

九、压缩和归档

[Linux黑客基础-61-压缩和归档（1）打包工具tar的使用](#)

[Linux黑客基础-62-压缩和归档（2）压缩工具gzip](#)

[Linux黑客基础-64-压缩和归档（4）压缩工具使用案例讲解](#)

[Linux黑客基础-65-压缩和归档（5）压缩工具compress使用](#)

[Linux黑客基础-66-压缩和归档（6）压缩工具7za使用](#)

[Linux黑客基础-67-压缩和归档（7）使用dd创建物理设备的存储副本](#)

Linux黑客基础-61-压缩和归档（1）打包工具tar的使用

What Is Compression? 什么是压缩

将压缩分为有损或无损

.mp3、.mp4、.png 和.jpg 都是有损压缩算法。

有损压缩的优点是它的效率和有效性。压缩比是非常高，这意味着生成的文件比原始文件小得多。

但是对于黑客来说，完整性通常比压缩比重要得多。

Tarring Files Together 将文件存档在一起

工具：tar

tar 命令从许多文件创建一个文件，然后将其称为归档文件、tar 文件或tar 包。

用法: tar [选项...] [FILE]...

NU 'tar' saves many files together into a single tape or disk archive, and can restore individual files from the archive.

常用的选项

<code>-c, --create</code>	创建一个新归档
<code>-f, --file=ARCHIVE</code>	使用归档文件
<code>-v, --verbose</code>	详细地列出处理的文件
<code>-t, --list</code>	列出归档内容
<code>-x, --extract, --get</code>	从归档中解出文件
<code>-r, --append</code>	追加文件至归档结尾
<code>-z, --gzip, --gunzip, --ungzip</code>	通过 gzip 过滤归档
<code>-Z, --compress, --uncompress</code>	通过 compress 过滤归档
<code>-C, --directory=DIR</code>	改变至目录 DIR
<code>-j, --bzip2</code>	通过 bzip2 过滤归档
<code>-J, --xz</code>	通过 xz 过滤归档
<code>--lzip</code>	通过 lzip 过滤归档
<code>--lzma</code>	通过 xz 过滤归档
<code>--lzop</code>	通过 lzop 过滤归档
<code>--no-auto-compress</code>	不使用归档后缀名来决定压缩程序
<code>--zstd</code>	通过 zstd 过滤归档

案例：

```
tar -cf archive.tar foo bar # Create archive.tar from files foo and bar.
```

```
tar -tvf archive.tar      # List all files in archive.tar verbosely.
```

```
tar -xf archive.tar      # Extract all files from archive.tar.
```

练习：

```
cp /etc/netconfig .
```

`cp /etc/host.conf .`

`cp /etc/network/interfaces .`

`tar -cf config.tar host.conf interfaces netconfig` 把多个文件打包成一个文件

`tar -tvf config.tar` 从tar包中显示这些文件，而不需要提取他们

`tar -xf config.tar` 解包

`tar -rf config.tar ssh_config` 把文件追加到包文件

`tar -xzf config.tar.gz` 解压并查看文件

`tar -tvzf config.tar.gz` 查看包文件

`tar -czf net2.tar.gz host.conf interfaces netconfig ssh_config`

`tar -xzf config.tar.gz -C /tmp` 解压至新的目录

Linux黑客基础-62-压缩和归档 (2) 压缩工具gzip

gzip, which uses the extension .tar.gz or .tgz

bzip2, which uses the extension .tar.bz2

compress, which uses the extension .tar.z

compress 是最快的，但是生成的文件是更大的；bzip2 是最慢的，但是生成的文件是最小的；gzip 介于两者之间。

1、gzip (GNU zip)，因为它是Linux 中最常用的压缩实用程序。

Usage: gzip [OPTION]... [FILE]...

`gzip config.tar` 压缩文件

`gzip -d config.tar.gz` 解压缩

`gunzip config.tar.gz` 解压缩

Linux黑客基础-64-压缩和归档 (4) 压缩工具使用案例讲解

用 bzip2 压缩

解压缩

```
bzip2 -d config.tar.bz2
```

```
bunzip2 config.tar.bz2
```

bzip2+tar结合使用

```
.tar.bz2 tar xjf tar xjf config.tar.bz2
```

```
.tar.gz tar xzf
```

案例:

apache-----web服务程序 httpd <https://httpd.apache.org/> HTTP Server ("httpd")

```
wget https://dlcdn.apache.org/httpd/mod\_fcgid/mod\_fcgid-2.3.9.tar.gz
```

如何校验下载文件的完整性?

hash算法---hash值 (指纹) 的比对校验下载文件的完整性

SHA-2 (SHA-256、SHA-512)

```
sha256sum httpd-2.4.57.tar.gz
```

```
bc3e7e540b83ec24f9b847c6b4d7148c55b79b27d102e21227eb65f7183d6b45
```

```
httpd-2.4.57.tar.gz
```

```
cat httpd-2.4.57.tar.gz.sha256
```

```
bc3e7e540b83ec24f9b847c6b4d7148c55b79b27d102e21227eb65f7183d6b45
```

```
*httpd-2.4.57.tar.gz
```

小文件：

方法1：推荐使用lrzsz软件包提供的程序

apt-get install lrzsz 安装软件

rz-----接受文件

sz-----发送文件

大文件：winscp、xftp类似的工具（原理：利用sftp协议实现远程linux文件交互）

tar.gz或tar.bz2文件的解压

.tar.bz2 tar xjf tar xjf config.tar.bz2

.tar.gz tar xzf

Linux黑客基础-65-压缩和归档（5）压缩工具 compress使用

用 compress 压缩

格式：.tar.Z

compress http2

compress 是最快的，但是生成的文件是更大的；bzip2 是最慢的，但是生成的文件是最小的；gzip 介于两者之间。

httpd2.tar.Z compress -d uncompress tar xZf

httpd3.tar.bz2 bzip2 -d bunzip2 tar xjf tar xaf

httpd4.tar.gz gzip -d gunzip tar xzf

httpd.tar

Linux黑客基础-66-压缩和归档（6） 压缩工具7za使用

hashcat---高级的密码破解（hash口令）

<https://hashcat.net/hashcat/>

7za x hashcat-2.00.7z -r -o./

```
(root👁kali) - [~/桌面/密码（hash口令）破解]  
# 7za x hashcat-6.2.6.7z -r -o./
```

-x 代表解压缩文件，并且是按原始目录树解压

-r 表示递归解压缩所有的子文件夹

-o 是指定解压到的目录，-o后是没有空格的，直接接目录。这一点需要注意。

Linux黑客基础-67-压缩和归档（7） 使用dd创建物理设备的存储副本

dd 命令逐个比特位复制文件、文件系统，甚至整个硬盘驱动器。

cp不会复制删除的文件

典型的一个用：

- (1) 磁盘完整的副本制作
- (2) 电子取证
- (3) 应用场景

基本用法：

dd if=输入 of=输出

常用选项：

bs=单位大小 默认是512字节 bs 选项允许您确定要复制的数据的块大小(每个块的读/写字节数)

count+N 指定单位的数量

noerror: 即使遇到错误, noerror选项也会继续复制

例:

```
——(root👁kali)-[~/桌面/work/exam/3]
```

```
└─# ls -l f1
```

```
-rw-r--r-- 1 root root 10485760 4月 10 11:07 f1
```

```
┌──(root👁kali)-[~/桌面/work/exam/3]
```

```
└─# ls -lh f1
```

```
-rw-r--r-- 1 root root 10M 4月 10 11:07 f1
```

案例2: 为指定U盘做一个副本

```
dd if=/dev/sdb of=/root/flashcopy
```

案例3:

```
dd if=/dev/media of=/root/flashcopy bs=4096 conv=noerror
```