**IPTV机顶盒FUZZ简述**

1. **机顶盒相关**

机顶盒进行一次PPPOE拨号，连接到电信的专用网络，盒子内置直播APP访问专网的指定地址实现节目观看。现在的连接方式我们不好抓包，最好是让观看的线路经过我们的电脑，这样抓包更直接有效。我的方法是将IPTV口的网线连接到电脑的网口，由电脑PPPOE拨号连接到电信的专网，再用电脑的无线网卡进行WIFI共享，IPTV盒子通过WIFI连接到电脑进行漏洞挖掘，这时候在电脑上运行抓包软件，就能获取相关源的连接地址

**二．机顶盒漏洞挖掘步骤**

1.配置机顶盒连接到电视机（显示器）

2.电脑（攻击机器）需开启wifi共享

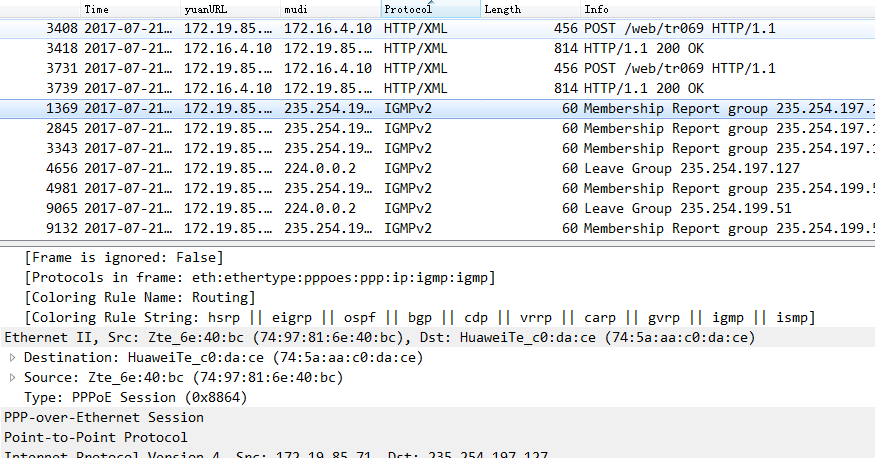
3.通过机顶盒设置连接到电脑开启的wifi（机顶盒设置弱口令123456）

3.在电脑上面开启Wireshark或BURP等抓包工具

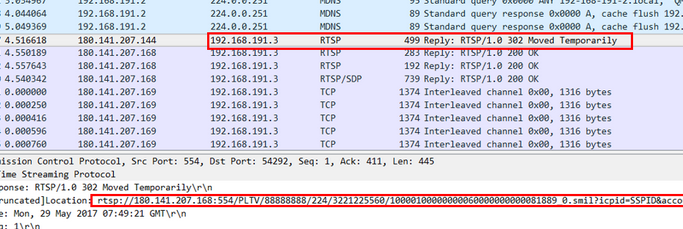
三．**机顶盒漏洞挖掘过程**

1.在wireshark或burp抓包工具上面开启抓包后，使用遥控器控制连接机顶盒的电视机不断进行电视节目更换或相关操作。

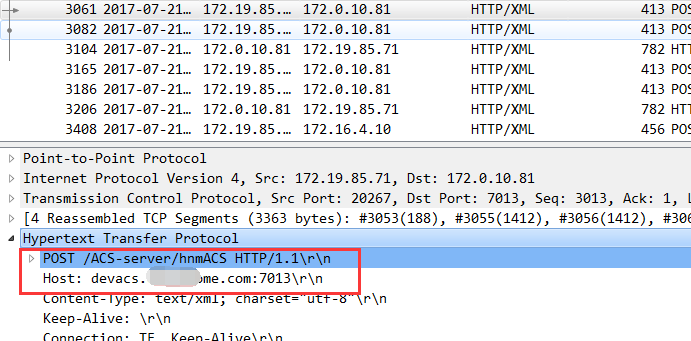
2.在wireshark抓包工具上面对操作过程的流量进行获取分析



1. 重点分析协议（IGMP、RTSP、HTTP）等
2. 对流量内的请求地址进行分析比对后进行保存（留着最后FUZZ攻击）
3. IGMP和RTSP协议存在但不限于泄露源播放地址、远程服务器等敏感信息泄露漏洞



1. HTTP协议存在但不限于WEB TOP10漏洞，深入即可对远程服务器进行攻击



相关导读链接：

Openwrt与IPTV之一----igmpproxy代理

<http://www.cnblogs.com/harryzwh/p/4279316.html>

IPTV 抓包探讨

<http://www.right.com.cn/forum/forum.php?mod=viewthread&tid=240468&highlight=%D7%A5%B0%FC>

IPTV 抓包2

<http://www.right.com.cn/forum/thread-240466-1-2.html>