路由器宽带帐号便携式窃取攻防实验

杨芸菲 | 360天马安全团队安全研究员

FIT · FREEBUF

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
东北大学无线安全课程客座讲师

- 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》

路由器黑科技—“一键换机”

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 ...

HACK DEMO

PPPoE 协商过程

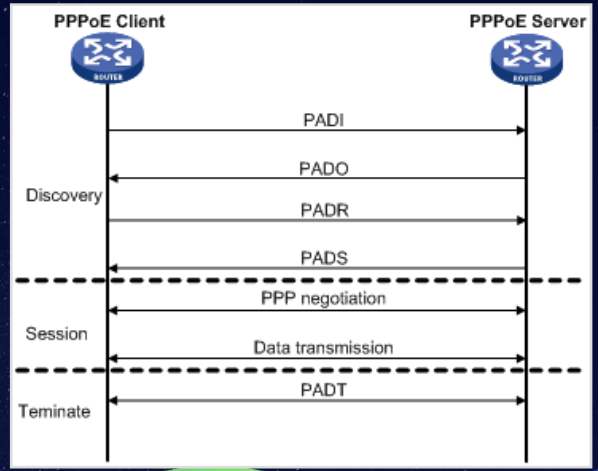
两个阶段：

1. 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。

2. 会话（Session）

PPP会话阶段



PPP会话

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

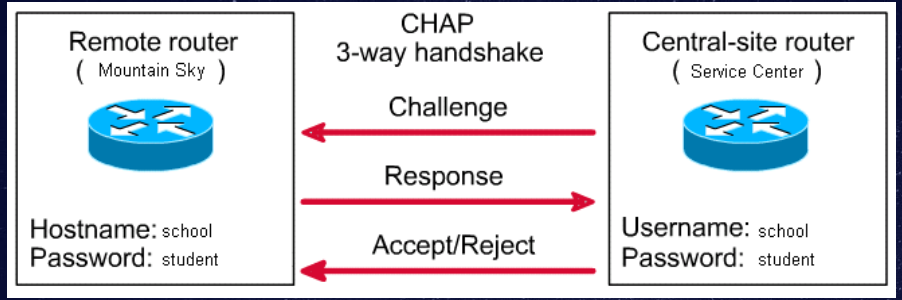
●会话维持

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。

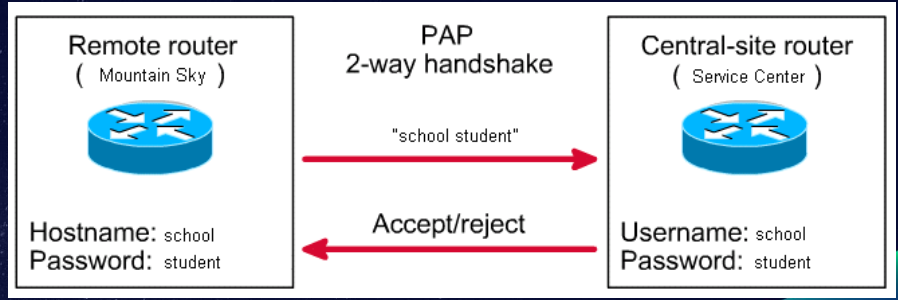
●会话结束

会话建立后的任何时候发送PADT，终止PPPoE会话。

CHAP Authentication



PAP Authentication



攻击面

缺陷：

- 客户端、服务端双方缺少有效的身份确认机制。
- 认证类型由双方协商决定。

攻击流程：

- 搭建PPPoE服务器，配置PAP认证。
- 连接PPPoE服务器至路由器WAN端口。
- 监听网卡捕获PPPoE PAP认证包，获取明文密码。

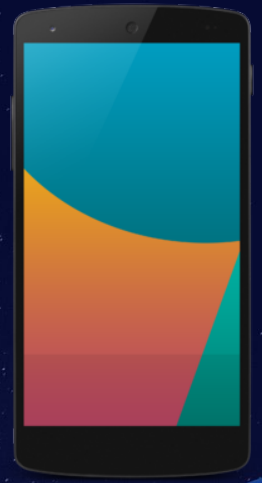
“鸡肋”漏洞

过去：

- 攻击成本高
  - 物理接触
  - 不易携带
  - 设备成本
- 账号信息价值不高

如今：

- 账号包含个人信息
  - 姓名拼音
  - 身份证后6位
- 移动设备的普及
  - 成本降低
  - 便携化



HACK DEMO

极简的部署过程

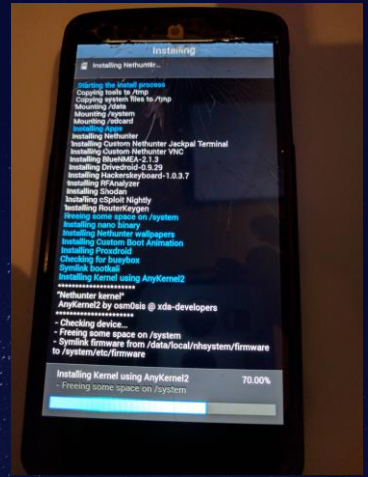
Dependent:

- Nethunter
- PPPoE Server
- Tshark

Script:

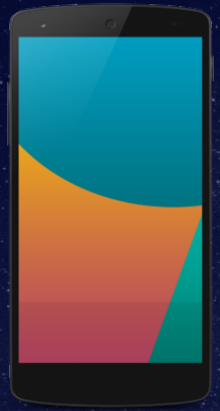
pppoe-server -L 10.5.5.1 -R 10.5.5.10 -I eth0 -S yyf

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



HACK DEMO

Demo Time



思考

许多含有缺陷的协议依然被广泛使用，比如GSM、GPS。因为客观需要没法直接禁止，但对它们的攻击门槛却逐渐降低。

它们的问题除了需要行业的主动推进，还需要等待终端设备的更新换代才能完全解决。

而这个时间可能长达数十年。

Thanks

qingxp9@gmail.com