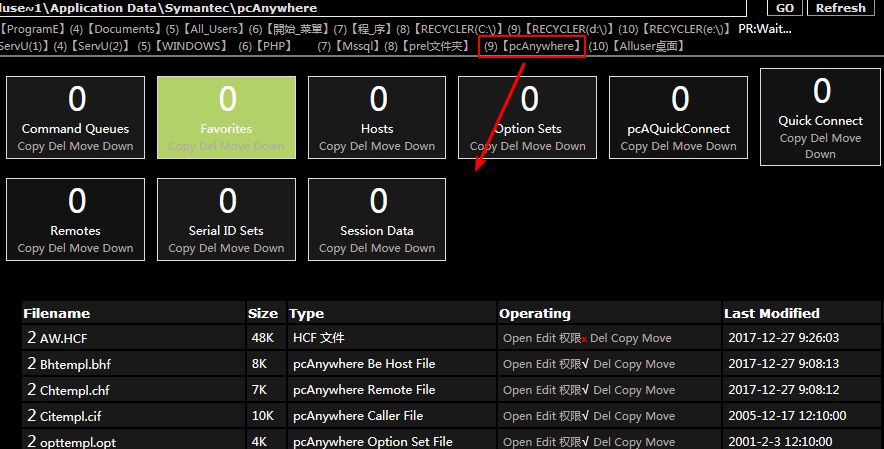
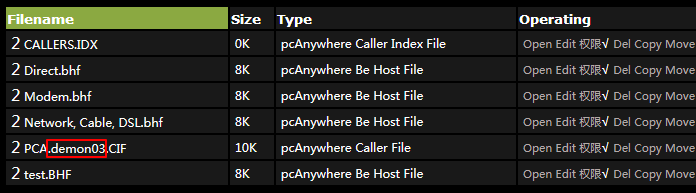
# pcanywhere提权

点快捷链接pcanywhere进入软件安装的默认路径



然后点Hosts目录，目录下面存放账号密码配置，名字中可以看出其用户名

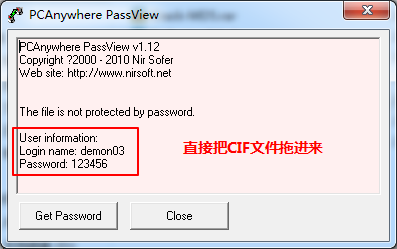


下载该.cif文件，使用工具破解出密码

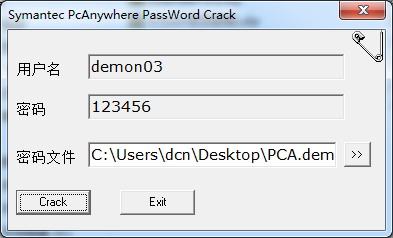


这里有两款工具推荐

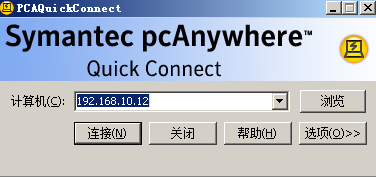
pcanypass



pcanywhere

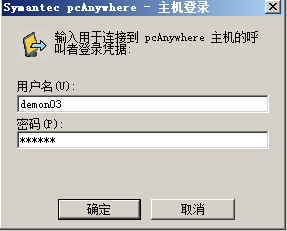


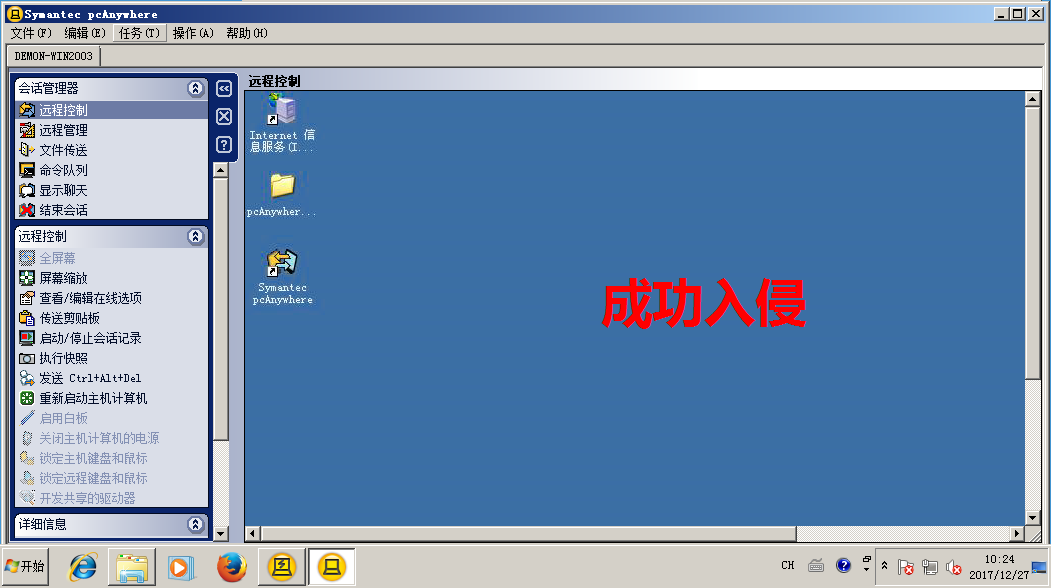
安装pcanywhere客户端（同时也是服务器）去连接目标即可



说明：win2003装的是可破密码版，win7装的是兼容版







入侵后可以锁定键盘和鼠标，可以net user，对方就只能强制关机了，

另外密码破解的速度很快，不管密码位数多长还是复杂度多高

