

Cain 使用教程图文并茂版(图)

- **摘要:** Cain & Abel 是由 Oxid.it 开发的一个针对 Microsoft 操作系统的免费口令恢复工具。号称穷人使用的 L0phtcrack。它的功能十分强大，可以网络嗅探，网络欺骗，破解加密口令、解码被打乱的口令、显示口令框、显示缓存口令和分析路由协议，甚至还可以监听内网中他人使用 VOIP 拨打电话。
- **标签:** [Cain](#) [使用教程](#) [sniffer](#)

Cain & Abel 是由 Oxid.it 开发的一个针对 Microsoft 操作系统的免费口令恢复工具。号称穷人使用的 L0phtcrack。它的功能十分强大，可以网络嗅探，网络欺骗，破解加密口令、解码被打乱的口令、显示口令框、显示缓存口令和分析路由协议，甚至还可以监听内网中他人使用 VOIP 拨打电话。

Abel 是后台服务程序，一般不会用到，我们重点来介绍 Cain 的使用。

Cain 安装：首先我们需要安装 Winpcap 驱动，



一路 next 下去就可以安装成功了



然后我们就可以使用 Cain 了，让我们打开传说中的 Cain，界面十分简单明了，



但是它的功能可就不简单了。

Cain 使用：

一、读取缓存密码：切换到“受保护的缓存口令”标签，点上面的那个加号



缓存在 IE 里的密码全都显示出来了。

二、查看网络状况

切换到“网络”标签，可以清楚的看到当前网络的结构，我还看到内网其他的机器的共享目录，用户和服务，通过上图，我们清楚的看到 Smm-DB1 开启了 IPC\$默认共享连接和其他盘隐藏共享。

三、ARP 欺骗与嗅探

ARP 欺骗的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。ARP 欺骗和嗅探是 Cain 我们用的最多的功能了，切换到“嗅探”标签



在“嗅探器”中选择要嗅探的网卡，在“ARP(Arp Poison Routing)”中可以伪造 IP 地址和 MAC 地址进行欺骗，避免被网管发现。



在“过滤与端口”中可以设置过滤器，



可以根据自己的需要选择过滤的端口，如嗅探远程桌面密码的话，就勾选 RDP 3389 端口。

小提示：比如我要嗅探上面的 61.132.223.10 机器，第二个网卡显示我的 ip 地址为 61.132.223.26，和目标机器是同一内网的，就使用第二个的网卡欺骗。



单击网卡的那个标志开始嗅探，旁边的放射性标志则是 ARP 欺骗。

	FTP server	Client	Username	Password
0:13:27	61.132.223.11	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:14:45	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:47:46	61.132.223.11	61.132.223.26	anonymi	IEUser@
0:47:46	61.132.223.11	61.132.223.26	anonymi	IEUser@
0:47:46	61.132.223.11	61.132.223.26	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:30	61.132.223.11	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:31	61.132.223.11	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:32	61.132.223.11	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:32	61.132.223.11	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:33	61.132.223.11	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:34	61.132.223.11	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:52	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:52	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:06:57	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:07:02	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:07:07	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:07:12	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:08:49	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:08:53	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:08:58	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:09:02	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...
0:09:07	61.132.223.10	61.132.223.13	sxQlfjy0521Ka40	HyvqWly1643D...

FTP

截获密码 VoIP



嗅探了 N 久之后，点击下面的“截获密码”，嗅探所得到的密码会按分类呈现在大家面前，包括 http、ftp、VNC、SMTP、ICQ 等密码。如果目标主机使用 voip 电话的话，还可以获得他使用 voip 电话的录音(恐怖吧)，如图





下面我们来进行 Arp 欺骗，点击下面的“ARP”标签，



在右边的空白处单击，然后点上面的“加号”，出现“新建 ARP 欺骗”对话框，在左边选网关，右边选择被欺骗的 IP。

这里要注意的是，你的机器性能比网关差的话，会引起被欺骗机器变慢。

1.DNS 欺骗:

在“DNS 欺骗”中填入请求的 DNS 名称和响应包的 IP 地址,



如图,当目标地址访问 www.hao123.com 的时候就自动跳转到 WwW.google.cn 的网站上面,其中的“#resp. 欺骗”就是目标主机被欺骗的次数。

这样对于目标机器进行挂马也不失为一种绝妙的方法。点上面的放射性标志开始 Arp 欺骗,

小提示: 网关 IP 可以在命令行下输入 ipconfig 获得



如图,网关 IP 为 61.132.223.4

2.远程桌面欺骗:

Cain 能够实行中间人攻击(Man-In-The-Middle)远程计算机的终端服务协议(Remote Desktop Protocol RDP)进行截获和解密工作。也就是截获目标主机的 3389 登陆密码。



在“ARP-RDP”里已经得到了 3 个数据包。右击右边得到的数据包，选择“查看”，



我的运气比较好,获得了目标主机登陆 3389 的用户和密码,如图,用户名为“administrator”密码为“asdf1234”。

小技巧: 在肉鸡上对密码进行嗅探的时候,可以按 Alt +Delete 对界面进行隐藏,按 Alt + Page Down 隐藏都任务栏,按 Alt +Page up 呼出界面。这个技巧在内网渗透的时候非常有用!

四、密码的破解

Cain 还具有强大的破解功能,可以破解 md5,md4,pwl,mssql 等加密的密文,我这里示范如何使用 Cain 破解 md5 密文。



切换到“破解器”标签，在右边空白处单击，按上面的加号，输入我们要解密的 32 位密文，




右击要破解的密文，选择“暴力破解”，选择口令长度和密码范围，我这儿选择的是 5 到 6 位纯数字密码。



五、追踪路由

切换到“追踪路由”标签，在目标主机中填入目标主机的 ip 或者域名，我这填
www.hackerrxfiles.net



Hop	IP 地址	响应	响应	响应
1	192.168.10.254	16 ms (TTL=64) ...	16 ms (TTL=64) ...	16 ms (TTL=64) ...
2	192.168.99.1	0 ms (TTL=63) ...	0 ms (TTL=63) ...	0 ms (TTL=63) ...
3	220.173.137...	16 ms (TTL=253) ...	0 ms (TTL=253) ...	0 ms (TTL=253) ...
4	202.103.209.10	0 ms (TTL=252) ...	0 ms (TTL=252) ...	0 ms (TTL=252) ...
5	222.217.175.5	0 ms (TTL=249) ...	15 ms (TTL=249) ...	0 ms (TTL=249) ...
6	202.97.66.121	31 ms (TTL=244) ...	31 ms (TTL=244) ...	16 ms (TTL=244) ...
7	202.97.21.205	16 ms (TTL=247) ...	0 ms (TTL=247) ...	0 ms (TTL=247) ...
8	202.97.42.153	343 ms (TTL=246) ...	32 ms (TTL=246) ...	15 ms (TTL=246) ...

选择协议和端口，点“开始”，一杯咖啡过后，就可以清晰的看到访问黑 X BBS 所经过的所有服务器 IP、访问所需的时间和主机名。

另外，Cain 还具有“LSA 分析”和“嗅探无线网络”等功能，这些功能我们不经常用到，感兴趣的朋友可以自行研究。最新版本 cain4.92 已经加入 vista 支持，但是“读取读取缓存密码”功能不是很稳定，如果要读取读取缓存密码的话请使用以前的版本。最后要说一句：Cain 的确是一款绝佳的黑界利器，威力无穷，请各位小黑们谨慎使用。