rmqtt

H3 攻击场景与漏洞危害

考虑共享场景下的物联网应用，即智能家居系统使用MQTT协议进行物联网设备和用户管理，其中有两个用户角色。管理员（即房主）可以授权其他普通用户（例如，客人、租户）访问他的智能家居设备的权利。普通用户的访问权限可能会被撤销（租约到期）。我们认为管理员和设备是良性的，而客人可能是恶意的，会尽可能地去试图越权访问设备（越权或是维持被撤销的权限）。

H5 0x01攻击场景

首先，攻击者拥有连接broker的权限。

01. 受害者（订阅者）连接Broker，并订阅了相关话题（比如“testtopic”）
02. 攻击者连接到Broker（我们认为攻击者具有连接权限），并且在连接时指定will topic为“testtopic”，消息内容为根据攻击者的意愿可以为“unlock”（注意，攻击者不具有发布权限）
03. 攻击者通过直接断开网络连接来伪装网络错误造成的掉线

04. broker认为攻击者的连接异常断开，投递其will message（但是攻击者不具备发布权限）
05. 受害者收到broker投递的消息（内容可由攻击者决定）

H5 0x02漏洞危害

攻击者能够在没有发布权限的情况下向订阅者发布消息（时机取决于攻击者何时断开连接，消息内容和话题都可以由攻击者控制）。未授权访问可能导致攻击者在没有发布权限的情况下，向智能门锁的控制话题发布解锁命令，打开智能门锁。

H3 测试

H5 0x01测试环境

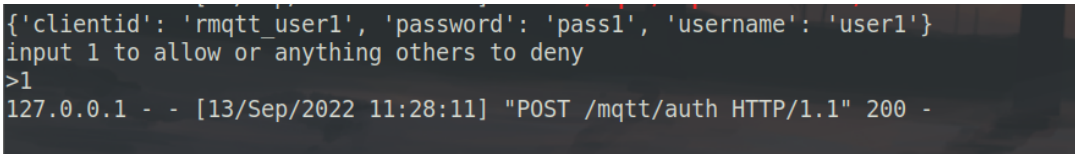
rmqtt v0.2.3

测试时使用rmqtt自带的rmqtt-auth-http插件

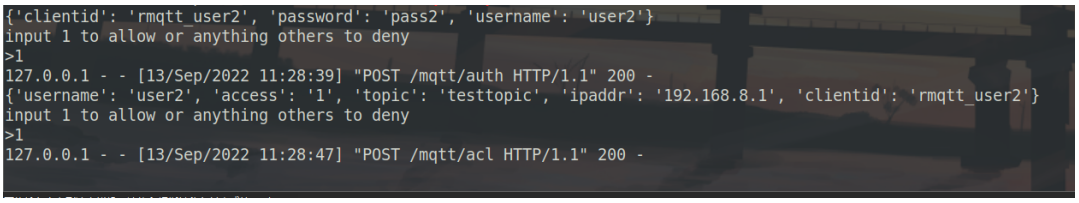
H5 0x02测试步骤

因为MQTTX客户端仅支持正常断开连接，因此使用python脚本模拟客户端连接到broker

- user1的客户端（作为攻击者）连接到broker，连接时指定will topic为“testtopic”，消息内容随意，连接时授权服务器将收到http请求（请求内容为user1的连接申请，但没有检查发布权限），我们认为user1具有连接权限，因此通过发送状态码为200的http响应来表示允许连接，如图，只收到了连接的权限检查请求



- user1连接后再使用user2（表示正常客户端）发起另一个连接，连接后订阅“testtopic”主题，我们认为user2具有连接和订阅权限，因此通过分别发送状态码为200的http响应来表示允许连接和订阅



- 在此之后user1直接关闭自己的网络连接（Ctrl+c退出脚本程序）

```
PS C:\Users\Rain\Desktop\MQTT\漏洞上报\rmqtt\rmqtt_unauthorized_will_message> python .\adversary.py
Connected with result code Success
except
PS C:\Users\Rain\Desktop\MQTT\漏洞上报\rmqtt\rmqtt_unauthorized_will_message>
```

- 此时user1 的连接断开，并且user2的连接收到了user1的will message（但是user1并不具有发布权限）