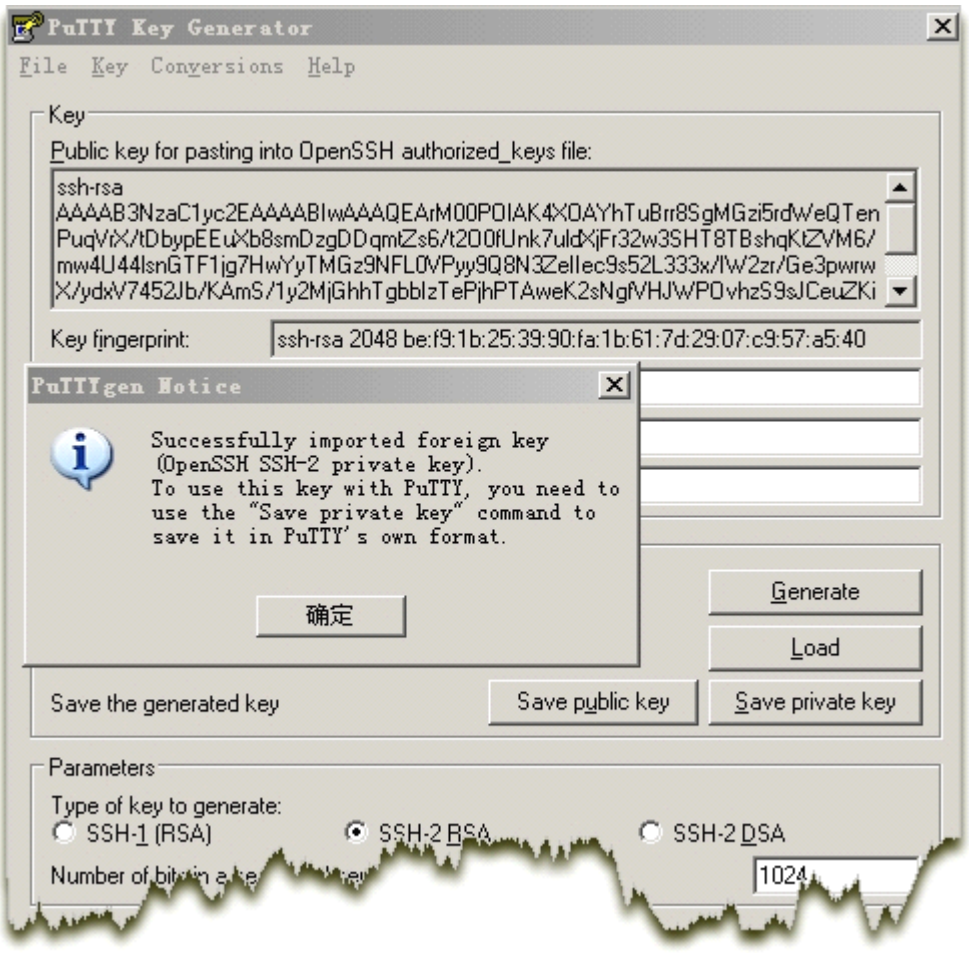
透过偷取 SSH 密钥搞定其他的机器

作者：mickey@pentest.cc

我进去 linux 主机后，都习惯看一看所有用户的.bash_history 文件，有时候，bash 脚本厉害的管理员会写出很有技巧性的 awk,grep,sed 语句来，很有意思。有的时候，管理员也会通过 vim 写一个 bash 备份数据库的脚本文件，而 mysql 密码往往也明文写在里面了。当然里面也往往存放着一些配置文件路径的信息，以及管理员通过 ssh,ftp 连接到其他 IP 的信息。

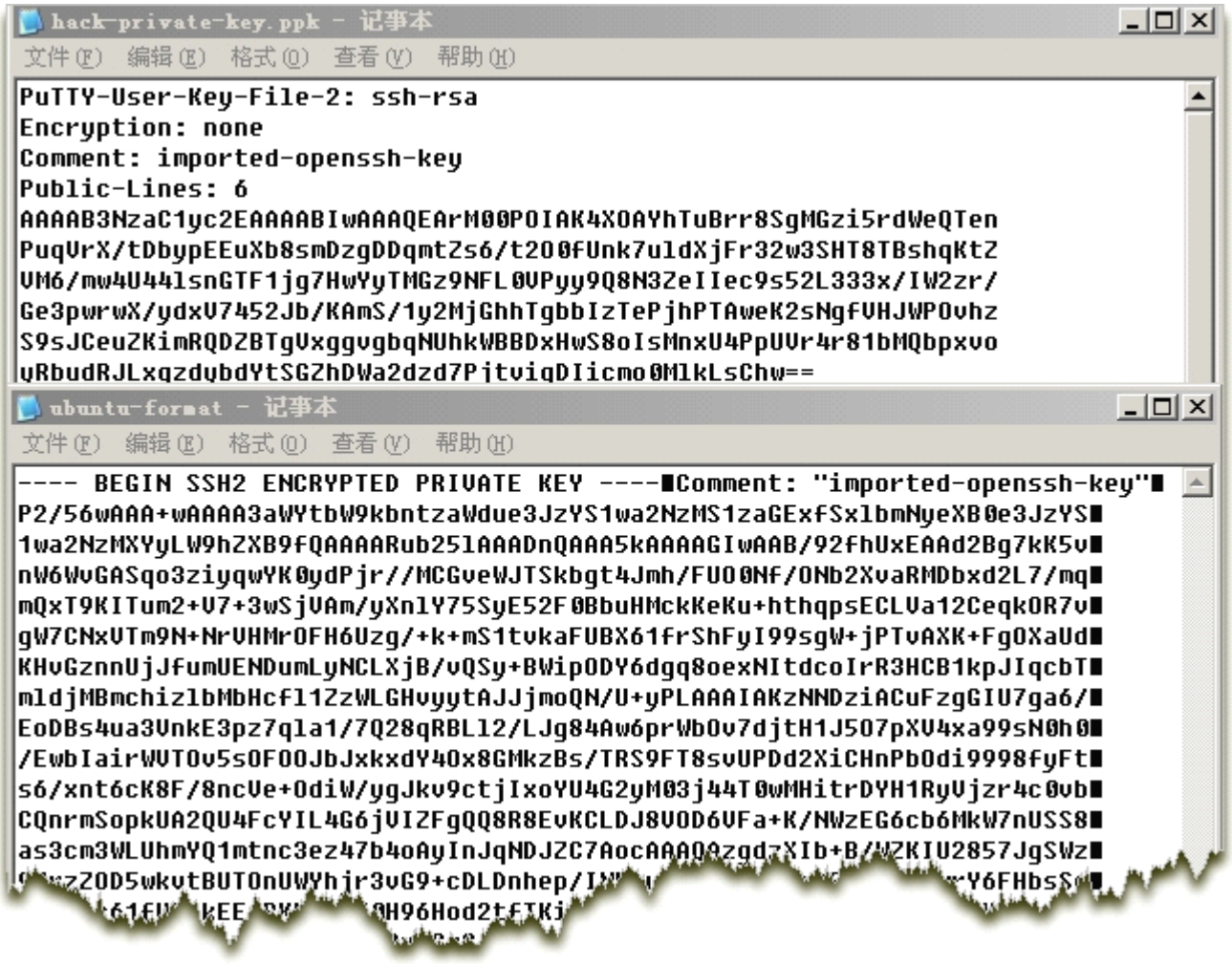
这次也是这样，我登陆了一台主机后,查看了他的.bash_history 文件，通过 cat .bash_history |grep "ssh"
把里面的 ssh 连接语句都摘录出来。然后浏览各个用户的.ssh 目录，寻找私钥，然后把这些私钥都拷贝回本地，尝试使用这些私钥去连接刚才在.bash_history 过滤出来的 ssh 主机。运气好的话，往往就能成功。

这个基本上都是体力活，但是这里只有一点要注意的，就是要注意私钥的格式。如果你是 WINDOWS 下使用 PUTTY 连接过去，则需要使用 puttygen.exe 来转换下格式，如下所示：

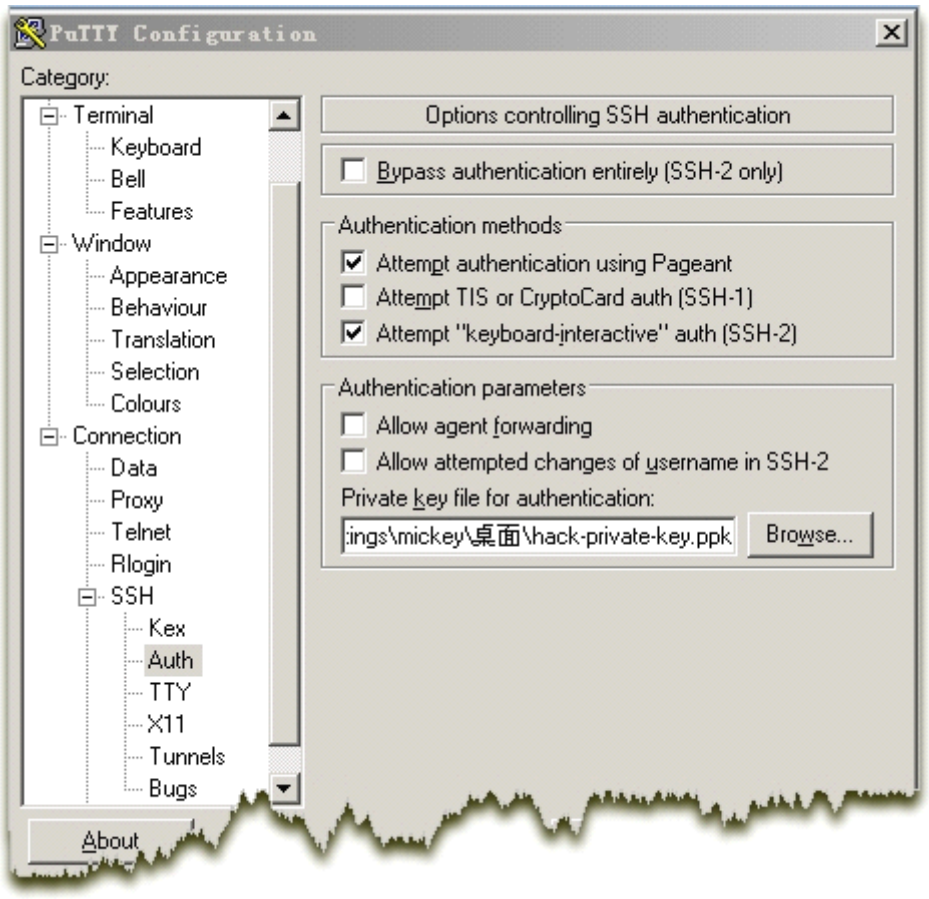


点"load"按钮，把从肉鸡上拷贝下来的私钥载入，然后点"save private key"保存成 putty 识别的格式。

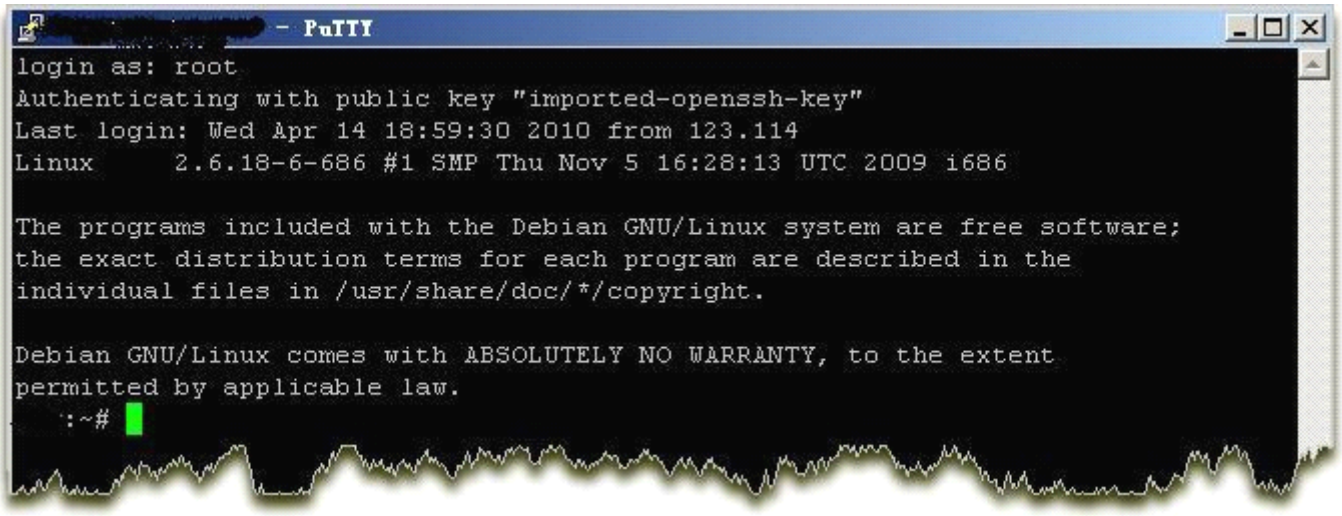
如下图可以看到转换前后，2 种格式的区别



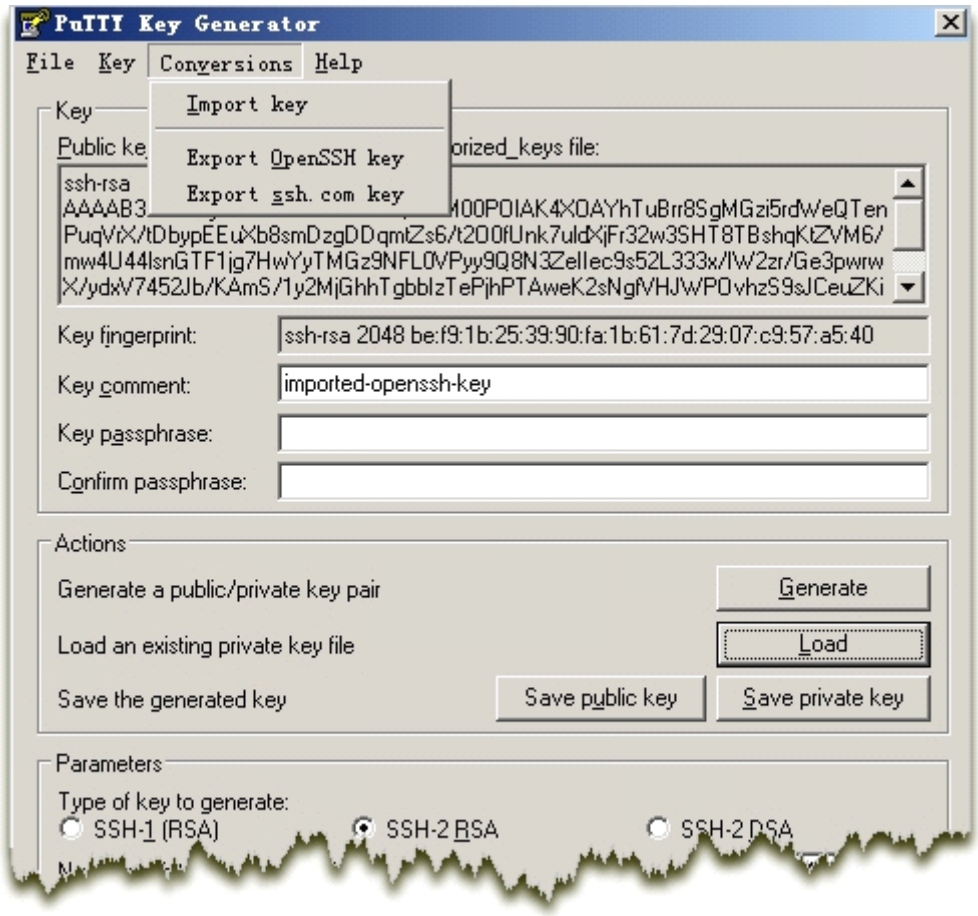
然后用 putty 载入转换好的私钥



现在连接过去，如果对方主机存放了公钥的话，就不需要输入密码了。



反之，如果你弄回来的是 putty 格式的私钥，同样使用 puttygen.exe 转换成 linux 下的格式，如下图



点"load"载入私钥，点"conversions"按钮，"export openssh key"就行了

这样你就能在 linux 下，把私钥放到当前用户的.ssh 目录下，然后使用 ssh 命令连接过去了