渗透常用命令之文件加解密

渗透过程中，对于一些重要文件，常常需要进行加密处理，以防止信息泄漏。`openssl`可以很方便的对文件进行加解密处理，主要优点为简单快捷，并且可以自定义加密算法。此方法也曾被黑客组织`THC`列入了命令技巧列表之中。

一、加密：

```
openssl enc -aes-256-cbc -pbkdf2 -e -in test.txt -out test.enc
```

> `-aes-256-cbc`：指定加密算法，使用命令`man openssl-enc`查看更多算法
>
> `-pbkdf2`：使用`PBKDF2`算法进行迭代
>
> `-e`：进行加密操作
>
> `-in`：指定输入文件
>
> `-out`：指定输出文件

或

```
openssl enc -aes-256-cbc -pbkdf2 -e -in test.txt -out test.enc -pass
pass:khdxs7
```

> - 此方法会在命令历史中显示明文密码，具有泄漏风险。好处则为无需进行交互。
> - `bash`不会记录开头为`" "`的命令。可以通过在命令前增加一个空格的方式，避免bash对命令进行记录。

二、解密：

```
openssl enc -aes-256-cbc -pbkdf2 -d -in test.enc -out test.dec
```

> `-aes-256-cbc`：指定加密算法
>
> `-pbkdf2`：使用`PBKDF2`算法进行迭代
>
> `-d`：进行解密操作
>
> `-in`：指定输入文件
>
> `-out`：指定输出文件

或

```
openssl enc -aes-256-cbc -pbkdf2 -d -in test.enc -out test.dec -pass
pass:khdxs7
```

> 危害及解决办法同上。

三、文件夹

使用`tar`打包后再使用`openssl`加密。

- 打包

  ```
  tar -cf folder.tar folder
  ```

- 列出包中内容

  ```
  tar -tf folder.tar
  ```

- 拆包

  ```
  tar -xf folder.tar
  ```