Atitt info scr 信息安全 lan 局域网嗅探

192.168.0.23192.168.0.23

目录

[1. 嗅探 获取敏感信息 1](#_Toc32161)

[1.1. Ip 与mac地址 1](#_Toc23052)

[1.2. 账号窃取 1](#_Toc1675)

[2. 嗅探方法 1](#_Toc11322)

[2.1. 嗅探mac地址ARP -a 1](#_Toc10330)

[2.2. 端口镜像 2](#_Toc24676)

[2.3. ARP欺骗攻击 2](#_Toc5942)

[3. Ref 3](#_Toc26981)

# 嗅探 获取敏感信息

## Ip 与mac地址

## 账号窃取

③ARP扫描+账号窃取（网站、邮箱、各种）；最强的莫过于Windows下的Cain，当然还有跨平台的Ettercap（需配合其他工具）

# 嗅探方法

## 嗅探mac地址ARP -a

接口: 192.168.0.23 --- 0x11

Internet 地址 物理地址 类型

192.168.0.1 00-1a-9a-de-ad-05 动态

192.168.0.12 86-3d-ca-4d-27-b8 动态

192.168.0.20 00-27-15-b6-b0-38 动态

192.168.0.25 5a-97-77-7f-82-6f 动态

192.168.0.26 ae-d2-76-0e-dd-f5 动态

192.168.0.29 e2-4a-0b-d8-d5-19 动态

192.168.0.255 ff-ff-ff-ff-ff-ff 静态

224.0.0.251 01-00-5e-00-00-fb 静态

224.0.0.252 01-00-5e-00-00-fc 静态

239.11.20.1 01-00-5e-0b-14-01 静态

239.255.255.250 01-00-5e-7f-ff-fa 静态

接口: 172.27.32.1 --- 0x2a

Internet 地址 物理地址 类型

172.27.47.255 ff-ff-ff-ff-ff-ff 静态

224.0.0.22 01-00-5e-00-00-16 静态

224.0.0.251 01-00-5e-00-00-fb 静态

224.0.0.252 01-00-5e-00-00-fc 静态

239.11.20.1 01-00-5e-0b-14-01 静态

239.255.255.250 01-00-5e-7f-ff-fa 静态

## 端口镜像

其次，检查路由器和交换机能不能支持“端口镜像”？支持的话，设置一个镜像端口。把安装监控软件的电脑接在镜像口就可以进行嗅探。免费的软件一般就用wireshark，收费的就多了（比如：WFilter）。

## ARP欺骗攻击

3. 如果硬件没有端口镜像支持，只能用ARP欺骗。不过对方有ARP防火墙的话，会提示攻击。所以不建议用。

可以在命令行窗口内输入 ARP -a 查看[路由表](https://www.zhihu.com/search?q=%E8%B7%AF%E7%94%B1%E8%A1%A8&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"article","sourceId":135263739}" \t "https://zhuanlan.zhihu.com/p/_blank)，如果发现你的网关的Mac地址，和局域网内某台主机的Mac地址相同，那么恭喜你中宝！如果是在公司那么有可能你的一些隐私已经被泄露。

局域网内主机的正常上网通信是通过和网关进行交互的。而“ ARP欺骗攻击 ”就相当于把“ 攻击者”的主机变成了中间商，这个中间商也真实可恶，俩边的数据通吃不误，关键的是吃完喝完，还不会让你发现他的存在。  
  
wifi 嗅探，这个是一个非常古老的技术 ，主要是利用ARP 技术 ，

但是Arp 利用得好，就是一个神器 ，可以进行vpn 通讯数据过滤 ，代理中间人数据解密 等等，

无论是路由器还是交换机连接，既然都是『局域网』和『内网』，那么监听嗅探的方法基本都是一致的，就是要用到『ARP欺骗攻击』技术。如果你是网络管理员的话，那就根本不用做这种『小偷行为』，堂堂正正在网络设备上面开启端口镜像，然后在电脑上安装Wireshark、科来网络分析等软件，对网络进行正常分析。  
  
2、强调一遍：无论是有线网络还是无线网络（WiFi），同一个局域网内，基于ARP欺骗实现的流量监听和嗅探都是适用的。  
  
3、常见的局域网ARP嗅探渗透工具：  
  
①无毒无害型的仅具备ARP扫描功能，用来发现内网主机；例如Metasploit里面的arping/arpscan相关模块；  
  
②ARP扫描+流量控制（限速或限制能上哪些网站和应用）；例如Windows下的P2P终结者；  
  
③ARP扫描+账号窃取（网站、邮箱、各种）；最强的莫过于Windows下的Cain，当然还有跨平台的Ettercap（需配合其他工具）  
  
带网管功能的交换机的话直接用端口镜像功能，然后进行抓包  
  
普通的交换机还是用ARP欺骗攻击然后再抓包

# Ref

局域网嗅探截取登陆密码 - 知乎