< 2016年11月 >

日	一	二	三	四	五	六
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

公告

昵称：懒懒的小猪
园龄：11个月
粉丝：0
关注：4
+加关注

Ubuntu下用wireshark抓取802.11封包并进行过滤分析

要用wireshark抓802.11的包 需要在linux下进行。

要在linux下抓802.11的包 需要在linux下安装无线网卡驱动。

所以 在正式抓取之前先把这两样东西搞起来。

没有特殊说明，均使用root权限 sudo su

一 安装无线网卡驱动

无线网卡：DWA-160 USB无线网卡

网卡驱动：http://alris1.dlinkddns.com/download/dlink/DWA-160/DWA-160_B2_DPO_RT5572_LinuxSTA_2.6.1.3_20121022.tar.bz2

DWA-160_B2_DPO_RT5572_LinuxSTA_2.6.1.3_20121022.tar.bz2 解压=>

DWA-160_B2_DPO_RT5572_LinuxSTA_2.6.1.3_20121022文件夹

安装步骤：

在DWA-160_B2_DPO_RT5572_LinuxSTA_2.6.1.3_20121022文件夹下执行以下命令：

```
# make
# make install
# cp RT2870STA.dat
/etc/Wireless/RT2870STA/RT2870STA.dat
```

统计
随笔 - 31
文章 - 0
评论 - 0
引用 - 0

搜索
找找看
谷歌搜索

常用链接
我的随笔
我的评论
我的参与
最新评论
我的标签

我的标签
ubuntu(17)
freeradius(9)
eap(5)
WLAN(4)
python(3)
mschapv2(3)
mysql(3)
md5(2)
tls(2)
ttls(2)
更多

随笔档案
2016年9月 (4)
2016年5月 (8)
2016年3月 (4)
2016年1月 (4)
2015年12月 (9)
2015年11月 (2)

阅读排行榜
1. Ubuntu下freeradius的EAP-MD5，PEAPv0/EAP-MSCHAPv2，EAP-TTLS/MD5，EAP-TTLS/MSCHAPv2方式认证(基于mysql)(264)
2. Ubuntu下iperf的安装(260)

```
# cd ./os/linux
# insmod rt5572sta.ko
```

不出意外，到这里就可以连接到wifi了

二 安装**wireshark**

wireshark的安装非常简单

```
# apt-get install wireshark
```

就可以了。

三 使用**wireshark**抓**802.11**封包

- 需要注意的是

因為工作的緣故，需要去監聽無線網路的封包，特別是IEEE802.11的管理控制訊框（frame ... 其實我還是比較喜歡直接叫作封包）。同事直接打開 wireshark 卻擷取 wifi 介面，卻發現聽到了一堆 ethernet 的訊框而聽不到 wifi 的訊框。為什麼呢？來看看 wireshark 的官網怎麼說：

If you're trying to capture network traffic that's not being sent to or from the machine running Wireshark or TShark, i.e. traffic between two or more other machines on an Ethernet segment, or are interested in 802.11 management or control packets, or are interested in radio-layer information about packets, you will probably have to capture in "monitor mode". This is discussed below.

Without any interaction, capturing on WLAN's may capture only user data packets with "fake" Ethernet headers. In this case, you won't see any 802.11 management or control packets at all, and the 802.11 packet headers are"translated" by the network driver to "fake" Ethernet packet headers.

答案揭曉，原來這是因為 wifi driver 會自動把 wireless frame 轉成 ethernet frame 後再給 kernel，這樣 kernel 裏面的 protocol stack 會比較好處理。

問題是，如果我想要聽到 wifi frame 的話，要怎麼做呢？答案很簡單，將 wifi adapter 設成 monitor mode。在 wifi adapter 中，通常都有 SSID/ESSID filter，所以就算把 wifi adapter 設定成為 promiscuous mode 也沒有用，因為還是無法收到非自己加入的 SSID 的 frame。那 monitor mode 呢？我們可以看看下面這句話：

In monitor mode the SSID filter mentioned above is disabled and all packets of all SSID's from the currently selected channel are captured.

最後的問題就是，如何在 Linux 裏面把無線網卡設定成 monitor mode了。步驟如下：

```
1.      iw dev wlan0 interface add mon0 type monitor
2.      ifconfig mon0 up
```

接下來就可以透過 mon0 這虛擬介面來聽封包了。要移除這介面的方法也很簡單：

```
1.      iw dev mon0 interface del
```

所以要做完上述设定之后再打开wireshark

```
# wireshark
```

四 打开**wireshark**出现的异常解决

错误如下：

直接运行wireshark的话会报错：

```
Lua: Error during loading:
[string
"/usr/share/wireshark/init.lua"]:45: dofile
has been disabled
```

解决方案：修改init.lua要对其进行修改，终端运行

```
sudo gedit /usr/share/wireshark/init.lua
```

倒数第二行原来为：

```
dofile(DATA_DIR.."console.lua")
```

改为：

```
--dofile(DATA_DIR.."console.lua")
```

五 对抓到的**802.11**包进行过滤

```
在Expression下Field name为
"802.11 MGT - IEEE 802.11 wireless LAN
management frame"
"802.11 Radiotap - IEEE 802.11 Radiotap
Capture header"
"IEEE 802.11 - IEEE 802.11 wireless LAN"
"IEEE 802.11 Aggregate Data - IEEE 802.11
wireless LAN aggregate frame"
"WLANCERTEXTN - Wlan Certificate Extention"
"Wi-Fi P2P - WiFi Peer-to-Peer"
"WiMax (wmx) - WiMax protocol"
...
中进行查找所需条件

下面列出一些比较常用的条件表达式

wlan.da - Destination address (Destination
Hardware Address)
wlan.sa - Source address (Source Hardware
Address)
wlan.addr - Source or Destination address
(Source or Destination Hardware Address)
wlan.ra - Recevier address (Receiving
Station Hardware Address)
wlan.ta - Transmitter address (Transmitting
Hardware Address)
wlan.bssid - BSS id (Basic Service Set ID)
wlan_mgt.ssid - SSID (Indicates the
identity of an ESS or IBSS)
wlan.fc.type_subtype - Type/Subtype (Type
```

```
and subtype combined (first type: type,
second type:subtype))
```

六 简单的**802.11**封包分析

至此 就可以自如的进行抓包了

下面是一些简单的分析

802.11帧的抓取以及分析

802.11抓包分析

至于高级一点的包的分析，等我学会了再回来写

标签: ubuntu, WLAN, wireshark

好文要顶 关注我 收藏该文

懒懒的小猪
关注 - 4
粉丝 - 0
+加关注

0 0

« 上一篇：win7下KiWi Syslog服务器的安装与配置
» 下一篇：用AE (Adobe After Effects) 处理视频

posted on 2016-01-20 16:31 懒懒的小猪 阅读(187) 评论(0) 编辑 收藏

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论，请 登录 或 注册，访问网站首页。

最新**IT**新闻:
· 社交越热闹，社会越失败？ 黑镜剧透慎入
· 【特写】华强北的守望者
· 小米无人机停产、研发团队撤离？蔡炜：谣言！
· 数据造假黑产技术帖：如何给微信公众号、微博大V、直播网红刷量
· 张小龙：这是特别可怕的事情
» 更多新闻...

最新知识库文章:
· 循序渐进地代码重构
· 技术的正宗与野路子
· 陈皓：什么是工程师文化？
· 没那么难，谈CSS的设计模式
· 程序猿媳妇儿注意事项
» 更多知识库文章...