Cain 使用手册

译：淄博网警 SeeYou
2007 年 2 月 14 日

Cain 是著名的 Windows 平台口令恢复工具。它能通过网络嗅探很容易的恢复多种口令，能使用字典破解加密的口令，暴力口令破解，录音VoIP（IP 电话）谈话内容，解码编码化的口令，获取无线网络密钥，恢复缓存的口令，分析路由协议等。

下载：http://www.oxid.it/cain.html

http://www.oxid.it/downloads/ca_setup.exe

系统组成

Cain & Abel 是两个程序。Cain 是图形界面主程序；Abel 是后台服务程序，由两个文件组成：Abel.exe 和 Abel.dll 。

- 10MB 硬盘空间
- Microsoft Windows 2000/XP/2003
- Winpcap 包驱动 （V2.3 或以上；4.0 版本支持 AirPcap 网卡）

- 程序由以下文件组成：

cain.exe	主程序
CA_UserManual.chm	用户手册
Abel.exe	名为 Abel 的可的 Windows 服务
Abell.dll	程序支持文件
Wordlist.txt	小型口令文件
Instal.log	程序安装日志
oui.txt MAC	地址厂商文件
<安装目录>\winrtgen\winrtgen.exe	字典生成器
<安装目录>\winrtgen\charset.txt	字符集文件
<安装目录>\Driver\WinPcap_4_0_beta2.exe	原始 Winpcap 驱动程序

Abel 是一个服务程序，由两个文件组成："Abel.exe" 和 "Abel.dll"，服务并不能自动安装到系统中。可用 Cain 将 Abel 安装到本地或远程，但需要管理员权限。

- 本地安装：

1、 复制"Abel.exe"和"Abel.dll"到系统安装目录%WINNT%(如 C:\Windows)

2、 运行 Abel.exe 安装服务

3、 使用 Windows 服务管理器开始 Abel 服务

- 远程安装：

1、 使用 Cain 的网络表（Network TAB），选择远程主机

2、 右击计算机图标，选择连接

3、 提供远程主机的管理权认证

4、 连接成功后，右击其“服务”图标，选择菜单“安装 Abel（Install Abel）”

5、 完成。此时服务文件自动传送到远程并自动开始服务

- 注册表修改：

  Cain 的注册表项是：HKEY_CURRENT_USER\Software\Cain

- Cain.exe 依赖如下库：

  Abel.dll、Crypt32.dll、Pstorec.dll、Kernel32.dll、Advapi32.dll、Comctl32.dll、Comdlg32.dll、Gdi32.dll、Iphlpapi.dll、Mpr.dll、NetApi32.dll、Odbc32.dll、Ole32.dll、Oleaut32.dll、Packet.dll (Winpcap)、Rasapi32.dll、Rpcrt4.dll、Shell32.dll、User32.dll、Wpcap.dll (Winpcap)、Airpcap.dll (AirPcap)、Ws2_32.dll、Wsnmp32.dll.

- Abel.exe 依赖如下库：

  Abel.dll、Kernel32.dll、Advapi32.dll、Iphlpapi.dll、User32.dll、Ws2_32.dll

- Abel.dll 依赖如下库：

  Lsasrv.dll、Kernel32.dll、Advapi32.dll、User32.dll、samsrv.dll

- Cain 将生成以下文件（逗号分隔的列表文件）

解密文件（Cracker）：

APOP-MD5.LST APOP-MD5 的凭证列表
CRAM-MD5.LST CRAM-MD5 的凭证列表
PIX-MD5.LST Cisco PIX 的凭证列表
IOS-MD5.LST Cisco IOS 的凭证列表
PWLS.LST PWL 文件列表和相关凭证列表
NTLMv2.LST NTLMv2 的凭证列表]
LMNT.LST LM & NTLMv1 的凭证列表
CACHE.LST MS-CACHE 的凭证列表
OSPF-MD5.LST OSPF-MD5 的凭证列表
RIP-MD5.LST RIPv2-MD5 的凭证列表
VRRP-HMAC.LST VRRP-HMAC 的凭证列表
VNC-3DES.LST VNC Triple DES 的凭证列表
MD2.LST MD2 的哈希值列表
MD4.LST MD4 的哈希值列表
MD5.LST MD5 的哈希值列表
SHA-1.LST SHA-1 的哈希值列表
RIPEMD-160.LST RIPEMD-160 的哈希值列表
K5.LST Ms-Kerberos PreAuth 的凭证列表
RADIUS_SHARED_HASHES.LST RADIUS PreShared Key 的凭证列表
IKEPSKHashes.LST IKE-PSK 的凭证列表
MSSQLHashes.LST Microsoft SQL 的凭证列表
MySQL.LST MySQL 的凭证列表
80211.LST 802.11 捕获文件列表

嗅探（Sniffer）：

HOSTS.LST 主机信息列表，包含 MAC、IP、主机名
APR.LST 用于 ARP 欺骗的主机列表
DRR.LST APR-DNS 使用的主机名和 IP 列表

SSH-1.LST SSH －1 嗅探过滤器生成的信息
CERT.LST APR-HTTPS 使用的信息
HTTPS.LST HTTPS 嗅探过滤器生成的信息
FTP.LST FTP 嗅探过滤器捕获的信息
HTTP.LST HTTP 嗅探过滤器捕获的信息
IMAP.LST IMAP 嗅探过滤器捕获的信息
POP3.LST POP3 嗅探过滤器捕获的信息
SMB.LST SMB 嗅探过滤器捕获的信息
TELNET.LST Telnet 嗅探过滤器捕获的信息
VNC.LST VNC 嗅探过滤器捕获的信息
TDS.LST TDS (Tabular Data Stream) 嗅探过滤器捕获的信息
SMTP.LST SMTP 嗅探过滤器捕获的信息
NNTP.LST NNTP 嗅探过滤器捕获的信息
KRB5.LST MS-Kerberos5 嗅探过滤器捕获的信息
RADIUS.LST RADIUS 嗅探过滤器捕获的预共享密钥列表
RADIUS_USERS.LST 嗅探过滤器捕获的用户信息
ICQ.LST ICQ 嗅探过滤器捕获的信息
IKE-PSK.LST IKE 嗅探过滤器捕获的预共享密钥列表
MySQL.LST MySQL 嗅探过滤器捕获的信息
SNMP.LST SNMP 嗅探过滤器捕获的通信串列表
VoIP.LST SIP/RTP 嗅探过滤器捕获的 VoIP交谈录音列表

其他文件：

RT.LST 加密破解时用的 Rainbow 表
QLIST.LST 网络（Network Tab）中主机的快速列表
CCDU.LST Cisco 配置 Downloader/Uploader View 信息
HTTP_USER_FIELDS.LST HTTP-FORM 和 HTTP-COOKIE 嗅探过滤器使用的用户名字段列表
HTTP_PASS_FIELDS.LST HTTP-FORM and HTTP-COOKIE 嗅探过滤器使用的口令字段列表
DUMP.IVS aircrack 兼容格式的 WEP Ivs 列表

子目录：

- <安装目录>\Certs\ APR-HTTPS 使用的伪造的电子证书文件(*.crt)
- <安装目录>\HTTPS\ APR-HTTPS 捕获的会话文件
- <安装目录>\SSH-1\ APR-SSH-1 捕获的会话文件
- <安装目录>\Telnet\ Telnet 嗅探过滤器捕获的会话文件
- <安装目录>\VoIP\ 嗅探器捕获的 VoIP 交谈文件，保存为 WAV文件
- <安装目录>\CCDU\ 来自 Cisco 设备的配置文件

程序配置

Cain & Abel 需要配置一些参数，可从主界面中的配置对话框中完成。

Sniffer 嗅探表

配置 Cain 或 APR（ARP 毒害路由）选择网卡，及启动参数等

APR（Arp Poison Routing）欺骗表

Cain 使用多线程每 30 秒向受骗主机发送 ARP 欺骗包，这是必须的，因为远程主机会定期整理 ARP 缓存。当间隔设置太短时会产生大量的 ARP 网络流量，而设置太长时此起不到欺骗劫持的效果。

注：以下也称 APR 为 ARP 欺骗。

欺骗选项（spoofing options ）定义 CAIN 向以太网写入数据时的地址、ARP 头、ARP 欺骗包、重路由包等。若不使用真实的地址攻击将是完全匿名的，因为攻击者真实的 MAC 地址和 IP 地址是隐藏的，不会发送到网络上去。

如果你想启用此选项，必须注意以下问题：

- 以太网地址欺骗只能用于攻击者的计算机接到 HUB 上，对于交换机则不能使用“端口安全”（Port Security）项，如果使用“端口安全”，以太网帧中的源 MAC 地址将与交换机中允许的 MAC 地址列表进行核对，如果不符，交换机将屏蔽此端口，你也将会失去连接。
- 欺骗者的 IP 地址必须是子网中的一个合法地址。所以如果设置的 IP 不在子网内，将会出现“IP 地址冲突”（IP address conflict），这很容易就注意到。以下是一些有效的欺骗地址例子：

真实 IP 地址	子网掩码	可欺骗的 IP 地址范围
192.168.0.1	255.255.255.0	192.168.0.2 - 192.168.0.254
10.0.0.0.1	255.255.0.0	10.0.0.2 - 10.0.255.254
172.16.0.1	255.255.255.240	172.16.0.2 - 172.16.0.14
200.200.200.1	255.255.255.252	200.200.200.2 - 200.200.200.3

以上真实 IP 必须保证在所处子网中未用。

- 欺骗者的 MAC 地址必须在子网中未使用。在同一个二层局域网中两个相同的 MAC 地址将导致交换机汇聚问题；为解决此问题特在配置中不允许轻易设置 MAC，默认是 001122334455，这是个无效地址，一般不会与实际情况冲突，但是在同一个二层网络不能有两个同时使用 APR 的 CAIN 主机。要改变此默认 MAC，可从注册表 HKEY_CURRENT_USER\Software\Cain\Settings 中的 SpoofMAC 键修改。

过滤器与端口表（Filters and Ports）

在这里可以开关 CAIN 的嗅探过滤器和程序协议 TCP / UDP 端口。Cain 只捕获认证信息，而不是每个包的全部内容，但可修改相关过滤端口。

HTTP 字段表（HTTP Fields）

此表中包含了 HTTP 嗅探过滤器使用的用户名和口令字段列表，用来检查 HTTP 包中携带的 Cookies 和 HTML 的表单元素，对于每个用户名字段，所有的口令字段均被检查，如果这两个字段都被捕获，结果就会在屏幕上显示。可以自己添加适合的相关字段。

下列 cookie 使用字段“logonusername=”和“userpassword=”实现认证，若未在上表中指定此两个字段，嗅探器将不会提取相关认证信息：

GET /mail/Login?domain=xxxxxx.xx&style=default&plain=0 HTTP/1.1

*Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */**

Referer: http://xxx.xxxxxxx.xx/xxxxx/xxxx

Accept-Language: it

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; (R1 1.3); .NET CLR 1.1.4322)

Host: xxx.xxxxxx.xx

Connection: Keep-Alive

Cookie: ss=1; **logonusername=user@xxxxxx.xx** *; ss=1; srclng=it; srcdmn=it; srctrg=_blank; srcbld=y; srcauto=on; srcclp=on; srcsct=web;* **userpassword=password;** *video=c1; TEMPLATE=default;*

Cain 的快捷键：

Alt+Del -> 隐藏主窗口

Alt+PgDwn -> 主窗口到系统栏

Alt+PgUp -> 恢复主窗口

Cisco 配置上传下载（Config Downloader/Uploader）

通过 SNMP/TFTP 上传、下载 Cisco 设备的配置文件。支持使用了 OLD-CISCO-SYSTEM-MIB 或新的 CISCO-CONFIG-COPY-MIB 的 Cisco 交换机和路由器。

l 工作原理：

1、Cain 使用 SNMP 协议向 Cisco 设备请求传输配置文件，请求包由一些厂商提供的 Cisco OID 属性构建，同样也包含其他参数，如协议类型、服务器 IP 地址、配置文件文件名等。

2、设备使用由请求包指定的协议传输文件（一般是 TFTP）。

3、Cain 打开 TFTP 接口监听模式，并操纵文件的传输。

l 用法：

下载配置文件用“Ins”插入键或点击工具栏上的“＋”按钮；上传则从弹出菜单中的相关功能中选择。

- **局限**

当有 ACL 访问控制列表、防火墙规则等限制时无效。

MAC 地址扫描

MAC 地址扫描是基于 ARP 请求**应答包**的，可实现快速 MAC 与 IP 对应。扫描器包括 OUI 数据库，它提供了 MAC 厂商信息，此功能可快速鉴别出局域网中的交换机、路由器、负载平衡设备和防火墙。因为 ARP 包不能穿越路由器或 VLAN，此功能只能解析本地广播域，OUI 数据库是一个格式化的 IEEE OUI 列表，可从：http://standards.ieee.org/regauth/oui/index.shtml 下载。一旦找到活动主机，就可使用弹出菜单中的“Resolve Host Name”功能解析其主机名。

- **要求：**嗅探（sniffer）必须启动
- **用法：**“INS”插入键或工具栏“＋”

网络调查员（Network）

用来鉴别域控制器（Domain Controllers）、SQL Server、打印服务（Printer Servers）、远程访问拨入服务（Remote Access Dial-In Servers）、Novell Servers、Apple 文件服务（Apple File Servers）、终端服务器（Terminal Servers）等，甚至能鉴别其操作系统版本。

左侧树用来浏览网络和连接到远程主机，一旦连接到服务器就可列出其用户的用户名、工作组、服务和共享资源。默认情况下 Cain 使用本地登录的用户名连接到远程主机的“IPC$”共享，若不能则使用空连接（匿名连接）。当列举用户名时，CAIN 也可提取它们的 SID（安全标识），并能鉴别出管理员（即使是改名了），这是通过查看帐号的 RID（SID 的最后部分）完成的，管理员的 RID 总是 500。

Windows NT 及以后版本有一个安全特性，就是限制匿名连接（空连接），这是通过将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 下的 键 RestrictAnonymous 设置为 1 完成的。如果程序不能列举用户，是因为这个限制，这时 CAIN 就自动启动 SID 扫描器（SID Scanner），使用工具sid2user 来提取。

口令破解（Cracker）

Cain 支持多数通用的哈希算法以及基于它们的加密方法。

- 哈希类型：

MD2、MD4、MD5、SHA1、SHA2(256bit)、SHA2(384bit)、SHA2(512bit)、RIPEMD160

- 加密算法：

PWL files、Cisco-IOS Type-5 enable passwords、Cisco PIX enable passwords、APOP-MD5、CRAM-MD5、LM、LM + Challenge、NTLM、NTLM + Challenge、NTLM Session Security、NTLMv2、RIPv2-MD5、OSPF-MD5、VRRP-HMAC-96、VNC-3DES、MS-Kerberos5 Pre-Auth、RADIUS Shared Secrets 、IKE Pre-Shared Keys 、Microsoft SQL Server 2000 、Oracle、MySQL323、MySQLSHA1.

暴力口令破解

暴力破解就是尝试所有可能的键组合来解密，是否可行一般与口令长度以及计算机的性能有关。Cain 的暴力破解器使用预定义或自定义字符集的所有可能组合来测试加密的口令。所有可能的组合空间可用以下公式来计算：

KS = L^(m) + L^(m+1) + L^(m+2) + ... + L^(M)

其中：L＝字符集字符个数；m＝最小口令长度；M＝最大口令长度。

例如，当破解 LM（LanManager）口令的一半时，使用“ABCDEFGHIJKLMNOPQRSTUVWXYZ”这 26 个大写字母，暴力破解将试验有 KS = 26^1 + 26^2 + 26^3 + ... + 26^7 = 8353082582 种不同的口令，而当同样的口令，使用下列字符集时：

“ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/”

所有可能性将是 6823331935124 个。

理论上暴力破解是可以破解出原文的，只是时间问题。

字典口令破解

字典破解是以字典中的每一个可能的词作为可能的口令尝试，这种方法可能比暴力破解更有效，因为用户一般选择的口令范围很小。有两个方法来改善字典破解，一个方法是使用更大的字典，或更多的字典（专业词典或外国词典能增加全面的破解）；另一个方法是字典中的字符串操纵。如：字典中可能有单词“password”，一般串操纵技术将尝试单词的反写“drowssap”，或添加数字到串尾（password00 - password99）或不同的大小写组合（Password, pAssword, ... passworD）。

Cain 的字典破解可配置成使用字典组列表文件，还提供一些变化：

- As Is: ->原样，与字典文件中的相同
- Reverse -> 反写 (password->drowssap).
- Lowercase -> 小写化 (Password -> password).
- Uppercase -> 大写化 (Password -> PASSWORD).
- Case Perms -> 不同位置大小写 (password, Password, pAssword, PAssword, ... PASSWORD).
- Two numbers Hybrid-Brute: 添加词尾一最大数字 (Password0, Password1,...Password9, Password00, Password01, ... Password99).

程序能记住上次中断的字典位置，Reset 按钮重置位置。

密码分析

使用“Faster Cryptanalytic time – memory trade off”（时空交换快速密码分析）方法，此破解技术使用名为缤纷表（Rainbow Tables），此表由一组大型的预计算好的加密口令表，并支持以下哈希／加密算法：LM, FastLM, NTLM, CiscoPIX, MD2, MD4, MD5, SHA-1, SHA-2 (256), SHA-2 (384), SHA-2 (512), MySQL (323), MySQL (SHA1) and RIPEMD160.

缤纷表可由程序“rtgen.exe”或“winrtgen.exe”产生。

此破解技术还算快速，然而只在破解一些加密口令时才有用，当双向认证时无效，这时

破解将是十分复杂的。

WEP 破解

WEP 破解依赖于某些 RC4 算法的缺陷，通过捕获足够数量的 WEP 包，能快速破解 64 位、128 位密钥，按照 Aircrack 的文档说，需要的最少唯一 WEP 包数量是：对 64 位 WEP 为 250000，对于 128 位是 1000000 或更多。但网络使用动态 WEP 密钥时无法破解。

口令解码

点击工具栏上的口令解码按钮可对常见的口令编码进行解码。

- Access 数据库口令解码（Access Database Passwords Decoder）

Access 主数据库的口令存储在文件中并只进行了简单的异或（XOR）编码，可立即得到解码，但对用户级口令无效。

- Base64 口令解码（Base64 Password Decoder）

解密 Base64 编码的口令，Base64 编码用于少数互联网协议，如 HTTP、MIME、IMAP 等，任何数据都能被编码为纯文本的 ASCII 文本。

- 星号查看（Box Revealer）

查看标准口令框中隐藏在星号后面的内容。要求帐号具备系统特权，通常是管理员。

- Cisco Type-7 Password Decoder

Cisco 设置使用自制的加密算法，此处解码配置文件中的 Type-7 口令，而 Type-5 不能解码，可用 IOS-MD5 破解。

- Cisco VPN Client Password Decoder

破解 Cisco VPN 客户端软件的配置文件（*.pcf）中存储的口令，口令是SHA1 和 3DES-EDE 编码的。

- 认证管理器口令解码（Credential Manager Password Decoder）

认证管理器在 Windows 2003 和 XP 中提供认证信息的安全存储，如当使用命令：

net use * \\computer_name\share_name /user:user_name password /savecred

认证管理器将存储提供的口令到本地名为“Enterprise Credential Set”（企业认证集）的集合中。此认证集合存储在文件“\Documents and Settings\%Username%\Application Data\Microsoft\Credentials\%UserSID%\Credentials”中，并使用 DPAPI 子系统加密。

还有另一个集合“Local Credential Set ”（本地认证集 ），它指向“\Documents and Settings\%Username%\Local Settings\Application Data\Microsoft\Credentials\%UserSID%\Credentials”。

- 拨号口令解码（Dial-Up Password Decoder）

解码存储在“拨号网络”组件中的口令，RSA 认证通常保存在 LSA 秘密（LSA Secrets）"L$_RasDefaultCredentials" 和 "RasDialParams!<UserSID>" 中，其他连接参数在电话本文件（*.pbk）中。

- 企业管理器口令解码（Enterprise Manager Password Decoder）

企业管理器是 Windows 用来管理 MS SQL Server 7.0 和 2000 的应用程序，当配置 SQL Server 认证时，企业管理器在注册表中存储连接认证信息，涉及以下键：

SQL2000:

HKEY_CURRENT_USER\\Software\\Microsoft\\Microsoft SQL Server\\80\\Tools\\SQLEW\\Registered Servers X\\

SQL 7.0:

HKEY_CURRENT_USER\\Software\\Microsoft\\MSSQLServer\\SQLEW\\Registered Servers X\\

SQL 使用简单的异或（XOR）算法加密、解密，算法如下：

```
void xor_cred (char *credential, int len)
{
    BYTE
    XorTable[]={0x67,0x66,0x3b,0x64,0x6b,0x6c,0x67,0x5e,0x25,0x24,0x5e,0x6c,0x3b,0x64,0x7
    3,0x27,0x63,0x00};
    int xorlen = strlen ((char*) XorTable);
    for (int j=0,i=0; i<len; i++,j++)
    {
        if (j==xorlen) j=0;
        credential[i] ^= XorTable[j];
    }
}
```

- 保护存储口令管理器（Protected Storage Password Manager）

保护存储用来保存发行给用户的私有键，所有保护存储信息都是加密的，加密与用户的登录口令有关，所以只有拥有它的用户才可访问。

认证保存在注册表中：

HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider\

此功能能对以下类型解码：

- MS Outlook 2002 (POP3, SMTP, IMAP, HTTP)
- Outlook Express (POP3, NNTP, SMTP, IMAP, HTTP, LDAP, HTTP-Mail)
- Outlook Express Identities
- MS Outlook (POP3, NNTP, SMTP, IMAP, LDAP, HTTP-Mail)
- MSN Explorer 登录口令
- MSN Explorer's 自动完成口令
- Internet Explorer 保护的网站口令
- Internet Explorer 自动完成口令

- PWL 缓存口令解码（PWL Cached Password Decoder）

解码 Windows 95/98 的 PWL 文件（口令列表文件）。

- 远程桌面口令解码（Remote Desktop Password Decoder）

远程桌面允许保存连接参数到扩展名为“.RDP”的文件中，当选择“保存密码”时，认证信息用 CryptProtectData API 加密并保存。例如有以下加密的口令：

password 51:b:01000000D08C9DDF0115D1118C7A00C04FC297EB01000000F471161752360D4496EDA14F658FDF8E000000
0008000000700073007700000003660000A8000000100000000188EFBFDCB0C5EC2CE831603376EAC390000000004800000A
0000000100000000C568F97E208D0F4431972967599F8CB08020000EA394AFF35DB15237E0565D4D152553FB1B56B166C4F
D4D4139D41E06864924F8CF6D62A8D5A022BD57FA6CC9FE596D7FF44C182A7BE289FA8F7104F974919F4AD821C717571A6
AC962B020460A02BE6B18912B24FC356C0B3E7B966D50DE6D80D28C80B1E7EE449758D592C9B90D1A9E4389625F6D0BD0
C77CF0E78BF25C6B9B8664C2CF71BFF597A5CC4F695FD2D969C241E18976F3BC0857728A9CAEAE5DD0D5046F7173274E0
CD071945A0428BA5EA36908B0928EED7B496DD6517A70531C1638A376C36E31DF682601BC4601E4D823F6E544933E3AD4B

7663CBC81443C214A16330FEE87BAB49902776AC2A2D9B7C222EE614C7D147AC8932EDABEB85341EFCE4579AE3D077F84

17E265C4CB3B26928ED6583EC76E456CDB16D768A22629DA4147769658698285C251F222F2AB180C376B2837CA83FBC825

6B5DB03A41CBC2599C0769578F9C02550743E9F3962E696FFBFD9BB22EDAFA4CAB3D072955EEB5589C2AA992D8C8FCFB2

C3665A8B30CF9CD0109FF232882B9493054565C4E26EB4566EAA7183E4CBBAB7C2A30575C3CC84946B121F0D044F6CAD20

DDFBF6647135D08CAA2D0A25281E16EE3BE19A017BEB64A6F79296CF7CEFB140C6E4BE71E66691FECBD9CBCD83EC3A748

791DE3D3E4433034F8968C71A793670E8F4CB0AC479AB5F045F514BB109ED5FCB2B1CFA8BCEB05D7E0186CD871DDB2C13

41E3E9688358D2932835B514000000E16BE7FD121813D382B2A02360FF427D0F8B23D20

以上加密口令只有创建“.RDP”的用户和相同的机器上才可解码。但 Cain 可以解码。

解密原理：使用"CryptUnprotectData" API 中的 CRYPT32.DLL。

- Syskey Decoder

从本地注册表或“离线”系统文件中提取系统工具 SYSKEY 产生的启动键。启动键中的信息用于在口令哈希存入 SAM 数据库文件之前进行加密。启动键如果存在本地，其信息分散在以下注册表子键中：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

Syskey 解码器能将以上信息收集解码出来。

- VNC 解码（VNC Password Decoder）

Virtual Network Computing（VNC）是远程桌面控制软件，可实现跨平台操作。服务器组件存储加密的登录口令在注册表中：

\\HKEY_CURRENT_USER\\Software\\ORL\\WinVNC3\\Password

或

\\HKEY_USERS\\.DEFAULT\\Software\\ORL\\WinVNC3\\Password

- 无线以太网配置口令转储（Wireless Zero Configuration Password Dumper）

解码保存在 Windows 的“Wireless Zero Configuration Service”中的无线密钥。其中 WEP 自动解码，WPA-PSK 键以十六进制格式显示（因为使用了 SHA1 单向哈希）。

- 802.11 捕获文件解码（802.11 Capture Files Decoder）

解码无线 WEP 或 WPA-PSK 包。

口令转储

- LSA Secrets Dumper

LSA 秘密常用来存储用来启动服务程序的帐户信息（如口令），PWDUMP2 也能实现此功能。

- MSCACHE Hashes Dumper

与 CacheDump 类似，转储缓存的口令哈希到注册表，Cain 的 MSCACHE Hashes Dumper 确实可直接导入哈希到相关的 MSCACHE Hashes 口令破解表，默认的，Windows 保存域登录口令的副本到本地注册表，这使得用户可登录本地，即使域控制器离线失效，缓存的口令哈希用“NL$KM LSA 秘密”加密。此处解密缓存的哈希并准备用字典或暴力破解之。

- MySQL Passwords Extractor（MySQL 口令提取）

MySQL 存储帐号的认证信息到用户表（USER）中，口令被加密并保存在哈希表下，此处通过 ODBC 连接到 MySQL，并转储所有帐号的哈希到 MySQL 哈希破解列表中去（命令是：select user, password from user）。

- NT Hashes Dumper

转储 SAM (Security Account Manager) 数据库中口令哈希，而不管是否 SYSKEY 加密。

- Oracle Passwords Extractor

Oracle 存储帐号认证信息到 DBA_USERS / SYS.USER$ 表中，口令由DES－CBC 算法加密并保存为哈希。此处用 ODBC 连接到 Oracle 服务器并转储帐号的哈希到 Oracle Hashes Cracker 列表中去。数据库连接后的处理命令是：

select username, password from DBA_USERS

select name,password from SYS.USER$

- SQL Server 2000 Password Extractor

Microsoft SQL Server 2000存储帐号的认证信息到 "master"数据库中，用户口令用 SHA-1 加密并存到“sysxlogins”表。SQL 命令是：

select name, password from master..sysxlogins

口令／哈希计算

- 哈希计算：

可计算输入文本的 MD2, MD4, MD5, SHA-1 ... 等各种哈希值，以及其他 LM, NTLM, MySQL323 和 Cisco PIX 。

- RSA SecurID Token Calculator（RSA 安全钥匙计算）

混杂模式扫描（Promiscuous-mode Scanner）

用于鉴别出网络中的嗅探器和入侵检测系统，此功能包含在 MAC 地址扫描中，是根据不同的 ARP 包应答判断的。测试结果在主机列表中相应列中显示“*”表示有某种模式。如以下某台 Windows 机器的结果：

表示网卡不是混杂模式（未嗅探）：

Host name	B31	B16	B8	Gr	M0	M1	M3
		*				*	

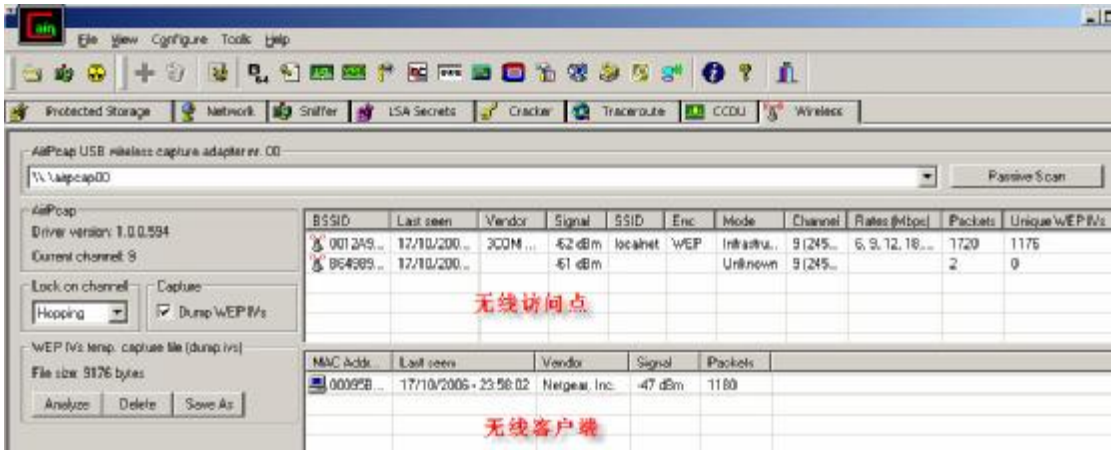
表示网卡是混杂模式（嗅探）：

Host name	B31	B16	B8	Gr	M0	M1	M3
	*	*				*	

正如你看到的 Windows 机器，那些没有处于嗅探状态的通常回答 16 位的 ARP 广播测试（B16）且仅组播 1 的 ARP 测试（M1）;相反，当处于嗅探时，网卡处于混杂模式，它们能回答 32 位 ARP 测试（B31）。

- 无线扫描（Wireless Scanner）

检测使用 802.11x 协议的无线局域网。



主动扫描：

不象其他程序，它不使用 Windows NDIS 用户模式 I/O 协议(NDISUIO) 而是 Winpcap 包驱动来控制无线网卡，每隔 5 秒钟，访问点和 ah-hoc 网络就被使用列举一次，并且无线网络参数（MAC 地址、厂商、WEP 密钥、频道等）显示在扫描列表中。

被动扫描：

被动扫描要求 AirPcap 网卡并使用了 CACE 驱动技术，此技术能使用 AirPcap 驱动捕获 802.11 原始帧，扫描器能悄悄的通过解码空中传输的 802.11b/g 包识别出无线访问点(上面的列表) 和客户端(下面的列表)，“Channel Hopping”（跳频）功能每秒钟都在改变网卡的频率，以便发现不同频道上的网络。

嗅探器（Sniffer）

Cain 的嗅探器功能主要集中的密码和认证信息的嗅探上，它不应与一些专业的嗅探软件相比，如 Observer、SnifferPro、Ethereal、OmniPeek，**但它可工作在交换式网络中**，关键技术是使用了 APR （Arp Poison Routing－ARP 毒害路由）技术，又称“**ARP 欺骗**”。

- 协议过滤器：只处理 ARP 和 IP 协议，而不处理 NetBEUI 等其他协议。
- 口令过滤器：只嗅探有限的几种认证信息

协议	认证类型
FTP	纯文本
HTTP/Proxy	Basic, Form, Cookie, LM, NTLMv1, NTLMv2, NTLM会话安全, NTLMSSP
IMAP	纯文本, LOGIN, CRAM-MD5, LM, NTLMv1, NTLMv2, NTLM Session Security, NTLMSSP
POP3	纯文本, APOP-MD5, CRAM-MD5, LM, NTLMv1, NTLMv2, NTLM会话安全, NTLMSSP
SMTP	纯文本, LOGIN, CRAM-MD5, LM, NTLMv1, NTLMv2, NTLM会话安全, NTLMSSP
NNTP	纯文本, LM, NTLMv1, NTLMv2, NTLM 会话安全, NTLMSSP
ICQ	v.7
VNC	3DES

TDS (Sybase / MSSQL)	v4.x, v5.0, v7.0 XOR, v7.0 NTLMv1, NTLMv2, NTLM 会话安全,NTLMSSP
MySQL	v3.23, SHA-1
SMB	纯文本, LM, NTLMv1, NTLMv2, NTLM会话安全, NTLMSSP
MS Kerberos5	预认证加密时间戳
Radius	预共享键, 用户口令
IKE	积极模式预共享键(MD5 和 SHA-1)
SNMP	公共串
RIP	纯文本, hash, RIPv2-MD5
HSRP	纯文本
EIGRP	MD5
OSPF	简单, MD5
VRRP	简单, IP-AH, HMAC_MD5_96
SIP	认证和代理认证 (MD5)
Telnet	整个会话转储到文件
*HTTPS	整个会话转储到文件 ＋HTTP 相同类型
*SSH-1	整个会话转储到文件(全双功, 秘密, 支持 DES, 3DES, Blowfish 均衡加密算法)
SIP/RTP	捕获并解码 VoIP 交谈 （RTP 协议）并保存为 WAV 文件

(*) = 需要启用 APR (Arp Poison Routing) －ARP 欺骗。

Cain 的嗅探过滤器可以捕获传输的明文口令，但一些协议使用交换应答机制，这样 CAIN 需要一些“客户端->服务器”和“服务器->客户端”传输的参数，在交换式网络可从交换机的镜像口或 APR 达到全路由状态。

当 APR (Arp Poison Routing) －ARP 欺骗激活时，嗅探器将能处理平常看不到的包并重路由到正确的目的地，但在高速繁忙的网络上这将可能导致性能瓶颈，所以**要小心使用**。APR（ARP 欺骗）的主要功能是能在交换式网络上实现嗅探，并允分析加密协议，如 HTTPS 和 SSH-1 。

口令和哈希被存储在安装目录下的“.LST”列表文件中，格式是逗号分隔的文本。

对于 HTTPS、SSH-1 和 Telnet 协议，整个会话被解密并转存到相应命名的文本文件中：

<协议名>-<年><月><日><时><分><秒><毫秒>-<客户端口>.txt

如：Telnet-20041116135246796-1141.txt

- 离线捕获文件处理

嗅探器可以处理捕获的离线协议文件（来自 Ethereal, Tcpdump 和 Winpcap 等其他嗅探器）,这可以从“Open”打开文件，此时 APR 功能自动关闭。

- 路由协议分析（Routing Protocols Analysis）

路由协议有 VRRP, HSRP, RIP, OSPF, EIGRP 此功能能快速鉴别子网路由与边界。

对于 EIGRP 和 RIP 协议，“Routes Extractor ”（路由提取）将转储真实路由表在路由器间共享，此功能只有在不需要认证时才有效。

用法：先激活嗅探，参数在配置里设置。

APR（ARP Poison Routing－ARP 欺骗)

ARP 欺骗是 Cain 的最主要的特色，能实现交换式网络中的嗅探，并对主机间通信进行

注入。APR 实现 ARP 欺骗攻击并路由到正确的目的地。

- ARP 欺骗（ARP Poison Attack）：

这种攻击是基于主机 ARP 缓存操作的。在以太或 IP 网络中，当两台主机互相通信时，它们必须知道对方的 MAC 地址（物理地址），源主机查看它的 ARP 缓存表中是否有与 IP 地址相应的 MAC 地址，如果没有，就广播一个 ARP 请求包到整个网络（子网），来询问目标主机的 MAC，因为这个询问包以广播形式发送给**子网内**所有主机，正常情况只有真正具备此 MAC 的 IP 地址才给予应答。但是，当目标主机的 ARP－IP 入口预先侵入到源主机的 ARP 缓存表中，源主机就不会再发出 ARP 询问包，从而实现了 ARP 的欺骗。

问：如果其 ARP 缓存表中有目标主机错误的 MAC，源主机会不会发生问题？
答：很简单，它将与有“错误”MAC 地址的目标主机通信，而不会与真正的目标主机通信。
问：怎样才能改变主机 ARP 缓存表中的 MAC－IP 地址对应？
*答：ARP（Address Resolution Protocol －地址解析协议）是无状态协议，不需认证，只要简单的发给它一个“**ARP 应答**”包，就能强制更新其 ARP 缓存表。*
问：这种欺骗攻击能用于互联网（广域网）吗？
答：不能。ARP 协议不能穿越路由器或 VLAN，所以 APR 很少在 2 层广播域之外使用。

通过操纵两台主机的 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，这样就强制两台主机经你代理来通信，这就是所谓的“**中间人攻击**”（Man-in-the-Middle），简称 MITM。

- 重路由包（Re-Routing Packets）

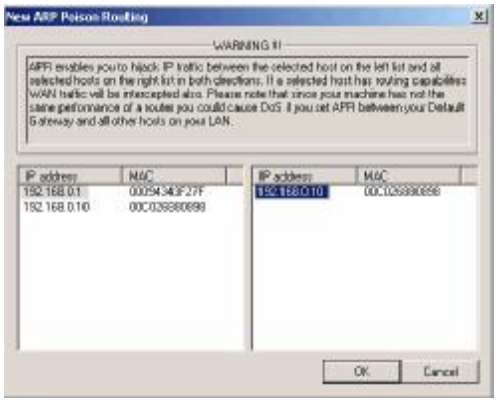
假如你成功的设置了 ARP 欺骗来截获两主机间的通信，这样你已经在 ARP 欺骗包中注入了嗅探器的 MAC 地址，并正强迫两主机通过你来代理通信。嗅探器收到发向其 MAC 的而不是其 IP 的包，协议栈将丢弃这些包，这样就引发了两主机间的 DOS（Denial of Service －拒绝服务）攻击，为避免这类问题，嗅探器必须能重路由受骗包到正确的目标主机（若主机不能正常通信了，也将不可能捕获任何实质内容，如口令）。

要求：为了重路由受骗包到正确的目的地，Cain 必须知道每一个受骗主机的 IP－MAC 对应，这是为什么首先要求用户扫描 MAC 地址的原因。

- 配置（Configuration）

要配置选项中可以指定伪造的 MAC 和 IP 地址来进行 ARP 欺骗攻击，这将很难被追查到攻击的源头，因为攻击者的真实地址并不发送到网络中。在交换式网络中，攻击也是隐蔽的，因为 Cain 在 ARP 欺骗包中使用的是单播以太网地址，这些包由交换机依照其 CAM 表来路由，从不以广播形式发送。

受骗主机可从 APR 表中使用工具栏中的“＋”来选择。



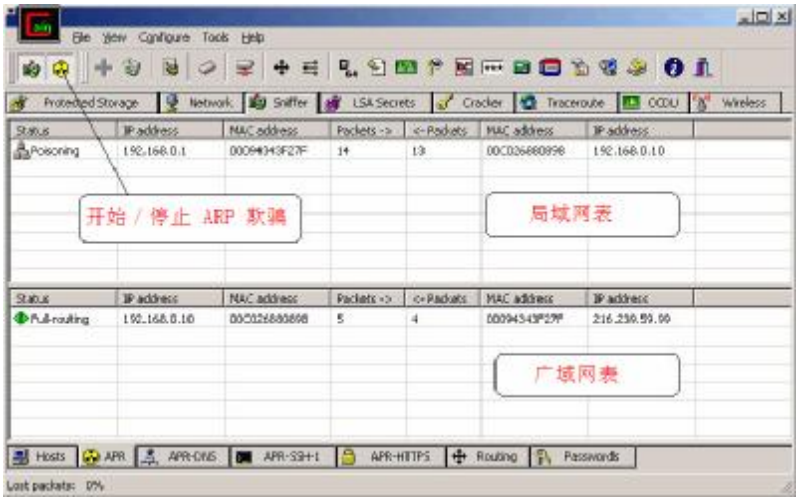
警告！！！

***APR** 允许你在左边列表中选择的主机与右边列表中所有选择的主机间通信执行双向注入，若某选择的主机具有路由功能，则与广域网的通信将被捕获，请注意，如果你在默认网关与所有其他局域网中的主机间设置 **APR**，而你机器的性能不及路由器，将会导致 **DoS** 拒绝服务。*

此例中的选择意思是：我想注入所有流经主机“192.168.0.1”和“192.168.0.10”的双向IP 通信，所以我的工作站将处于中间人地位。

- ARP 欺骗视图（APR Views）

你可以从下面 APR 子表中监视活动的通信，上半部的表（局域网表）显示在受骗主机间重路由包的数量及路由方向，有时因为某些原因（如静态路由表）只能攻击一个主机，这时你将看到一个方向上的重路由包数量上升，这仅意味着嗅探器正处理一半的预期通信。



下半部的表显示内网与外网的通信情况，若两者之一是路由器，则 Cain 的 APR 欺骗也可以处理广域网通信。

- 欺骗路由器时的注意事项

1、如果设置 APR 为内部主机与网关间的注入欺骗，则捕获此主机与的默认网关外主机的通信。

2、当有多个网关时 APR 怎样重路由？新版本的 Cain 做了一些工作：选择使用本地操作系统的路由表中的最佳路由。如果你的局域网使用的是不均匀路由，可以用路由管理器（Route Table Manager）或命令行 route.exe 来修改本地路由表。

3、欺骗网关与所有内部主机的通信，易引起通信瓶颈，因为 APR 不可能有同高速路由相同的性能。

4、默认网关地址通常是由 HSRP 或 VRRP 路由协议产生的虚拟地址，若你要欺骗一般主机与默认网关虚拟地址的通信，必须也欺骗 HSRP/ VRRP 成员的真实地址。

- APR WAN Status（APR 广域网状态）

从广域网状态表中的每个条目可得到以下信息：

1、广播（Broadcasting）：APR 将广播包广播到局域网内所有主机。

2、半路由（Half-Routing）：此状态意味着 APR 能正确的路由通信，但只有一个方向（如：“客户端－>服务器”或“服务器－>客户端”），当局域网内有不均匀路由或两主机之一不能欺骗时会发生此情况，此时若有使用交换应答机制的认证通信，Cain 是不能捕获认证信息的。

3、全路由（Full-Routing）：意味着能欺骗注入两主机间的通信，并以全双功工作，如：“客户端<－>服务器”，嗅探器可完全捕获认证信息。

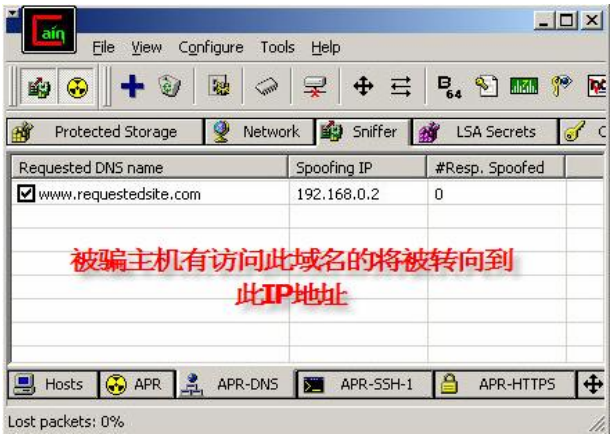
DNS 欺骗（APR-DNS）

对 DNS 应答包执行 DNS 欺骗。

- **工作原理**

ARP－NDS 欺骗只简单的改写 DNS 应答包中的 IP 地址，Cain 嗅探器提取 NDS 请求包

中的域名，并从欺骗列表中查找相应的地址，若有匹配的，数据包就被重写为相关欺骗的 IP 地址，并用 APR 欺骗引擎重路由之，这样客户端就收到了被欺骗的 DNS 应答包，从而有效的重定向到了预定目标 IP。



注意： 只有 DNS 应答包中的“Type-A”（主机地址）域被重写，DNS 缩略名也可被支持。

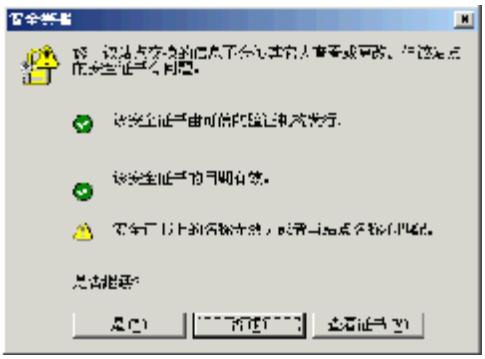
局限：因为使用 Winpcap 驱动程序，不能用于重写去往本地主机的 DNS 应答包，不能对本地进行欺骗。

用法：首先配置要欺骗的域名和相应要重写的 IP 地址，添加到 APR－DNS 表中，然后执行欺骗。表中“#Resp. Spoofed”列指示了欺骗应答的数量。

HTTPS 欺骗（APR-HTTPS）

APR-HTTPS 可以捕获并解密两主机间的 HTTPS 通信，它与 Cain 的证书收集器（Certificate Collector）协同工作注入伪造的证书到 SSL 会话中去，使用此欺骗，可能在到达真实目的地前解密加密的数据，此种攻击也是中间人攻击。

警告：客户端会注意到此类攻击，因为被注入到 SSL 会话服务器证书是伪造的，尽管它很象真实的证书，因为证书未经受信任的 CA（证书机构）签名。当受害主机开始一个 HTTPS 会话时，他的浏览器显示一个弹出对话框警告此类问题（右图）。



APR-HTTPS 使用证书收集器操纵的证书文件，它们包含与真实证书除不对称密钥外的相同参数，这将会欺骗绝大多数用户接受服务器证书并继续 SSL 会话。

APR-HTTPS 表中下部分表包含了 MITM 攻击捕获的所有的会话文件，加密的数据保存在 HTTPS 子目录下的文本文件中。

Ⅰ 工作原理

Cain 的 HTTPS 嗅探器工作在全双功客户端透明模式，服务器和客户端的通信被加密，且如果欺骗被激活，攻击者的 IP 和 MAC 地址决不暴露给受害客户端，连接被本地监听的 HTTPS“接收器”接收（配置中指定），劫持客户端连接。OpenSSL 库用来管理多个 SSL 通信，一个用于“客户端<－>CAIN”，另一个用于“CAIN<－>服务器”。

以下是工作的详细步骤：

1、 HTTPS 过滤器由用户从配置对话框中激活；
2、 APR 欺骗由用户从工具栏按钮激活，中间人攻击就绪；
3、 受害主机开始一个新 HTTPS 的会话（如 https://login.passport.com）；
4、 来自客户端的包被 APR 注入，并被 Cain 的嗅探器捕获；
5、 APR-HTTPS 从证书收集器中搜索一个与服务器相应的伪造的证书，若有则使用它，若无则自动下载，并适当修改存入本地以备后用；

6、 受害包被修改以便重路由到本地接收者，修改项目有：MAC 地址、IP 地址、TCP 源端口（端口地址转换－PAT用于处理多重连接），修改的数据使用 Winpcap 重新发送到局域网上，以便与客户端建立连接；

7、 创建服务器端连接，连接到受害者想要连的真实的服务器；

8、 使用 OpenSSL 库管理加密的通信，此连接是用受害客户端的伪造证书与真实服务器建立的；

9、 包由客户端发送出去，被修改后又再次回到受害客户端；

10、来自服务器的数据被加密并保存到会话文件中，重新加密并经客户端连接发送到受骗主机；

11、来自客户端的数据被加密并保存到会话文件中，重新加密并经服务器端连接发送到服务器。

尽管使用伪造的证书能被发现，但这种攻击对客户机来说还是秘密的，因为受害者认为连接到了真实的服务器，可自己运行“netstat -an”检查一下。

一旦加密，来自客户端的通信还是发送给 HTTP 嗅探器来对证书做进一步的分析，可以通过会话文件来查看详细内容。

局限：不能象代理服务器那样工作，因为使用 Winpcap 驱动不能从本地主机发起加密 HTTPS 会话。

用法：成功设置 APR 后，激活 HTTPS 嗅探过滤器，会话自动的保存进 HTTPS 子目录，可以通过列表中菜单的相应功能查看它。

远程桌面欺骗（APR-RDP）

APR-RDP 能捕获并解密 RDP 远程桌面协议（Remote Desktop Protocol RDP ），RDP 是 Windows 远程计算机的终端服务协议。Windows 2000 终端服务可被安装为两种模式之一：可管理的和应用程序服务器，在管理模式中只有具有管理权限的用户能访问终端服务器。默认情况下终端服务的通信是被加密的，协议使用 RC4 对称加密算法并分为以下级别：

高：客户端、服务器使用 128 位密钥双向加密；

中：56 位密钥双向加密；

低：只加密从客户端向服务器的数据，依客户端版本不同使用 56 或 40 位密钥加密。

RDP 攻击的原理也是 MITM，是中间人攻击。详略。

微软已经对此弱点有所意识，但用 MITM 还是可以攻破的。在密钥交换初始化阶段，终端服务器发送到客户端一个服务端创建的证书（终端地创建的），此证书保存在服务器的注册表中：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters\Certificate

它包含一个 RSA 公钥和它的数字签名，如下图：

公钥系统与存储在服务器的 LSA 秘密“L$HYDRAENCKEY”中的 RSA2 键提供的相同（可

从 LSA 秘密转储器中检查它），签名是用于客户端校验服务器标识的信息。

微软使用另一种 RSA 私钥签名终端服务公钥并且它的私钥也是公开的！!不可思议，却是事实！相关文件是“mstlsapi.dll”，每个 Windows 用户都有此文件，这是一种新型公私钥（PPK）?!? Windows 的终端服务器 PPK 如下：

```
public exponent: e
0x5B,0x7B,0x88,0xC0

public modulus: n
0x3D,0x3A,0x5E,0xBD,0x72,0x43,0x3E,0xC9,0x4D,0xBB,0xC1,0x1E,0x4A,0xBA,0x5F,0xCB,
0x3E,0x88,0x20,0x87,0xEF,0xF5,0xC1,0xE2,0xD7,0xB7,0x6B,0x9A,0xF2,0x52,0x45,0x95,
0xCE,0x63,0x65,0x6B,0x58,0x3A,0xFE,0xEF,0x7C,0xE7,0xBF,0xFE,0x3D,0xF6,0x5C,0x7D,
0x6C,0x5E,0x06,0x09,0x1A,0xF5,0x61,0xBB,0x20,0x93,0x09,0x5F,0x05,0x6D,0xEA,0x87,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00

private exponent: d
0x87,0xA7,0x19,0x32,0xDA,0x11,0x87,0x55,0x58,0x00,0x16,0x16,0x25,0x65,0x68,0xF8,
0x24,0x3E,0xE6,0xFA,0xE9,0x67,0x49,0x94,0xCF,0x92,0xCC,0x33,0x99,0xE8,0x08,0x60,
0x17,0x9A,0x12,0x9F,0x24,0xDD,0xB1,0x24,0x99,0xC7,0x3A,0xB8,0x0A,0x7B,0x0D,0xDD,
0x35,0x07,0x79,0x17,0x0B,0x51,0x9B,0xB3,0xC7,0x10,0x01,0x13,0xE7,0x3F,0xF3,0x5F,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00

secret prime factor: p
0x3F,0xBD,0x29,0x20,0x57,0xD2,0x3B,0xF1,0x07,0xFA,0xDF,0xC1,0x16,0x31,0xE4,0x95,
0xEA,0xC1,0x2A,0x46,0x2B,0xAD,0x88,0x57,0x55,0xF0,0x57,0x58,0xC6,0x6F,0x95,0xEB,
0x00,0x00,0x00,0x00

secret prime factor: q
0x83,0xDD,0x9D,0xD0,0x03,0xB1,0x5A,0x9B,0x9E,0xB4,0x63,0x02,0x43,0x3E,0xDF,0xB0,
0x52,0x83,0x5F,0x6A,0x03,0xE7,0xD6,0x78,0x45,0x83,0x6A,0x5B,0xC4,0xCB,0xB1,0x93,
0x00,0x00,0x00,0x00

d mod (p-1): dmp1
0x65,0x9D,0x43,0xE8,0x48,0x17,0xCD,0x29,0x7E,0xB9,0x26,0x5C,0x79,0x66,0x58,0x61,
0x72,0x86,0x6A,0xA3,0x63,0xAD,0x63,0xB8,0xE1,0x80,0x4C,0x0F,0x36,0x7D,0xD9,0xA6,
0x00,0x00,0x00,0x00

d mod (q-1): dmq1
0x75,0x3F,0xEF,0x5A,0x01,0x5F,0xF6,0x0E,0xD7,0xCD,0x59,0x1C,0xC6,0xEC,0xDE,0xF3,
0x5A,0x03,0x09,0xFF,0xF5,0x23,0xCC,0x90,0x27,0x1D,0xAA,0x29,0x60,0xDE,0x05,0x6E,
0x00,0x00,0x00,0x00

q^-1 mod p: iqmp
0xC0,0x17,0x0E,0x57,0xF8,0x9E,0xD9,0x5C,0xF5,0xB9,0x3A,0xFC,0x0E,0xE2,0x33,0x27,
0x59,0x1D,0xD0,0x97,0x4A,0xB1,0xB1,0x1F,0xC3,0x37,0xD1,0xD6,0xE6,0x9B,0x35,0xAB,
0x00,0x00,0x00,0x00
```

根据所知的 PPK 密钥，攻击者为 MITM 攻击中的 MITM 公钥计算一个有效的签名，客户端能正确的校验 MITM 签名，并接受此会话而不用通知用户服务器密钥已被修改。

SSH 欺骗（APR-SSH-1）

SSH（Secure Shell ）远程登录协议在不安全的网络中提供安全的认证和加密的通信。APR-SSH-1 使用 Cain 的 APR MITM 中间人攻击捕获并解密 SSH 会话。

SSH 通信的构成分为以下几个阶段：

连接：客户端连接到服务器的 SSH 端口（通常是 TCP 22 端口）。

认证阶段：服务器发送到客户端一个认证串，格式是“SSH-<主>.<次>-<版本>”，客户端分析此服务器串，并发送一个一致的串作为应答，此时 APR-SSH-1 自动替换服务器第一

个包中为特定版本，降级为 SSH v1.51 通信。

协商阶段：服务器发送一不对称加密密钥和其他参数到客户端，Cain 收集服务器密钥并替换为本地新生成的密钥，以便客户端使用 MITM 密钥而不是服务器密钥。

会话设置阶段：客户端选择使用对称加密，并发送加密的会话密钥到服务器，此时会话密钥已经由客户端使用 Cain 的密钥加密，而不是用服务器密钥。因此程序能在发送回服务器之前解密并保存会话密钥，会话密钥对后续的解密是非常重要的。

加密阶段：服务器和客户端使用指定的对称密钥开始一个安全会话，Cain 可使用此会话密钥解密从网络上捕获的通信。

APR-SSH-1 工作在全双功模式来处理客户端和服务器双向的 SSH－1 通信，因为使用 APR（ARP 欺骗），攻击者的 IP 和 MAC 地址可以完全隐藏，而不暴露到网上，嗅探器劫持的加密算法有：DES、3DES、Blowfish。

证书收集器（Certificates Collector）

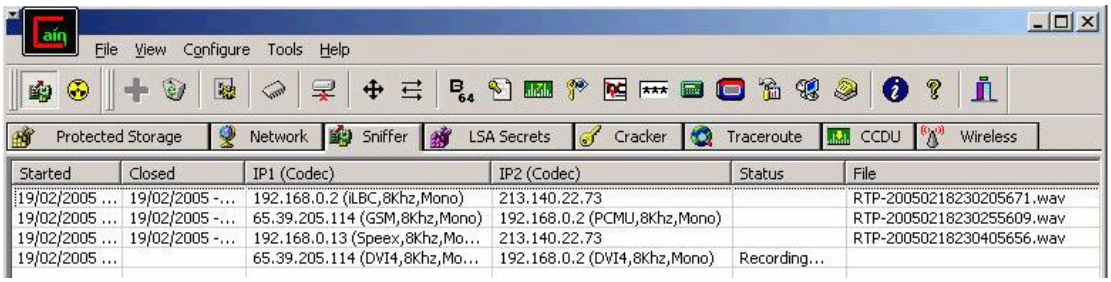
Cain 的证书收集器收集来自 HTTPS 站点的服务器证书，并为 APR－HTTPS 作准备。此功能由 HTTPS 嗅探过滤器自动使用，也可以手动创建一预计算的伪造的证书，这是为 APR－HTTPS 能通过 MITM 加密解密 HTTPS 通信而准备的。伪造的证书是由 Cain 自签名的，所以客户端浏览器会弹出对话框报告来自不受信息的证书机构，然而因为其他参数与真实证书一样，多数用户一般不会注意此警告。

伪造的证书保存在“Certs”子目录下，那些当前对 APR-HTTPS 活动的证书列表在“CERT.LST”文件中，你可以手动修改此列表文件以指示 Cain 的 APR-HTTPS 注入你选择的证书到自 APR 受害主机到指定 HTTPS 服务器地址的连接中。

用法：此功能 HTTPS 过滤器自动调用，你可以使用工具栏上的“＋”按钮手动收集并准备一伪造证书列表；非标准端口可指定端口，语法：“主机名：端口”或“IP 地址：端口”。

VoIP 嗅探（网络电话监听）

VoIP（Voice over IP）嗅探器捕获网络中的谈话并录音到硬盘，若被嗅探器发现，每个方向（呼叫者<－>应答者）的声音数据就被捕获，然后保存为单声道或立体声的 WAV文件。若用 APR 欺骗，能悄悄捕获网上的 VoIP通信。



VoIP使用信号协议，如 H323、SIP。声音数据流通常用 RTP（Real-Time Transport Protocol）实时传输协议来传输，RTP 提供不间断网络传输功能，适合程序在多播或单播网络服务上传输实时数据，如音频、视频和模拟数据，声音数据以压缩格式传送以节约带宽，编解码器常用来在发送接收端编码解码。

工作原理：嗅探器提取 RTP 会话参数，如 RTP 端口、呼叫应答者的 IP 地址、SIP 会话动态编解码器类型，然后捕获并解码 RTP 音频流，音频流一般用以下编解码器编码：

G711uLaw、G771aLaw、ADPCM、DVI4、LPC、GSM610、MicrosoftGSM、L16、G729、Speex、iLBC、G722.1、G723.1、G726-16、G726-24、G726-32、G726-40、LPC-10，同时解码的音频保存到 WAV文件中。

FAQ

Q：此程序是病毒吗？

A：不是，绝对不是！它不感染文件，不会发送你的口令到互联网上，它不传播自己，并且不含有间谍代码。若不相信，可用防火墙检查它。

Q：什么是 APR?

A：APR(ARP Poison Routing) 是程序的一项重要功能，它能在交换式局域网中劫持、嗅探 IP 通信，APR 使用 ARP 欺骗（毒害）技术完成此项目的，所以你可用此功能重定向不同子网的或 VLAN 的主机间的通信。以下网址是 APR 的动画演示：http://www.oxid.it/downloads/apr-intro.swf。

Q: 录制 RTP 会话后，VoIP 嗅探器说“unable to convert”（不能转换），并且 WAV 没有被保存，为什么？

A: 嗅探器不支持 RTP 会话使用的编码。

附录

HTTPS 嗅探器输出举例

数据来自登录 http://www.hotmail.com 的 HTTPS 会话：

```
==========================================
=== Cain's HTTPS sniffer generated file ===
==========================================

[Client-side-data]
POST
/ppsecure/post.srf?lc=1040&id=2&ru=http://www.hotmail.msn.com/cgi-bin/sbox&tw=20&fs=1&cbid=24325&da
=passport.com&kpp=2&svc=mail&msppjph=1 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: it
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Cookie: BrowserTest=Success?; vv=25
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: login.passport.com
Content-Length: 95
Connection: Keep-Alive
Cache-Control: no-cache
Referer: http://login.passport.net/uilogin.srf?id=2
login=testuser@test.test&domain=passport.com&passwd=testpassword&sec=&mspp_shared=&padding=xxxx

[Server-side-data]
HTTP/1.1 200 OK
```

Connection: close
Date: Wed, 08 Dec 2004 18:33:52 GMT
Server: Microsoft-IIS/6.0
PPServer: PPV: 25 H: BAYPPLOG2A04 V: 1113
Content-Type: text/html
Expires: Wed, 08 Dec 2004 18:32:52 GMT
Cache-Control: no-cache
cachecontrol: no-store
Pragma: no-cache
P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"
Content-Length: 412

[Server-side-data]
<HTML><HEAD><meta HTTP-EQUIV="Content-Type" content="text/html; charset=iso-8859-1"><META HTTP-EQUIV="REFRESH" CONTENT="0; URL=http://login.passport.com/login.srf?lc=1040&sf=1&id=2&ru=http://www.hotmail.msn.com/cgi-bin/sbox&tw=20&fs=1&cb=&cbid=24325&ts=0&login=testuser%40test.test&domain=passport.com&sec=&mspp_shared=&ec=e5a&seclog=0&kpp=2&svc=mail&msppjph=1"><script>function OnBack(){}</script></HEAD></HTML>

SSH－1 嗅探器输出举例

==
=== Cain's SSH-1 sniffer generated file ===
==
SSH-1 connection

Server address: 192.168.1.1
Client address: 192.168.1.14
Identification phase

Server ID string: SSH-1.5-Cisco-1.25
Client ID string: SSH-1.5-OpenSSH_3.4p1
Negotiation phase

Ciphermask from server: 0x4
Supported ciphers: DES,
Authmask from server: 0x8
Supported authentications: Password,
Session setup phase

Cookie: 810840239c21da11
Server-side SessionID: 9b3184746c54071009f992446684e9b7
Client-side SessionID: afdbfbc65991d658886bf6d571d3e535
Session Key: 87d08c9e22f891ac62f66a0059def069258bcce2e21a3e6969091edc60f36f46
Client cipher: DES
Encrypted state reached

[Server] Message type 14 (Command Success)
[Client] Message type 4 (Username)
Authentication phase

Username: pix
[Server] Message type 15 (Command Failure)
[Client] Message type 9 (Password Authentication)
Password: test [Server] Message type 14 (Command Success)
[Client] Message type 10 (PTY Request)
[Server] Message type 14 (Command Success)
[Client] Message type 12 (Shell Session Request)
Type help or '?' for a list of available commands.
pixfirewall>
pixfirewall> eenn
Password: t*e*s*t*
pixfirewall# sshhooww rruunn

```
: Saved
:
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password N7FecZuSHJlVZC2P encrypted
passwd N7FecZuSHJlVZC2P encrypted
hostname pixfirewall
domain-name test.lab
clock timezone CEST 1
clock summer-time CEDT recurring last Sun Mar 2:00 last Sun Oct 3:00
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list outside_access_in permit icmp any any
access-list inside_access_in permit ip any any
pager lines 24
logging trap alerts
interface ethernet0 10baset
interface ethernet1 10full
icmp deny any outside
mtu outside 1500
mtu inside 1500
ip address outside dhcp setroute retry 4
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
access-group outside_access_in in interface outside
access-group inside_access_in in interface inside
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server community local.net.snmp
no snmp-server enable traps
floodguard enable
sysopt noproxyarp outside
sysopt noproxyarp inside
no sysopt route dnat
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 5
dhcpd address 192.168.1.2-192.168.1.33 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd domain test.lab
```

dhcpd auto_config outside
dhcpd enable inside
terminal width 80
Cryptochecksum:64904979a6185a10596856cde6104bb1
: end
pixfirewall# eexxiitt
Logoff
[Server] Message type 20 (Exit status)
[Client] Message type 33 (Exit confirmation)