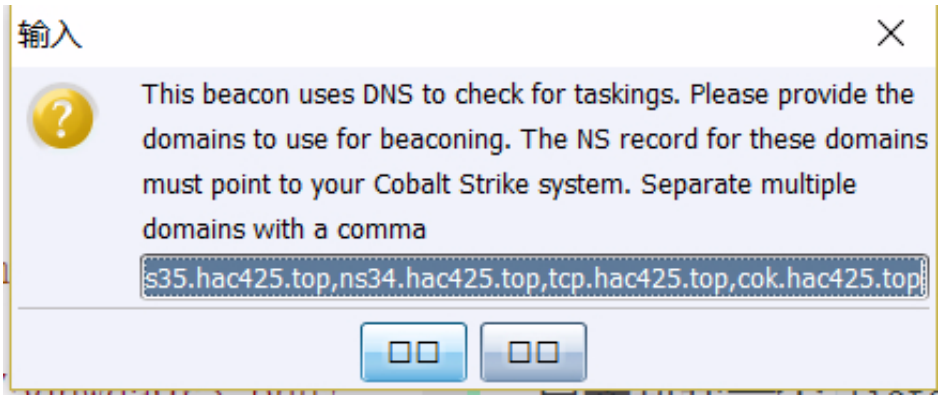
然后本地运行 cobaltstrike.jar, 连接上去，用户名随便写，密码就是运行 teamserver 设置的 password, 在这里就是 1234



首先新建一个 listener

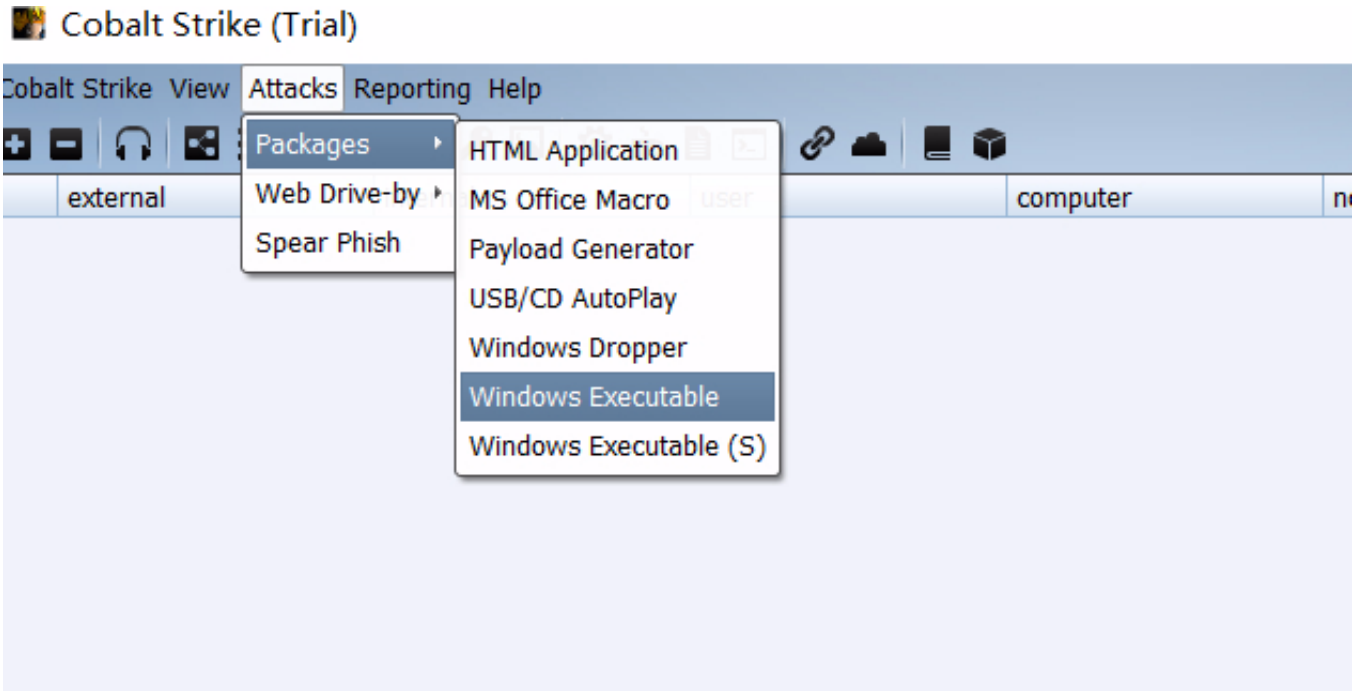


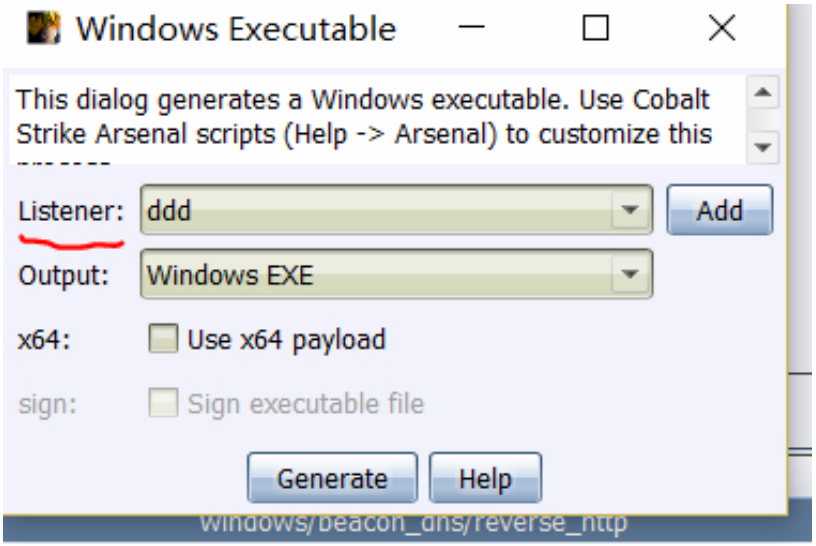
host就是 vps的 ip



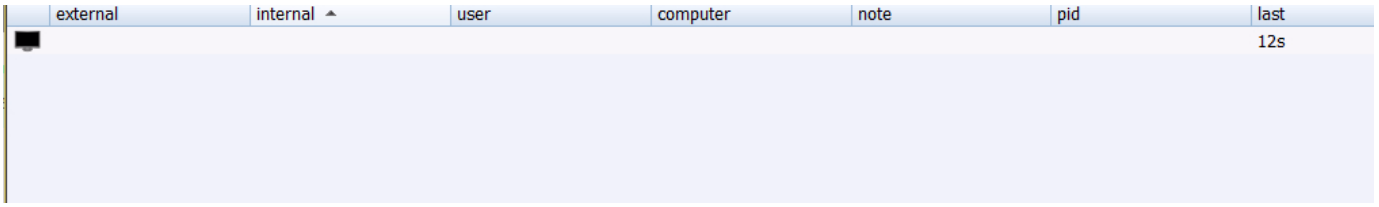
填写设置好 `ns` 记录的 域名，以 `,` 分割

然后新建 `payload`

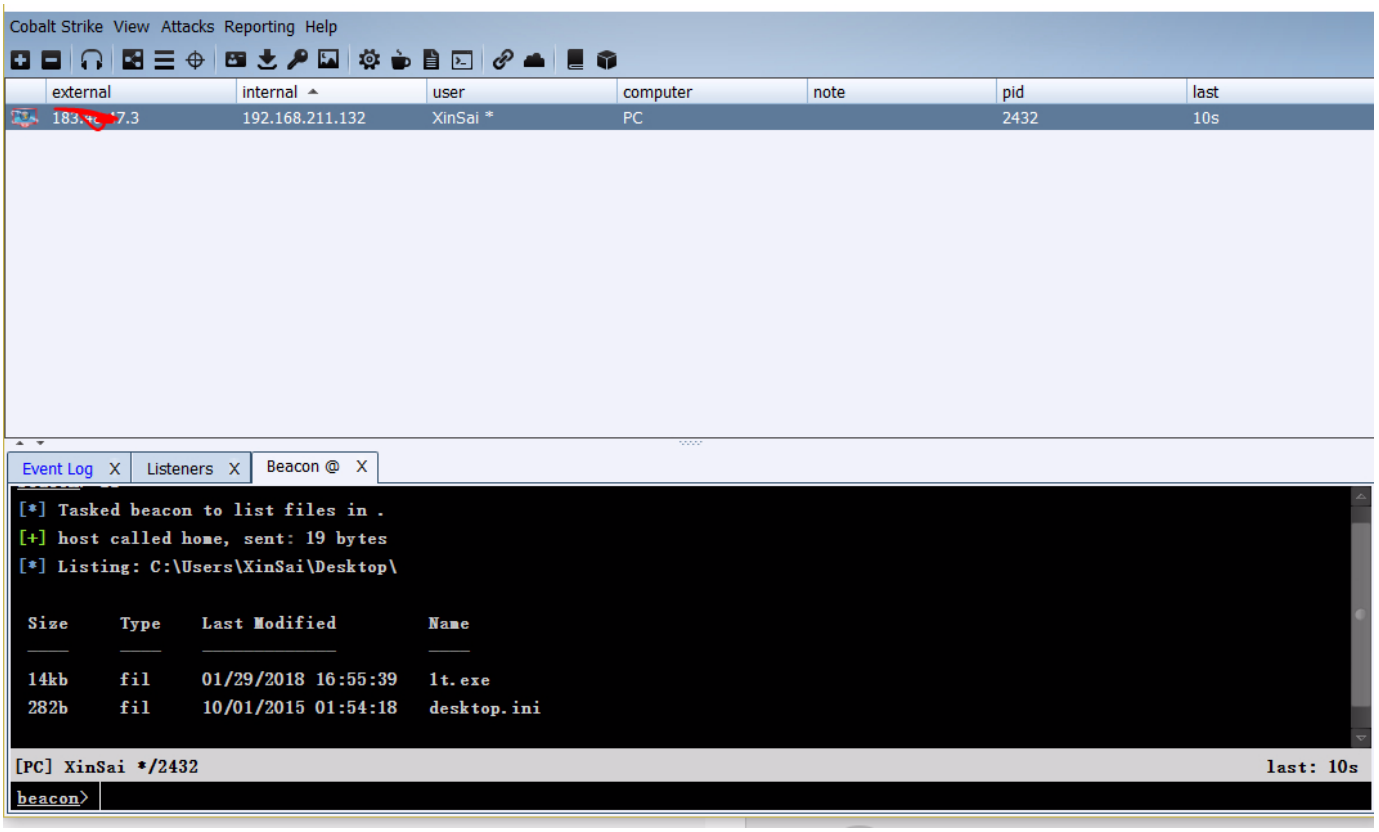




生成文件，运行，过一会儿应该就有了。



此时还得等一会（ dns 比较慢）



变成这个样子就可以进行操作了。

来源： https://www.cnblogs.com/hac425/p/9416926.html