Wireless Ad-hoc Network Exp1 report

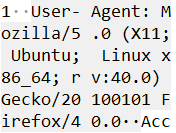
刘昱辰 0840042

Wiresharck Packet Sniff

Q1. Can you get any detail information from received packets for HTTP, FTP, Telnet and SSH via Open Access AP!?

1. HTTP:





接收端使用火狐浏览器，在ubuntu64位操作系统下向网址请求html页面。



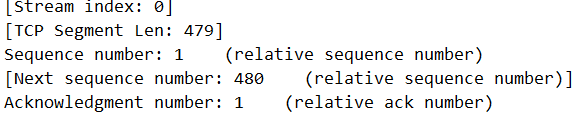
同样也可以看到接受的语言和编码方式。



以及完整的URL请求，192.168.0.1是路由器保留地址。

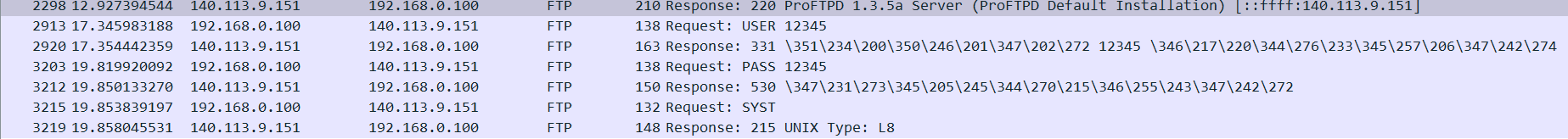


端口是http常用端口80。



因为http是基于tcp的，会有滑动窗口的大小，封包序列号等信息。

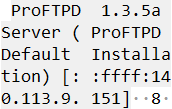
1. FTP



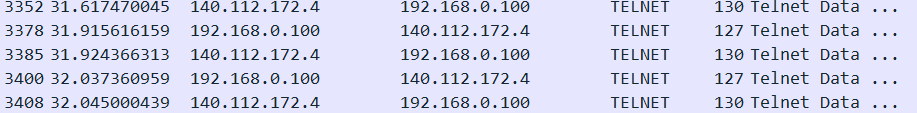
用户名：12345

密码：12345

通过三次交互建立连接，基于TCP



1. Telnet



连续的几个telnet封包，封包未加密，可以看到其中的data。

在telnet中每次敲击一下键盘，就会产生一个telnet封包，因此我们可以看到这几个封包的内容均为一个字母。







1. SSH



可以从封包内容中看到ssh所用的协议版本号为OpenSSH\_6.6.1，在ubuntu系统上运行。

SSH交换的过程中还会有登陆密钥交换的过程。





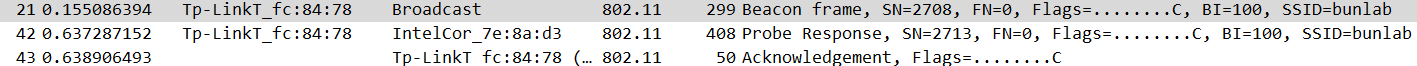
之后的封包会被加密。

Q2. Can you get any detail information from received packets for HTTP, FTP, Telnet and SSH via Encrypted AP!?



在加密的传输中进行封包嗅探，可以接收到封包却无法进行解析，使用过滤器搜索tcp未显示任何结果说明了这点（HTTP, FTP, Telnet, SSH都是基于TCP的）。

搜索AP的MAC地址，显示出的协议类型仅为802.11，无法显示更多信息。



能解析出来的封包只有以下几种不进行加密的类型。



广播的Beacon封包。



RTS封包。



ACK封包。

以下的这个QoS Data表示的是收到的加密封包，因为上一题的四种封包均是有服务质量保障的。但是因为进行了加密，无法对具体内容进行解析，显示如下。



