



**《网络安全与应用》实验报告**

**学 院 计算机**

**专 业 信息安全**

**年级班别 1601**

**学 号 3216005166**

**学生姓名 郭鹏燕**

**指导教师 孙宇平**

**提交时间 2018年11月**

**2018 年 11月**

**广东工业大学**

实验题目 实验一 RSA算法

1. **实验目的**
2. 理解非对称密码算法的工作原理
3. 了解RSA算法的密钥对生成、加密、解密过程，掌握其工作原理
4. 验证RSA 算法产生公钥和私钥的方法
5. 验证RSA的加密、解密过程
6. **实验要求**
7. 通过理解RSA算法，掌握使用蓝盾云安全实训平台
8. 熟练使用密码学教学软件crypto.exe用RSA算法进行加解密
9. **实验原理**
10. 公钥和私钥的产生 假设Alice想要通过一个不可靠的媒体接收Bob的一条私人信息。她可以 用以下的方式来产生一个公钥和一个私钥： RSA体制生成密钥的过程可以简单描述如下：

（1）、生成两个大素数p和q。

（2）、计算这两个素数的乘积n=p×q。

（3）、计算欧拉函数φ(n)=(p-1)(q-1)。

（4）、选择一个随机数e满足1<e。

（5）、计算ed=1 mod φ(n)。同余：ed-1能被φ(n)整除

（6）、保密d，p和q，公开n和e 这里的（n, e）就是公开的加密密钥。 （n，d）就是私钥。 Alice將她的公钥(N,e)传給Bob，而將她的私钥(N,d)藏起來。

1. 加密消息 假设Bob想给Alice送一个消息m，他知道Alice产生的N和e。他使用起先 与Alice约好的格式将m转换为一个小于N的整数n，比如他可以将每一个字 转换为这个字的Unicode码，然后将这些数字连在一起组成一个数字。假如 他的信息非常长的话，他可以将这个信息分为几段，然后将每一段转换为 n。用下面这个公式他可以将n加密为c：

n^e ≡ c(mod N)

计算c并不复杂。Bob算出c后就可以将它传递给Alice。

1. 解密消息 Alice得到Bob的消息c后就可以利用她的密钥d来解码。她可以用以下这 个公式来将c转换为n：

c^d ≡ n(mod N)

得到n后，她可以将原来的信息m重新复原。

解码的原理是 c^d ≡ n^(ed)(mod N)

以及ed ≡ 1 (mod p-1)和ed ≡ 1 (mod q-1)。由费马小定理可证明（因为p和q 是质数）n^(ed) ≡ n(mod p) 和 n^(ed) ≡ n(mod q)

这说明（因为p和q是不同的质数，所以p和q互质）

n^(ed) ≡ n(mod pq)

1. **实验过程及内容**
2. 以mod((学号后两位+15)\*3，100)右边最近的素数作为p，mod((学号后两位+52)\*4，100)右边第二个邻近的素数作为q。超出100的循环移位到0开始。
3. 手算p，q

**(66+25)\*3mod100=73** 🡪 **p=73**

**(66+52)\*4mod100=73** 🡪 **q=79**

1. 设置p、q、e参数，如图1.1



图1.1

1. 公钥随机选，分析私钥产生过程；



图1.2

1. 点击加密按钮，明文选自己名字的拼音，观察密文信息；

明文：**guopengyan**

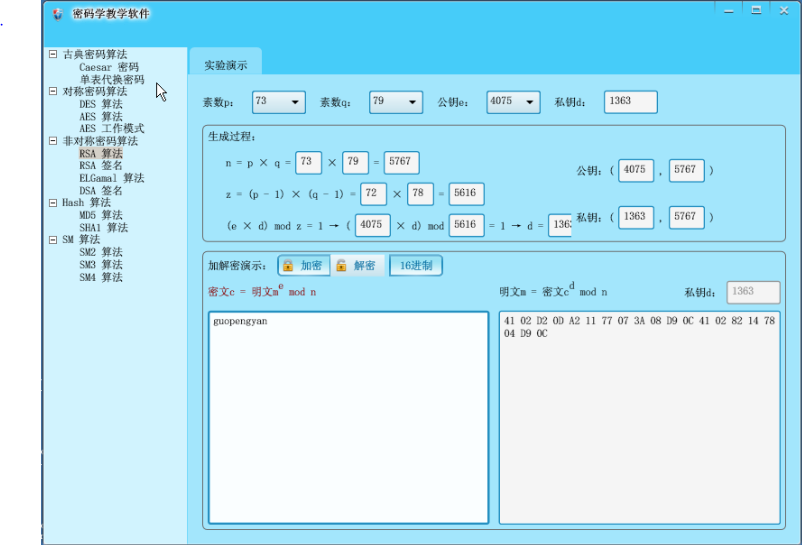


图1.3

点击解密按钮，修改私钥，观察解密后明文信息：修改私钥为：888

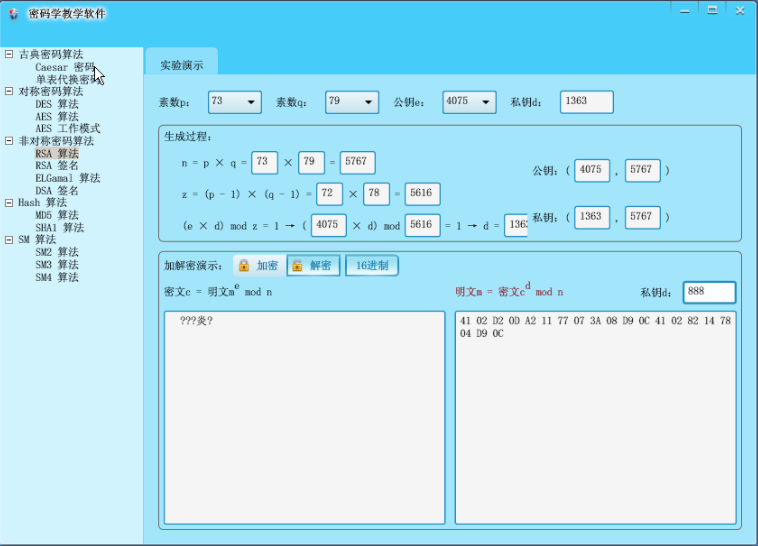


图1.4

1. **实验分析与结论**

通过该实验了解了RSA加解密的原理和安全性。

RSA算法安全性在于

* 使用更大长度的密钥
* n如何分解为两个素数看，由于大数n具有很大的素因子，因此分解因式非常困难。

1. **实验思考题**
2. 非对称密码算法适用于哪种场合？

速度较慢，适用于小数据量加解密或数据签名的场合。

1. 为什么RSA算法中即使公开公钥，也能保证私钥的安全？

如果根据公钥求私钥需要解决一个大素数分解成两个素数的问题，目前没有好的算法可以有效解决这个问题。

1. RSA公钥如何公开？RSA私钥如何分发？

公钥：通过可靠权威的三方平台但不一定是秘密的路由将公钥（*n*，*e*）发送出去；

私钥：永远不可能分发。

**广东工业大学**

实验题目 实验二 DDoS攻击

**一、实验目的**

1. 掌握DDOS攻击的基本原理

**二、实验要求**

通过windows主机，利用ddos攻击工具，对Linux主机进行攻击。

**三、实验原理**

拒绝服务就是用超出被攻击目标处理能力的海量数据包消耗可用系统，带宽资源，致使网络服务瘫痪的一种攻击手段。在早期，拒绝 服务攻击主要是针对处理能力比较弱的单机，如个人pc，或是窄带宽 连接的网站，对拥有高带宽连接，高性能设备的网站影响不大，但在 99年底，伴随着DDoS的出现，这种高端网站高枕无忧的局面不复存 在，与早期的DoS攻击由单台攻击主机发起，单兵作战相较，DDoS实现 是借助数百，甚至数千台被植入攻击守护进程的攻击主机同时发起的 集团作战行为，在这种几百，几千对一的较量中， 网络服务提供商所 面对的破坏力是空前巨大的。

分布式拒绝服务攻击,攻击者利用因特网上成百上千的“Zombie”(僵 尸)：被利用主机，对攻击目标发动威力巨大的拒绝服务攻击。攻击者的身份很难确认。

所有DDoS 攻击均由三部分组成:

1、客户端程序：Client Program（黑客）

2、主控端：Master Server

通常安装在ISP或大学网络

- 带宽保证

- 网络性能

3、“僵尸”：Agent (Zombie) Program

4、在TFN中，Master与Zombie间的通讯只是ICMP\_ECHOREPLY 数据包，没有TCP/UDP通信

DoS/DDoS攻击通常不会对敏感数据产生直接威胁。攻击者主要目 的是让被攻击系统停止正常服务，而不是窃取资料。

但是，DoS/DDoS经常被利用来掩盖真正的入侵攻击。另外，网络 管理人员在对付拒绝服务攻击时，往往修改系统或网络设备的一些设 置，从而留下其他可能被黑客利用的漏洞，例如停止或重新启动某种 服务，就可能产生问题。修改网络配置时，一定要清楚可能造成的后果。

* 1. **实验过程及内容**
* 在靶机-linux靶机打开终端，输入sudo iptraf（一个流量分 析工具），查看数据包情况（我们可以看到数据包流量正常）。

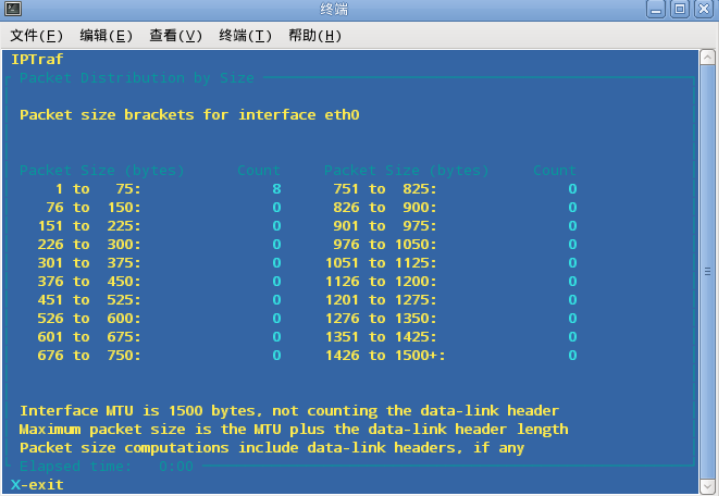


图2.1

* 在windows虚拟机启动ddos攻击工具，新建攻击--目标ip为linux虚拟机200.200.0.187

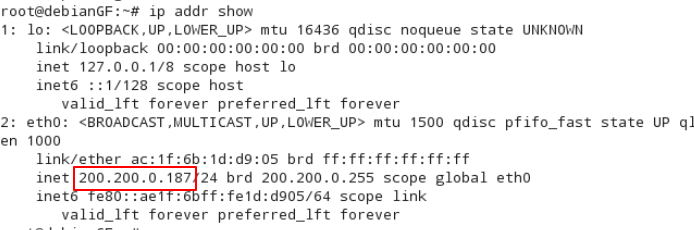


图2.2

* 选中刚刚新建的攻击然后点击“激活进程”



图2.3

* 观察靶机中iptraf的数据包变化

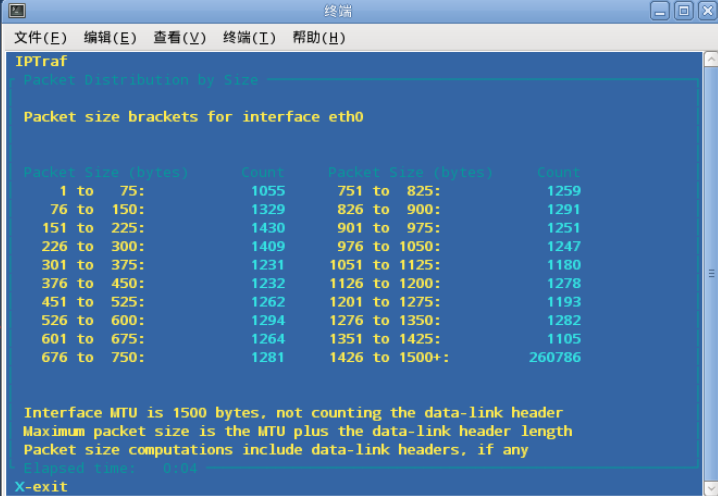


图2.4

* 回到windows虚拟机暂停攻击，再观察靶机上数据包的变化

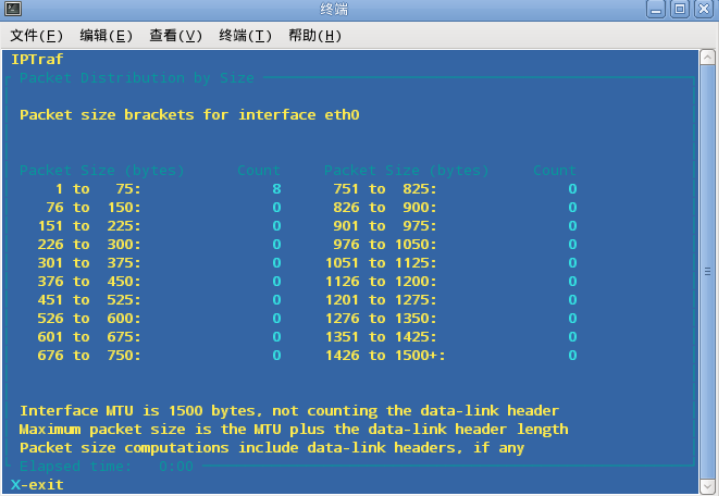


图2.5

**五、实验分析与结论**

DDOS攻击试图消耗目标设备的资源，使其不能提供服务。

**六、实验思考题**

DDOS攻击的基本原理是什么？

答：路由器转发处理能力强大，但是控制面和管理面处理能力有限。攻击者通过向路由器发起海量的消息请求或者畸形报文，导致CPU无法实时处理消息，引发正常的业务交互流程、内部处理流程阻塞，达到拒绝服务的目的。

DDOS难以彻底防御的原因是什么？

答：Ddos攻击其实就是攻守两房进行资源带宽的比拼，攻击方会使用大量的僵尸对目标服务器进行攻击，耗尽服务器的资源。而防御方需要购买足够的带宽，以硬件防护。然而攻击成本很低，防御成本却很高。而且攻击方常常使用多种攻击方式进行ddos攻击，几乎不需要技术上的创新。

**广东工业大学**

实验题目 实验三 SSL安全套层实现网络安全通信

**一、实验目的**

1. 掌握SSL协议的基本概念。
2. 掌握SSL协议体系结构的组成部分及其内涵。
3. 掌握SSL协议的实现步骤。

**二、实验要求**

1. 系统环境：Linux靶机一台，需关闭默认apache，开启lampp的http和 https对外web服务，自带wireshark可进行实时抓包。 Windows客户机一台，带有Firefox火狐浏览器。
2. 实验工具：Linux靶机需安装lampp(已安装)、wireshark(系统已自带)； Windows客户机需安装Firefox火狐浏览器（已安装）。
3. 开启lampp和http和https对外web服务

**三、实验原理**

SSL和TLS在传输控制协议（TCP）中通过结合对称和非对称算法提供 了加密、身份验证和数据完整性。在建立SSL会话时，要使用服务器的公钥 证书来验证服务器身份，并使用服务器的公钥加密以保护在客户端和服务器 之间安全交换共享密钥，并使用共享密钥生成在SSL通讯过程中对称加密算 法和基于哈希的消息验证码（HMAC）所需要的加密密钥和消息验证码， 以确保客户端与服务器之间数据传输的保密性和完整性。 SSL协议位于TCP/IP协议模型的传输层和应用层之间，使用TCP来提供 一种可靠的端到端的安全服务。SSL协议在应用层通信之前就已经完成加密 算法、通信密钥的协商以及服务器认证工作，在此之后应用层协议所传送的 数据都被加密。SSL实际上是由共同工作的两层协议组成，如下图所示。从 体系结构图可以看出SSL安全协议实际是由SSL握手协议、SSL修改密文协 议、SSL警告协议和SSL记录协议组成的一个协议族。

SSL记录协议：该子协议主要是为SSL连接提供保密性和消息完整性保 护。当通过SSL握手协议确定了客户端和服务器之间密码套件后，客户端和 服务器都拥有了加密和消息完整性验证所需的共享密钥，并且身份验证过程 也已完成，客户端和服务器之间的安全数据交换可以开始了。在通信过程 中，SSL记录协议实现安全数据交换过程涉及以下步骤：

* 1. 使用商定的压缩方法压缩数据；
  2. 根据商定的消息完整性验证方法创建数据的哈希值；
  3. 根据商定的加密方法加密数据；
  4. 发送数据到客户端或服务器；
  5. 根据商定的解密方法解密数据；
  6. 使用商定的消息完整性验证方法验证数据完整性；
  7. 使用商定的压缩方法解压数据

SSL密钥修改协议：该子协议主要为了进一步加强SSL通讯过程的安全 性，规定SSL通信双方在通信过程中每隔一段时间改变共享加密。协议由单 个消息组成，该消息只包含一个值为1的单个字节。该消息的作用就是协助 通信双方更新用于当前连接的共享密码。

SSL警报协议：该协议是用来为对等实体传递SSL的相关警告。如果在 通信过程中某一方发现任何异常，就需要给对方发送一条警报消息。警报消 息有两种：一种是关键错误警告消息，如传递数据过程中，通过完整性验证 算法发现传输数据有完整性错误，双方就需要立即中断会话，同时清除自己 缓冲区相应的会话记录；第二种是一般性的警告消息，在这种情况下通信双 方通常都只是记录日志，而通信过程仍然继续。

SSL握手协议：该协议主要用于建立SSL会话，并完成密码套件协商、 确定并交换共享密钥和身份验证。在建立SSL会话时，要使用服务器的公钥 证书来实现客户端和服务器之间安全的交换共享密钥。以下步骤介绍了建立 SSL会话的主要过程：

①客户端向服务器请求公钥证书；

②服务器发送公钥证书给客户端；

③客户端发送用服务器的公钥加密的会话密钥给服务器；

④服务器用公钥证书对应的私钥解密从客户端收到的会话密钥。

在①和②的通信过程中，客户端除了请求并验证服务器的公钥证书 外，还要完成密码套件的协商，协商的密码套件组合包括：协议版本、公钥 交换算法、对称加密算法、消息摘要算法、数据压缩方法等。密码套件协商 示例见下表：

在③和④的通信过程中，需要确定并交换相应的共享密钥。该共享密 钥是作为“预备主密钥”（pre-master secret），在通信双方得到“预备 主密钥”后，将其转换成主密钥，并通过相应算法计算得到用来加密和解密 客户端与服务器间交换的数据所需的对称加密密钥、实现完整性HMAC算 法所需的消息验证码和加密系统所需的初始值。完成后每端将得到6个密 钥，其中三个用于服务器到客户端的通信加密、消息完整性验证码以及初始 化加密系统的初始值，另外三个用于客户端到服务器的相应密钥。密钥交换 后所得的密钥值示例如下表所示:

当我们与一个网站建立https连接时，我们的浏览器与Web Server之 间要经过一个握手的过程来完成身份验证与密钥交换，从而建立安全连接。 其具体过程如下：

①用户浏览器将其SSL版本号、加密设置参数、与会话有关的数据以及 其它一些必要信息发送到服务器。

②服务器将其SSL版本号、加密设置参数、与会话有关的数据以及其它 一些必要信息发送给客户端浏览器，同时发给浏览器的还有服务器的证书。 如果配置服务器的SSL需要验证用户身份，还要发出请求要求浏览器提供用 户证书。

③客户端检查服务器证书，如果检查失败，提示不能建立SSL连接。如 果成功，那么继续。客户端浏览器为本次会话生成pre-master secret，并 将其用服务器公钥加密后发送给服务器。如果服务器要求验证客户身份，客 户端还要对另外一些数据签名后并将其与客户端公钥证书一起发送给服务 器。

④如果服务器要求验证客户身份，则检查签署客户证书的CA是否可 信。如果不在信任列表中，结束本次会话。如果检查通过，服务器用自己的 私钥解密收到的pre-master secret

⑤客户端与服务器通过某些算法生成本次会话的master secret，使用 此master secret生成本次会话的会话密钥(对称密钥)、消息验证码和加密 系统所需的初始值。

⑥客户端通知服务器此后发送的消息都使用这个会话密钥进行加密。 并通知服务器客户端已经完成本次SSL握手。

* 1. 服务器通知客户端此后发送的消息都使用这个会话密钥进行加密。 并通知客户端服务器已经完成本次SSL握手。
  2. ⑧本次握手过程结束，会话已经建立。双方使用同一个会话密钥分别 对发送以及接受的信息进行加解密

**四、实验过程及内容**

1. 在Linux中，开启xampp，不启用SSL安全通信的情况下用网络抓包工具wireshark，抓取浏览器的信息（过滤http）

打开”Terminal” > “cd/opt/lampp” >”./lamp start”



图3.1

1. 用windows系统的浏览器浏览：<http://200.200.0.114>



图3.2

1. 在终端运行wireshark

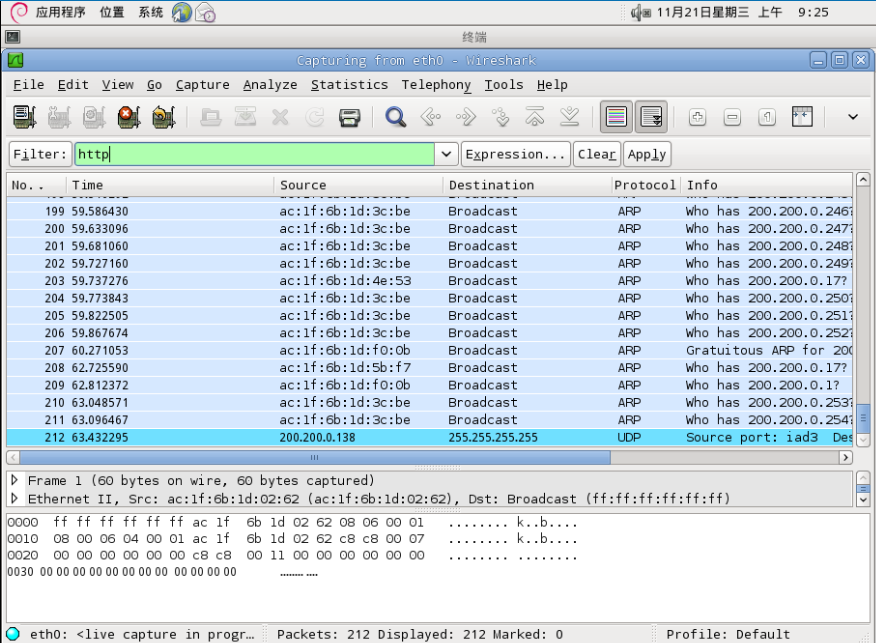


图3.3

1. 在window浏览器点击打开“phpinfo()”和”安全”页面查看

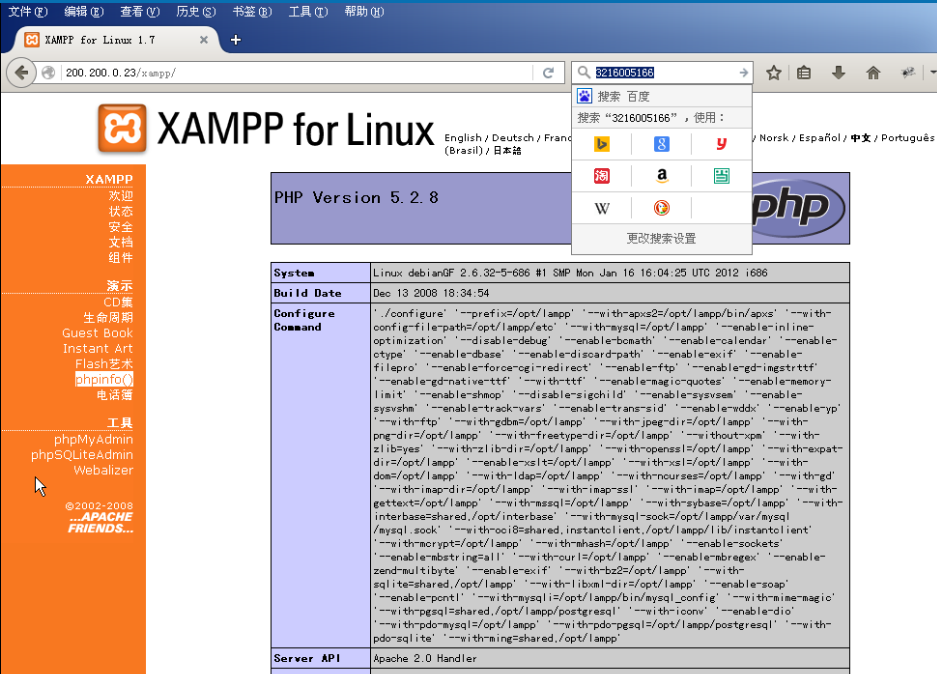


图3.4



图3.5

1. 回到终端

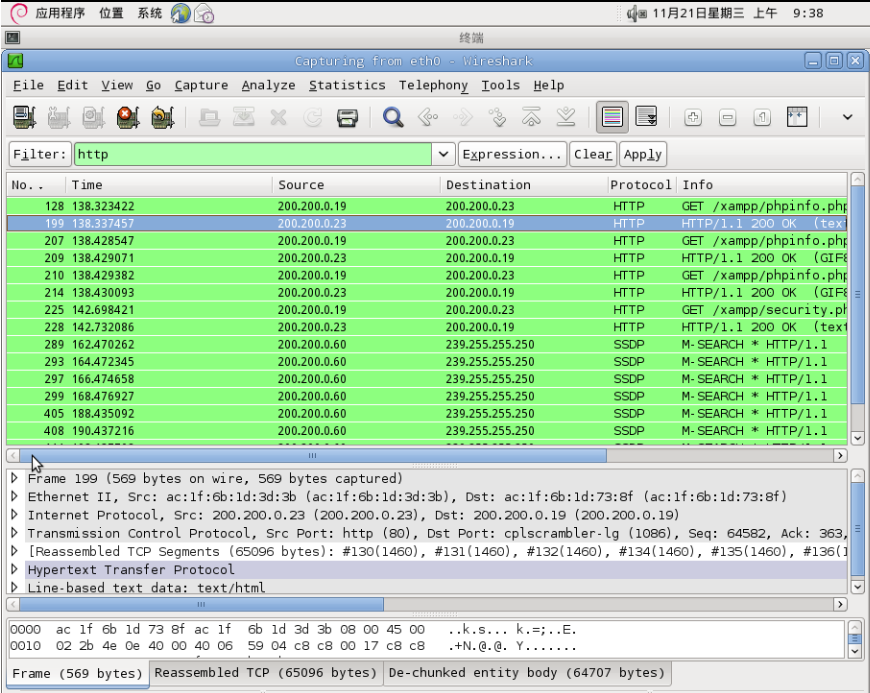


图3.5Wireshark截取http包

1. 开启apache的SSL模版，在用网络抓包工具，抓取浏览器信息

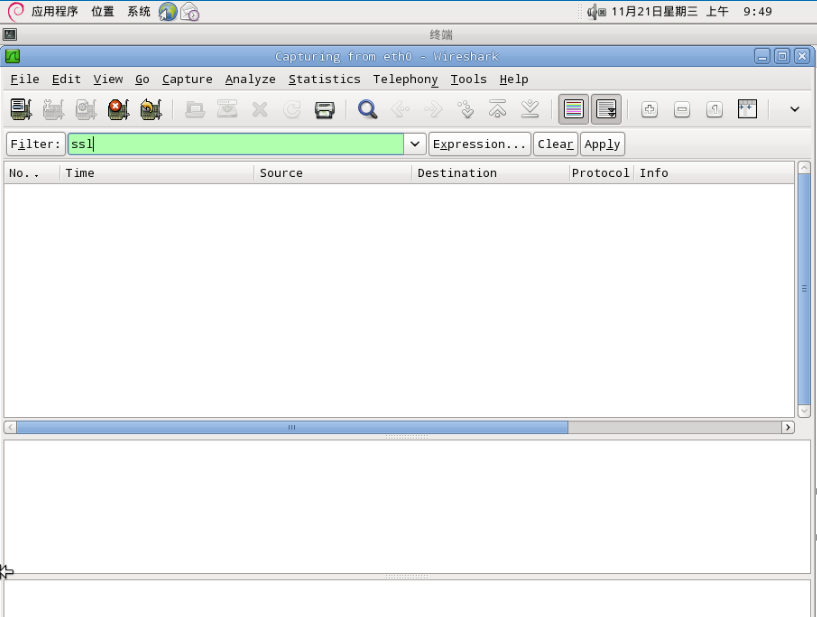


图3.6

1. 在浏览器打开https://200.200.0.114/xampp



图3.7

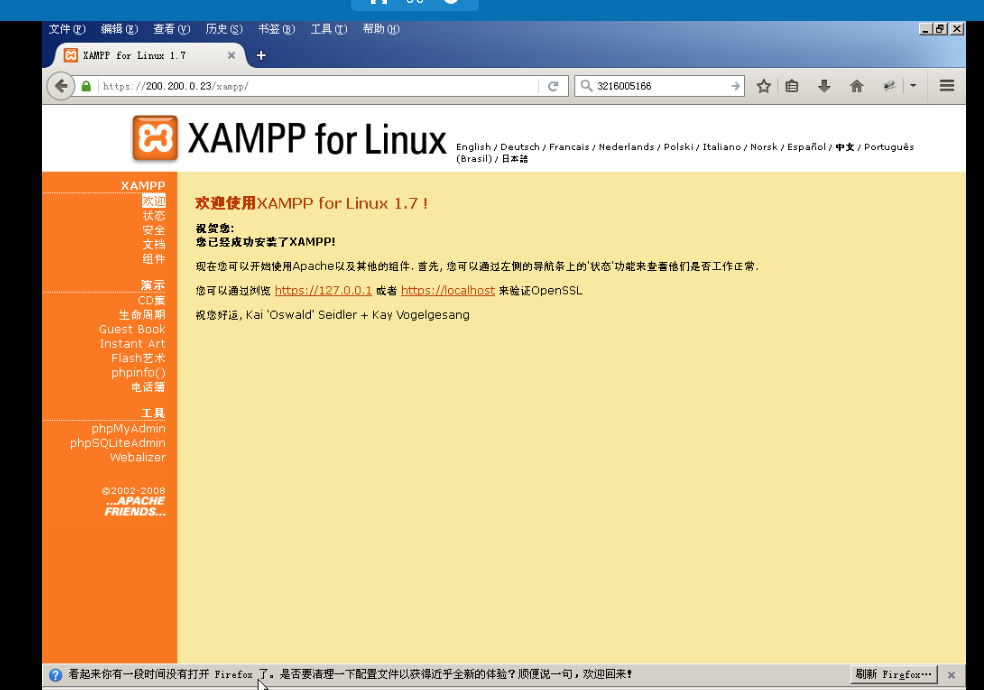


图3.8

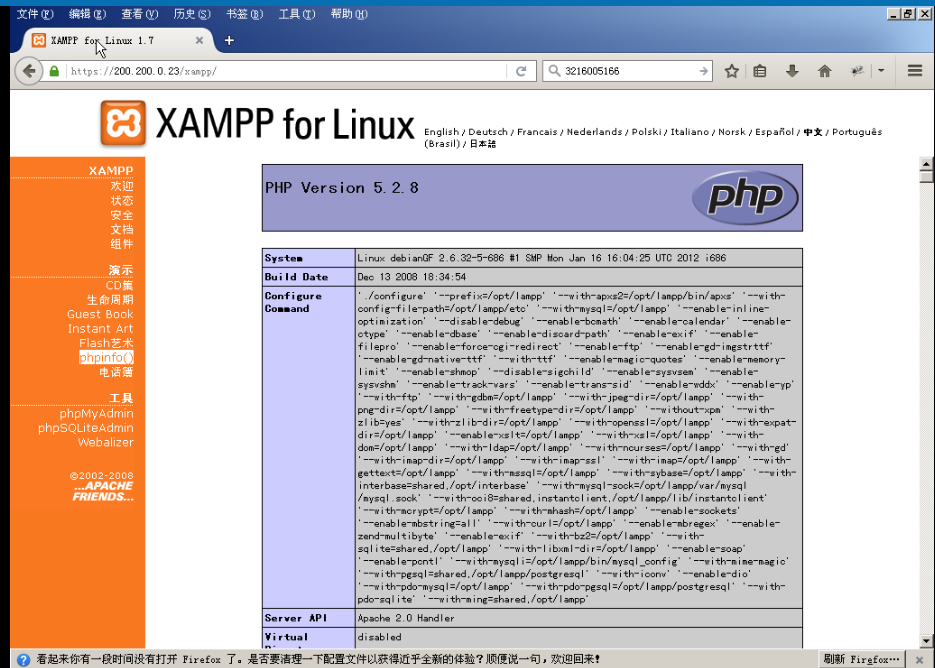


图3.9

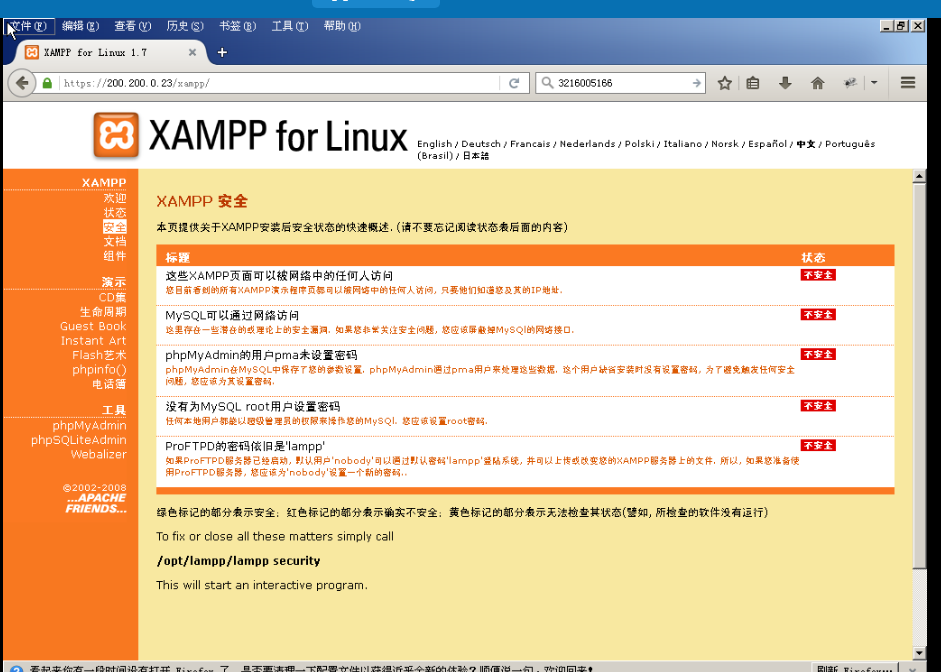


图3.10

1. 回到抓包工具”wireshark”查看结果

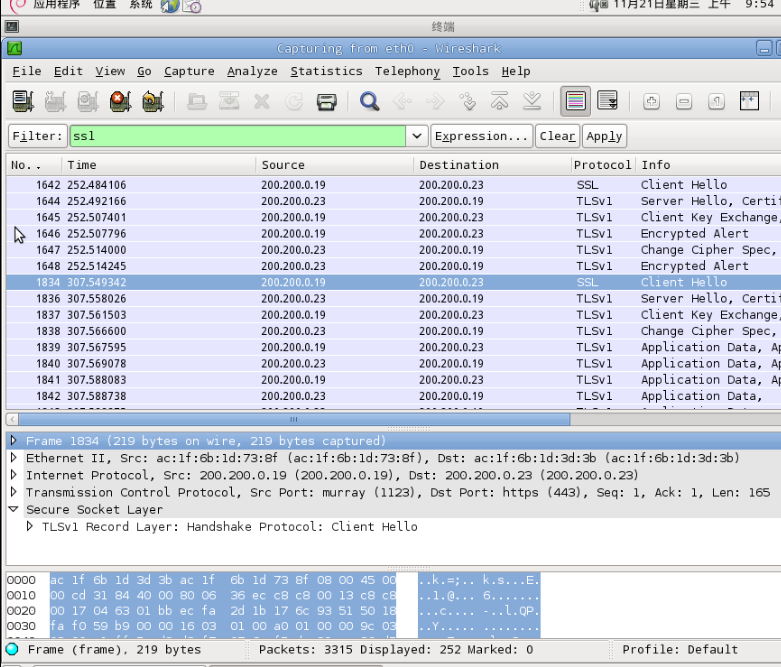


图3.11

* 1. **实验分析与结论**

对比前后两次抓取信息，可以看出没有SSL安全访问的时候，抓到浏览器的信息包是明文的，而设置了SSL安全访问的时候抓到的包是加密的。

* 1. **实验思考题**

1. SSL协议的基本概念是什么？具有哪些主要的特性？

答：SSL协议是Web浏览器与Web服务器之间安全交换信息的协议，提供两个基本的安全服务：鉴别与保密。

特性：保密，鉴别，完整性。

1. SSL协议体系结构有哪几部分组成的？它们之间有哪些联系？

答：SSL协议位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持。SSL协议可分为两层： SSL记录协议：它建立在可靠的传输协议之上，为高层协议提供数据封装、压缩、加密等基本功能的支持；SSL握手协议：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

1. 如何通过apache的SSL模块对数据包进行加密？

答：先生成签名证书，配置Apache Web服务器，调整虚拟主机，强制Apache Web服务器始终使用https。

**广东工业大学**

实验题目 实验四 冰河木马

**一、实验目的**

1. 掌握冰河木马的具体功能
2. 熟悉冰河木马的使用操作
3. 懂得冰河木马的清除方法
4. 理解木马对系统的危害

**二、实验要求**

1. 配置冰河木马的服务端、
2. 连接到目标主机并传送木马，实现对目标主机的攻击
3. 目标主机清除冰河木马

**三、实验原理**

一个完整的特洛伊木马套装程序含了两部分：服务端（服务器部分）和 客户端（控制器部分）。植入对方电脑的是服务端，而黑客正是利用客户端 进入运行了服务端的电脑。运行了木马程序的服务端以后，会产生一个有着 容易迷惑用户的名称的进程，暗中打开端口，向指定地点发送数据（如网络 游戏的密码，即时通信软件密码和用户上网密码等），黑客甚至可以利用这 些打开的端口进入电脑系统。 特洛伊木马程序不能自动操作， 一个特洛伊木马程序是包含或者安装 一个存心不良的程序的，它可能看起来是有用或者有趣的计划（或者至少无 害）对一不怀疑的用户来说，但是实际上有害当它被运行。特洛伊木马不会 自动运行，它是暗含在某些用户感兴趣的文档中，用户下载时附带的。当用 户运行文档程序时，特洛伊木马才会运行，信息或文档才会被破坏和遗失。 特洛伊木马和后门不一样，后门指隐藏在程序中的秘密功能，通常是程序设 计者为了能在日后随意进入系统而设置的。 特洛伊木马不经电脑用户准许就可获得电脑的使用权。程序容量十分轻 小，运行时不会浪费太多资源，因此没有使用杀毒软件是难以发觉的，运行 时很难阻止它的行动，运行后，立刻自动登录在系统引导区，之后每次在 Windows加载时自动运行，或立刻自动变更文件名，甚至隐形，或马上自 动复制到其他文件夹中，运行连用户本身都无法运行的动作。

**四、实验过程及内容**

1. 打开冰河木马客户端

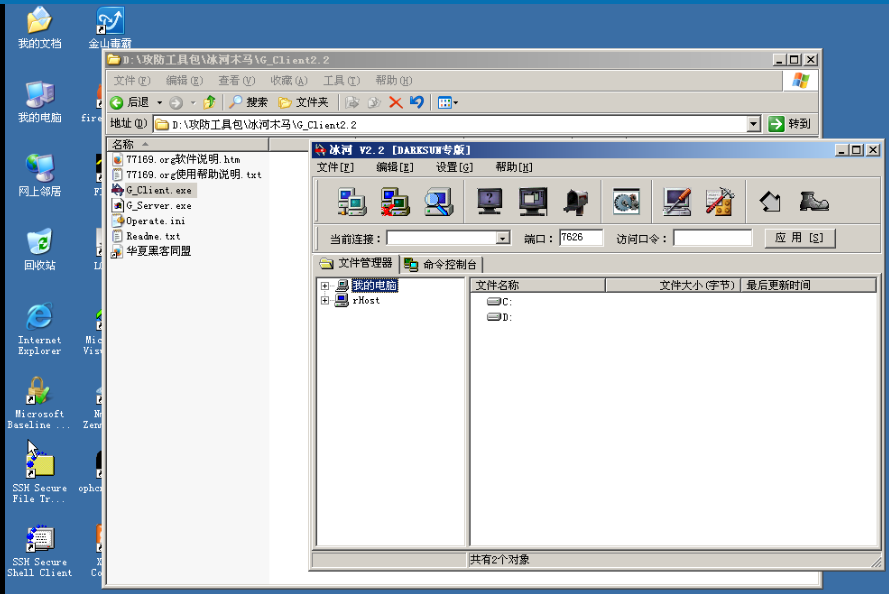


图4.1 打开客户端

1. 配置服务器端，对“基本设置”、“自我保护”、“邮件通知”三个模块设置完毕后点击“确定”。
2. 使用IPC弱口令扫描工具(netscan)扫描目标机(200.200.0.19)，发现目标机存在IPC弱口令，所以IPC共享的方式，把G\_service.exe传送给目标机。



图4.2 扫描IPC

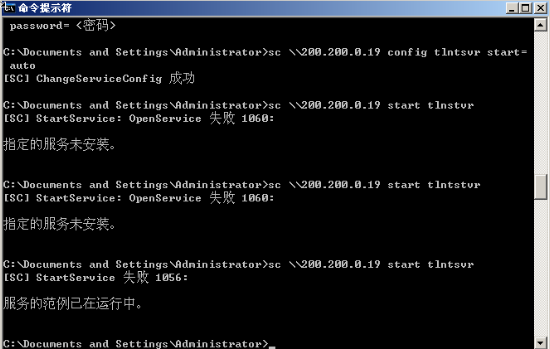


图4.3 建立IPC连接

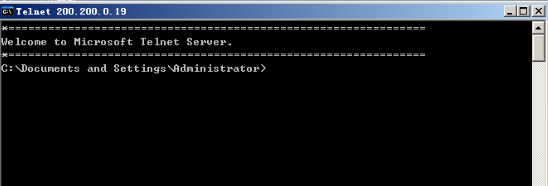


图4.4 连接目标主机

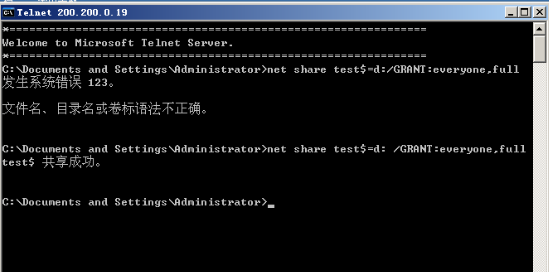


图4.5 共享D盘



图4.6 传送木马

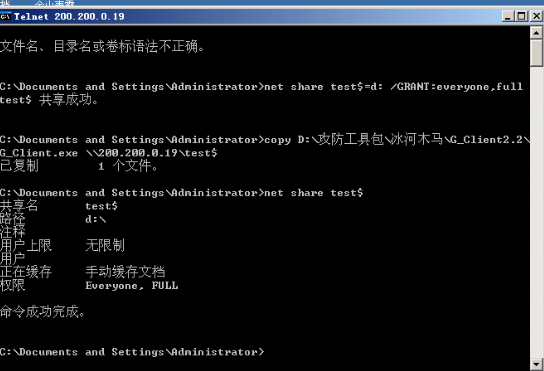


图4.7查看共享路径

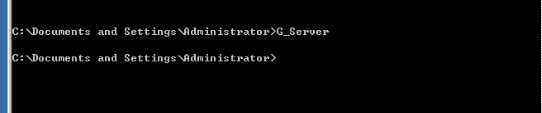


图4.8 激活木马

1. 木马激活后系统没任何反馈，但实际木马已经运行，在进程中可以看到Kernel32.exe。以后Kernel32.exe在系统启动时自动加载运行，即使结束了Kernel32.exe进程，但只要打开TXT文件，sysexolr.exe就会被激活，于是冰河又回来了。

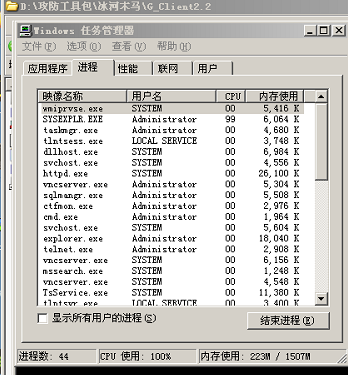


图4.9 查看木马进程

1. 通过木马的客户端的自动搜索功能，搜索某一网段里中并和木马的主机，并且连接到该远程主机。



图4.10 搜索存在木马的网段

1. 连接到远程主机，并且可以实现磁盘管理。

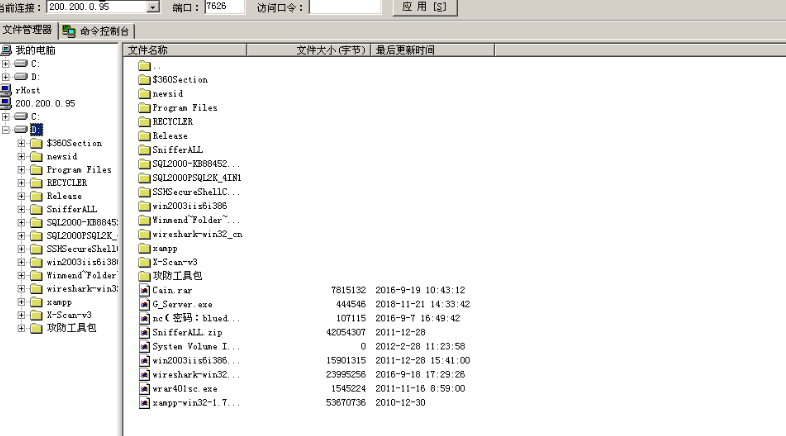


图4.11连接远程主机

1. 该木马具有很高的隐藏性，不像其他安装程序一样可以在系统开始菜 单下的所以程序里看大，或者在控制面板里面看到，只有在进程中可以看 到，即使在进程中杀死Kernel32.exe，但如果打开TXT文件（配置服务时设 置的关联类型文件），木马又会重新被启动（启动后进程的名字是配置服务 端时，关联文件名Sysexplr.exe），所以清除木马办法：

1 删除 C:\Windows\system32(或sysWoW64) 下的 Kernel32.exe 和 Sysexplr.exe 文件。

2 冰河会在注册表 HKEY\_LOCA L\_MACHINE\software\microsof\twindows CurrentVersionRu下扎根，键值为 C:\WINDOWS\system32\KERNEL32.EXE ，删除该项

3 注册表的 HKEY\_LOCA L\_MACHINE\software\microsoft\windows CurrentVersionRunservices 下，还有键值为 C:\windows\system\Kernel32.ex的项 也要删除。

4 最后，修改注册表 HKEY\_CLASSES\_ROOT xtfileshellopencommand 下 的默认值，由中木马后的 C:\windows\system32（或sysWoW64） Sysexplr.exe%1 改为正常情况下的 C:\windows\system32（或sysWoW64） otepad.exe %1 即可恢复 TXT 文件关联

1. 清除木马后木马的客户端将无法连接。

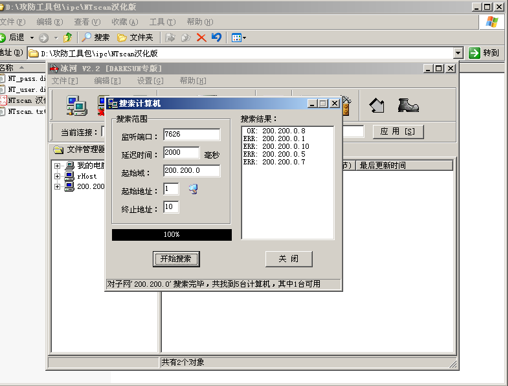


图4.12清除木马结果

**五、实验分析与结论**

通过木马可以实现对目标计算机的信息窃取和远程控制。

**六、实验思考题**

1. 木马的特征是什么？

隐蔽性、自动运行性、欺骗性

1. 木马如何传播？

 网页浏览时利用浏览器漏洞或浏览器插件（Flash，迅雷等）漏洞；通过[QQ](https://www.baidu.com/s?wd=QQ&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)，MSN等即时通讯软件，发送恶意网址链接或[木马病毒](https://www.baidu.com/s?wd=%E6%9C%A8%E9%A9%AC%E7%97%85%E6%AF%92&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)文件；使用U盘等移动存储介质；打开陌生的邮件，通过电子邮件内恶意代码或含[木马病毒](https://www.baidu.com/s?wd=%E6%9C%A8%E9%A9%AC%E7%97%85%E6%AF%92&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)的附件；伪装成多媒体影音文件或植入木马的应用软件，利用P2P平台和网站传播；利用[操作系统](https://www.baidu.com/s?wd=%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)漏洞或弱口令直接远程置入；载来源不明的程序。

1. 该如何防范木马？

安装杀毒软件，定期扫描杀毒，更新补丁；不随意打开不明网页链接，不随意下载安装不明来源的软件