# SAM-HASH提权

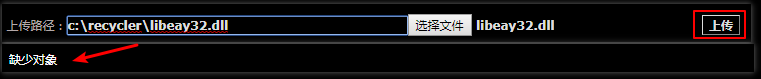
获取SAM文件中的HASH工具有几款，如

* QuarksPwDump.exe
* GetPass.exe
* Pwdump7.exe

但是经测试，每一款都需要有权限，于是就进入蛋生鸡，鸡生蛋的问题，

没有权限怎么运行这些工具？没有这些工具有怎么拿到管理员权限？

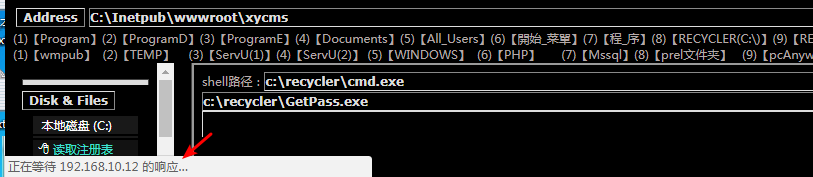
问题1：Diskill的大马，上传大文件会爆没有对象。

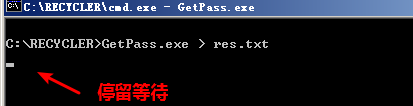


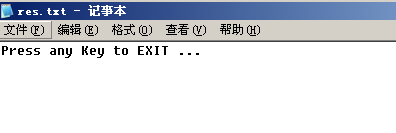
解决办法就是搞个一句话，用菜刀上传就好了



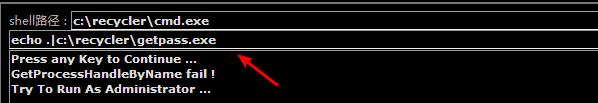
问题2：执行获取HASH工具时Diskill的大马会卡顿半天不出结果。



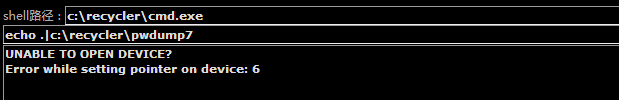


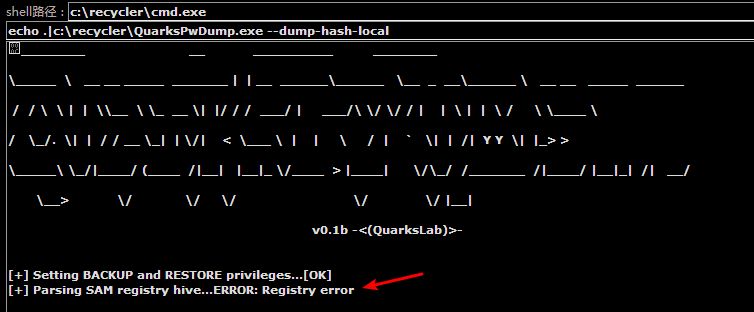


这是因为dos暂停了，需要按任意键，但是我们在大马是无法直接发送任意键，利用echo.管道传递即可解决，所以以后不管发送什么命令，都给这个命令传个回车（echo.）



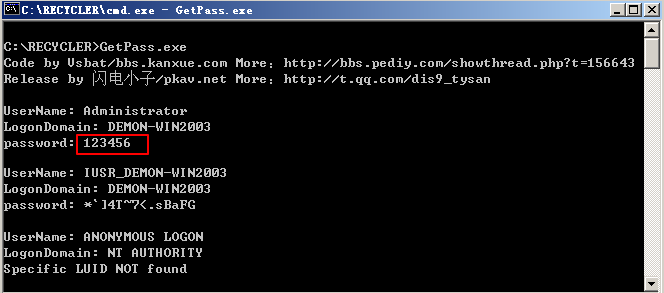
问题3：正如上图所示需要用Administrator用户来运行才行，但拿不到HASH密码又怎么以它运行呢？如果能以Administrator用户运行那还需要破解密码干嘛。。。其他工具也是类似



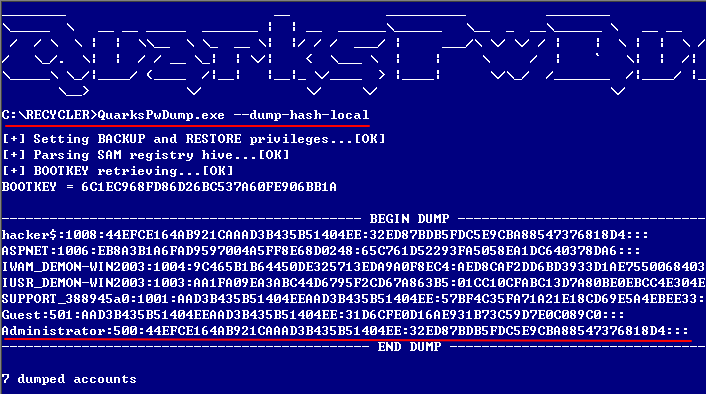


这个权限问题只能暂时放一边，我们直接用win2003靶机的admin~用户运行吧，这里就假设权限够大足以读取到HASH值来进一步破解和利用，

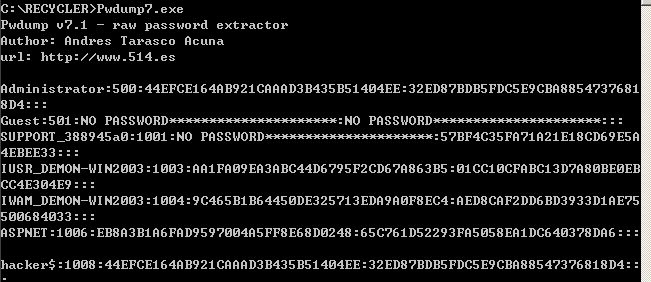
闪电小子写的GETPASS直接爆出密码，不需要去破解HASH了



QuarksPwDump.exe获取HASH值，包括隐藏账号 hacker$ 也获取到了

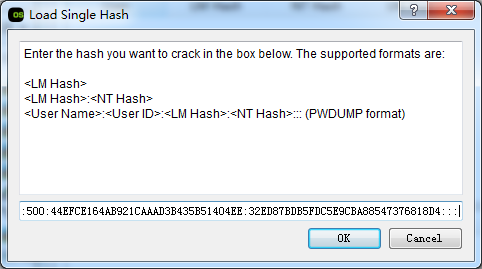


pwDump7.exe也差不多



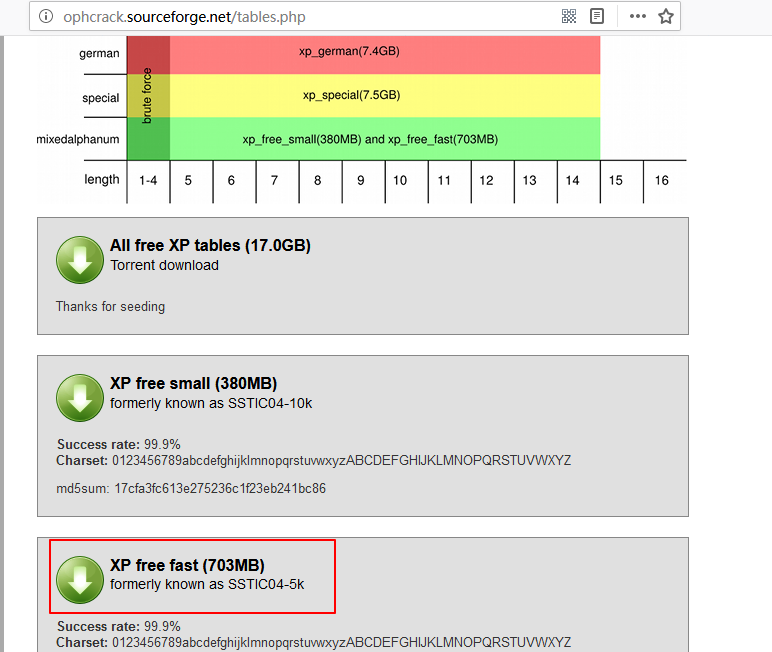
有了HASH值，如何对其破解呢？使用彩虹表破解开源工具ophcrack\_nogui.exe

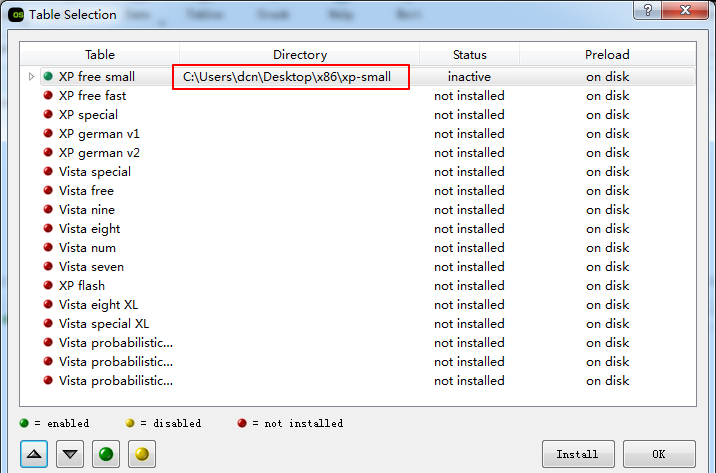
Administrator:500:44EFCE164AB921CAAAD3B435B51404EE:32ED87BDB5FDC5E9CBA88547376818D4:::



默认不带字典，字典需要自己去下面下载

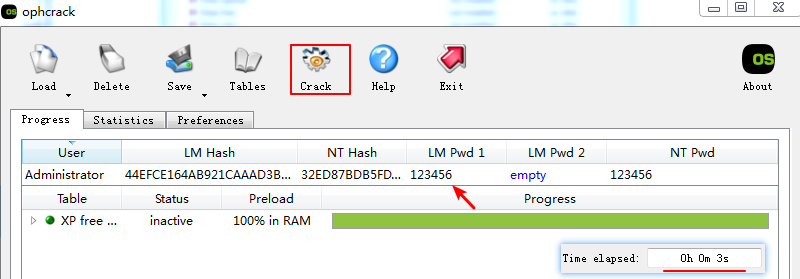
http://ophcrack.sourceforge.net/tables.php





然后点击Crack即可开始破解字典

彩虹表破解的速度还是蛮快的



有了密码就可以3389去连，但是这个哈希如何在没有管理员权限获取呢？留给以后解决吧