Cain 在 windows 下的应用

CAIN 是一个 WINDOWS 平台上的破解各种密码，嗅探各种数据信息，实现各种中间人攻击的软件。

首先下载 cain 软件

CAIN 下有两个程序，一个是 CAIN 主程序，一个是 Abel 服务程序。Abel 服务程序需要手动进行安装。正确安装 CAIN 后从 CAIN 目录下拷贝 Abel.exe 和 Abel.dll 到 C:\Windows\System32 目录下，运行 Abel.exe 安装，并在服务里设置为自动启动。运行 CAIN，主界面如图所示

我们先来看看 CAIN 的几个大类的使用，大类页面如下图

1）解密器：

解密器的作用主要是读取缓存中保存的各种密码。你可以点击左边的各选项然后点击上面的。

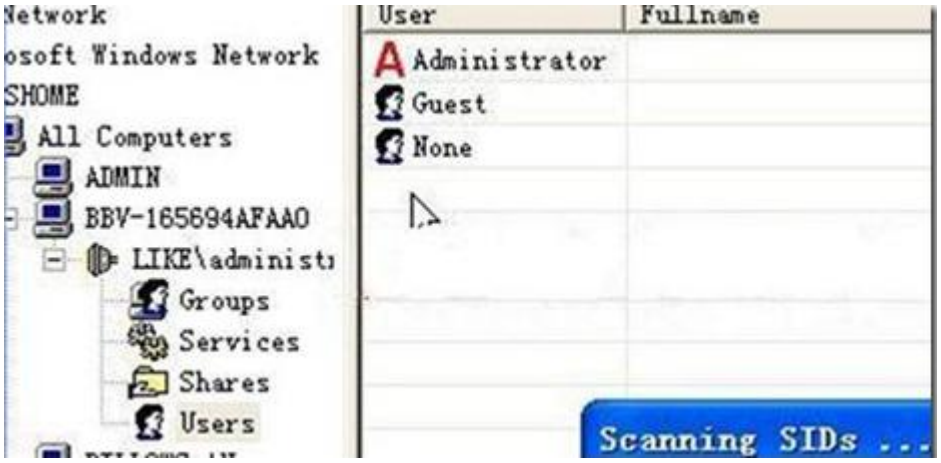
你就可以在右边的窗口看到保存在缓存中的密码。我的电脑中我都看到了我 MSN 的账号和密码，曾经登陆路由的账号和密码，邮箱的密码。

2）网络

这个网络主要用来鉴别各域控制器，SQLserver，打印服务，远程拨入，终端服务等。网络的左侧用来浏览网络结构和连接远程主机。连接到主机就可列出

用户名，工作者，服务，共享资源等。如下图，我们清楚的看到 SMM-DB1 开启了 IPC$默认共享连接和文件夹共享。

同时也可以搜索到计算机的用户组和组的用户名，虽然 NT 版本以后不能建立空连接了，但是还是可以通过提取 SID 来获得 Admin 的账号，因为管理员的 SID 总是 500。如下图所示



3）嗅探器（包含局域网的嗅探和 ARP 欺骗）

嗅探器是 CAIN 的重点，很多人用 CAIN 主要就是用这个嗅探器和 ARP 欺骗。CAIN 中的嗅探器，主要嗅探局域网内的有用信息，比如各类密码等。CAIN 中的 ARP 的欺骗，原理是操纵两台主机的 ARP 缓存表，以改变它们之间的正常通信方向，这种通信注入的结果就是 ARP 欺骗攻击，利用 ARP 欺骗可以获得明文的信息。

1．程序配置

首先点击菜单的配置按钮

出现下图所示的配置菜单

首先选择用于嗅探的以太网卡（可以是有线网卡也可以是无线网卡），本文中将选择第二个无线网卡。下面的选项可以不选。然后转到 ARP 欺骗选项卡。欺骗选项中可以用真实的 IP 地址也可以使用伪装 IP 地址和的 MAC。

但是使用伪装 IP 和 MAC 有几个前提条件：

1. 攻击者的机器只能连接在 HUB 中，不能连接在交换机中。

2. 设置的 IP 地址需是子网内的合法的而且是未使用的 IP 地址预欺骗 ARP 缓存勾选，下面默认每 30 秒发送一次 ARP 欺骗包。XP 系统每 2 分钟更新 ARP 缓存，因此设置太大就不能达到欺骗的效果，设置太小会产生太多的 ARP 流量，如下

图所示。

接下来看看其他的几张选项卡，如下图

这两张选项卡中 HTTP 区域主要定义了 HTTP 的字段，用来检查和过滤 HTTP 包中包含的敏感字符，比如用户名密码等。过滤与端口选项是 CAIN 定义的过滤程序和协议的各种端口，你可以关闭你不需要过滤的程序协议，比如 POP3、ICQ、

FTPS、RDP 等。另外两张选项卡就不用看了不需要进行什么设置。

1． MAC 地址扫描

选择功能栏的嗅探器，然后选择下面的主机

扫描之前需要先激活嗅探器，点击上面的

 ，然后在下面空白处点右键选择扫描 MAC 地址，如图所示

1． 扫描整个子网

2． 规定扫描的范围

3． 扫描哪些网卡工作在混杂模式下(B31)

注：处于混杂模式下网卡接口能接受所有通过它的数据流，不管是什么格式，什么地址的。它会接收并响应 网络上任何的数据。一般网卡接口默认关闭混杂模式。扫描混杂模式的网卡主要是检测网络中的嗅探器。处于混杂模式的网卡在

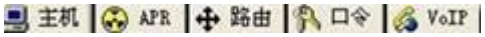
B31 那一栏就会有*号。

通过扫描我们将得到如下 MAC（注：本机是扫不到的）

从上图可以看到 192.168.2.1 是个 netgear 的网关地址。MAC 地址扫描是基于 ARP 请求包因此可快速定位 MAC 和 IP 的对应关系，OUI 指纹中包含了各大 MAC 厂商的信息，因此你可看到 Netgear 的路由器和 Cisco-Linksys 的网卡。扫描到 MAC 以后可以点右键来解析主机名。

2． ARP 欺骗

点击下面的 APR



出现下图所示

点击左侧栏最上面的 APR 后就出现下图所示，这时在右边空白处点一下鼠标，

上面的  就从灰色变成了深蓝色。点一下这个加号，出现下图所示

在这个左侧选择被欺骗的主机，在右侧选择一台或多台 PC，这时候将捕获所有被欺骗主机和其他多台主机之间的通信数据。也可以在右侧选择网关地址，则左侧被欺骗主机与广域网的通信将被捕获。例中左侧选择被欺骗主机 192.168.2.2 右侧选择网关地址 192.168.2.1 点确定。这时将出现下图所示

配置好 APR 欺骗的主机后我们可以进行 ARP 欺骗了，看左侧栏我们可以进

行各种 ARP 欺骗。a． APR-Cert 这个是数字证书收集器，配合 APR-HTTPS 使用。

由 HTTPS 嗅探过滤自动使用，也可手动创建一个伪造的证书。伪造的证书保存在 Certs 下。当前 APR-HTTPS 获得证书列表在 Cert.lst 文件中。也可 手动修改，定义 APR-HTTPS 使用指定的伪证书注入到“被 ARP 欺骗主机”和指定的 HTTPS 服务器的连接中。b． APR-DNS 这是 DNS 欺骗，点击 APR-DNS 欺骗，再点击上面的 

出现如下图所示的对话框在 DNS 名称请求中输入被欺骗主机要访问的网址。在回应包中输入用于欺骗的网址。图中输入百度的网址，下面输入华东理工大学的网址（网址为举例说明，并无任何目的）。这时被欺骗的主机如果访问百度网站的话会出来华东理工的主页。一些盗取银行账号的垃圾就是自己做一个和银行主页一样的钓鱼网站，然后在下面的回应包中输入钓鱼网站的网址。当对方访问银行主页时将会自动转到你的钓鱼网站上。（银行钓鱼网站，WEB 认证页面钓鱼）等等。

c． APR-SSH-1 欺骗

SSH 是远程登陆协议，ARP 可以利用 MITM 中间人攻击捕获并解密 SSH 会

话。

d． APR-HTTPS-1 欺骗

APR-HTTPS 可以捕获和解密主机和服务器间的 HTTPS 通信，与 APR-Cret 证书收集器配合使用，注入伪造的数字证书到 SSL 会话中，在被欺骗主机到达真正的服务器之前解密和加密数据。这种 HTTPS 欺骗会利用伪造的数字证书，因此对方会看到这个弹出的未经认证的数字证书请求认证。一般人不会看这个数字认证的（各位朋友你们仔细看过几次这种数字认证证书？）。

主要过程：

1) 开启 HTTPS 过滤，

2) 激活 APR 欺骗，

3) “被欺骗主机”开启一个 HTTPS 会话，

4) 来自“被欺骗主机”的数据包被 APR 注入，并被 CAIN 捕获，

5) APR-HTTPS 从 APR-Cret 证书收集器中搜索一个相近的伪证书，并是使用这个伪证书。

6) 捕获的数据包修改了 MAC、IP、TCP 源端口，然后使用 Winpcap 重新发送到局域网，与客户端建立连接

7) 创建 HTTPS 服务器连接，（“被欺骗主机”要连接的真实的服务器）

8) 使用伪证书与真实服务器连接，并使用 OpenSSL 库管理加密的通信。

9) 包由客户端发送出去，被修改后再回到“被欺骗主机”

10) 来自 HTTPS 服务器的数据被加密保存到会话文件中，重新加密并经客户端连接发送到“被欺骗主机”。