实验一 CA 证书与 SSL 连接

应用场景

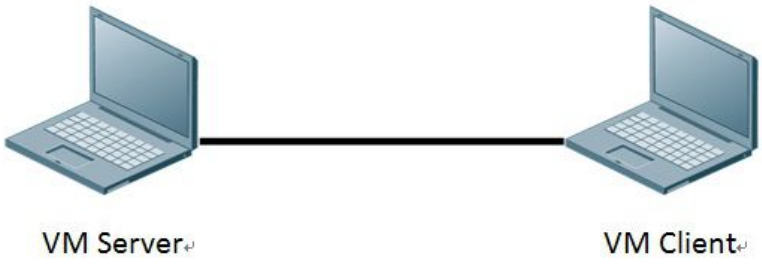
在访问 Web 站点时，如果没有较强的安全措施，用户访问的数据是可以使用网络工具捕获并分析出来的。在 Web 站点的身份验证中，有一种基本身份验证，要求用户访问输入用户名和密码时，是以明文形式发送密码的，蓄意破坏安全性的人可以使用协议分析程序破译出用户名和密码。那我们该如果避免呢？可利用 SSL 通信协议，在 Web 服务器上启用安全通道以实现高安全性。

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（SSL Record Protocol）：它建立在可靠的传输协议（如 TCP）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（SSL Handshake Protocol）：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。每一个 Windows Server 2003 证书颁发机构都有可供用户和管理员使用的网页。

实验目标

- 掌握在 Windows Server 2003 下独立根 CA 的安装和使用。
- 使用 WEB 方式申请证书和安装证书。
- 建立 SSL 网站。
- 分析 SSL 网站的数据包特点。

实验拓扑



实验环境

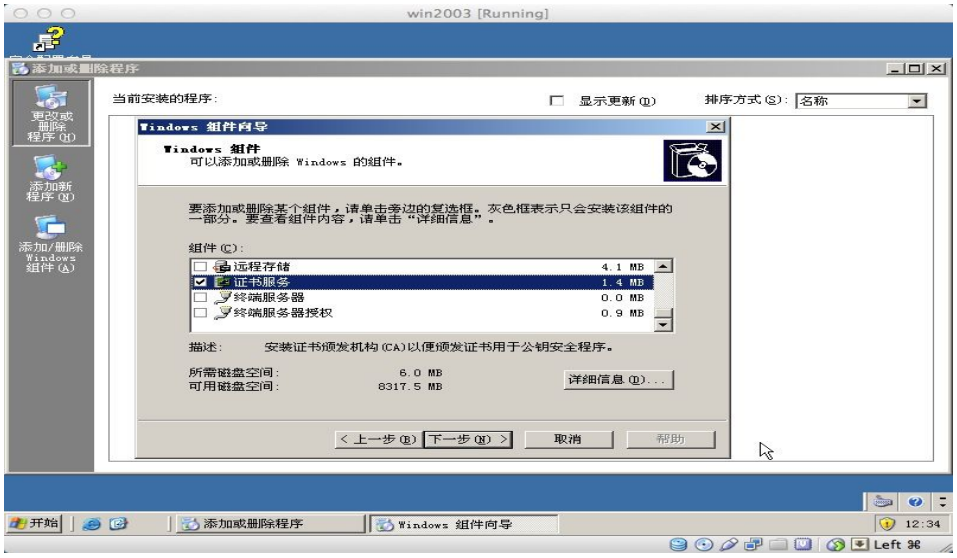
虚拟机：Windows Server 2003，Windows XP，Wireshark 抓包软件。

实验过程指导

任务一：windows server 2003 环境下独立根 CA 的安装及使用

1、启动 Windows Server 2003 和 Windows XP，配置其 IP，使其在同一局域网网段。

2、在 Windows Server 2003 中，选择【开始】|【控制面板】|【添加和删除程序】，在弹出窗口中选择【添加和删除 windows 组件】，在【组件】列表框中选择【证书服务】，再单击【下一步】按钮，如下图所示。



3、在弹出的窗口中选择【独立根 CA】单选按钮，单击【下一步】按钮，在弹出窗口中按要求依次填入 CA 所要求的信息，单击【下一步】按钮，如下图所示。

4、继续选择【证书数据库】、【数据库日志】和配置信息的安装、存放路径，如下图所示，

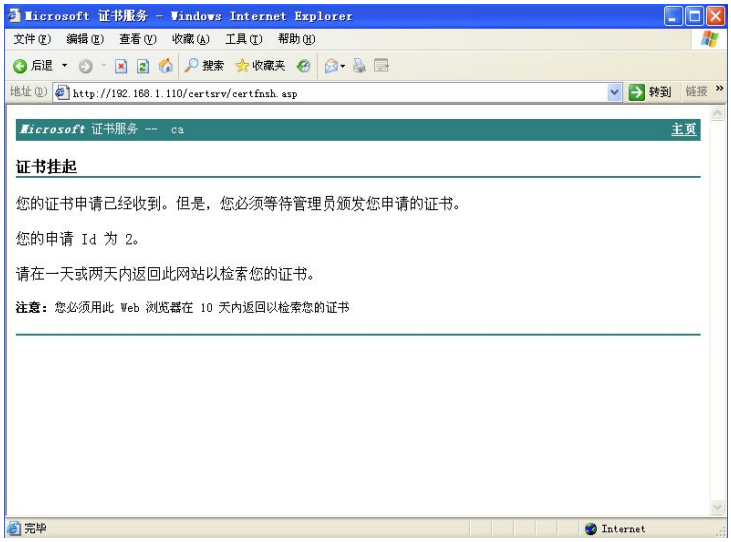
单击【下一步】按钮。安装的时候，可能会弹出如下窗口，为了实验方便，已经把 I386 文件夹复制到 C:\下，选择【浏览】，选择文件夹“C:\I386”，点【确定】，完成安装。

5、选择【开始】|【程序】|【管理工具】，可以找到【证书颁发机构】，说明 CA 的安装已经完成，如下图所示。

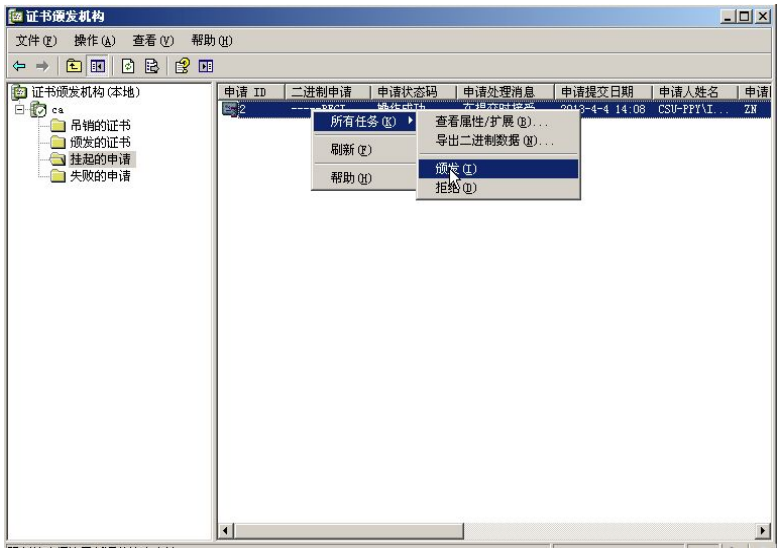
6、从同一局域网中的另外一台 XP 开启 IE 浏览器，输入 http://windows2003 的 IP/certsrv/，选中【申请一个证书】，如下图所示，在弹出的页面中选择【web 浏览器证书】。

7、在弹出窗口中填写用户的身份信息，完成后进行【提交】。此种情况下，IE 浏览器采用默认的加密算法生成公钥对，私钥保存在本地计算机中，公钥和用户身份信息按照标准的格

式发给 CA 服务器，如图所示,单击【是】，进入下一步。CA 服务器响应后，弹出证书申请成功页面，如下图所示。

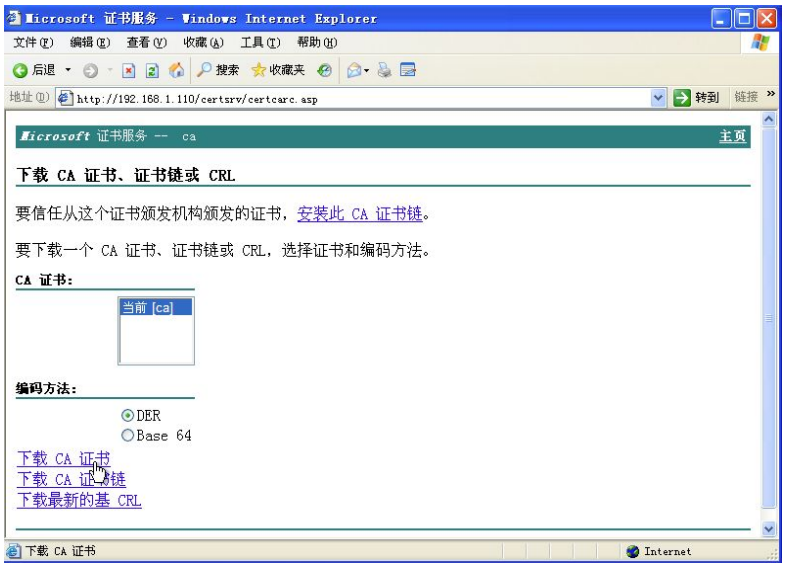


8、在根 CA 所在的计算机上，选择【开始】|【程序】|【管理工具】|【证书颁发机构】，上面申请的证书便会出现在窗口右边，选择证书单击右键，选择【所有任务】|【颁发】，进行证书颁发，如下图所示。证书颁发后将从【挂起的申请】文件夹转入【颁发的证书】文件夹中，表示证书颁发完成。



9、在申请证书的计算机上打开 IE，输入 http://windows2003 的 IP/certsrv/，进入证书申请页面，选择【查看挂起的证书申请状态】，弹出的页面中选择一个已经提交的证书申请，如下图所示。选择安装此证书。

10、现在验证此 CA 系统颁发的新证书是否可信，为此需要安装 CA 系统的根证书，进入证书申请主页面，选择当前的 CA 证书进行下载，并保存到合适路径，如下图所示。

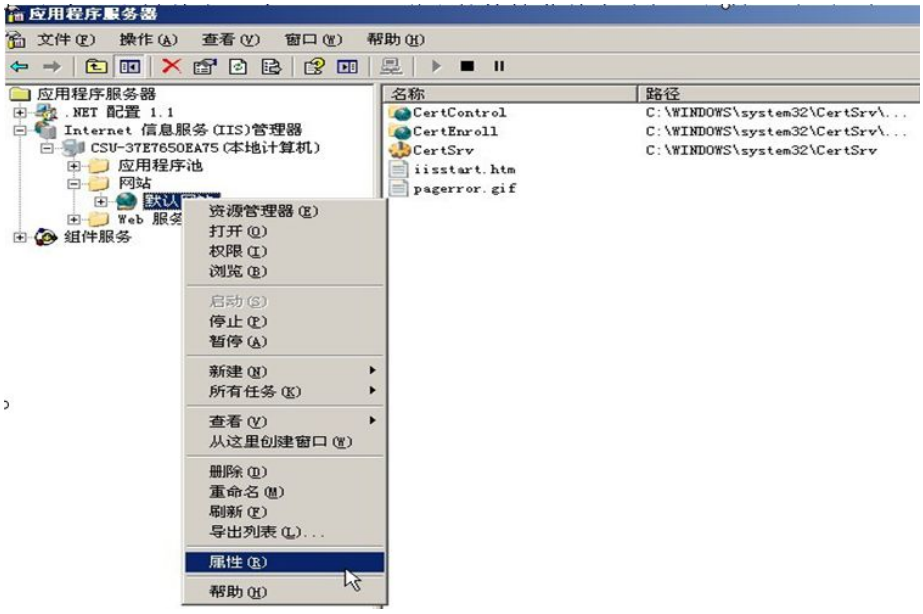


11、下载完毕之后，在证书的保存目录中查看证书信息，单击【安装证书】按钮，进入证书导入向导，按照默认的配置完成证书的导入，导入成功后，单击【确定】按钮，之后完成。

任务二：基于 Web 的 SSL 连接设置

1、在 XP 中，左下角【开始】，打开【Wireshark】，并点击开始抓包的按钮。打开 IE 浏览器，输入网址 http://windows2003 的 IP/?id=1(比如：http://192.168.1.130/?id=1)，然后保存 Wireshark 的抓包结果 1。

2、选择【开始】|【程序】|【管理工具】|【IIS（Internet 信息服务）管理器】，在弹出窗口右键单击【默认网站】，弹出的快捷菜单中选择【属性】选项，如下图所示。



3、在弹出窗口内选择【目录安全性】标签，单击【安全通信】中的【服务器证书】按钮，如下图所示。

4、弹出【IIS 证书向导】窗口，选中【新建证书】复选项，一直单击【下一步】按钮，输入自定义的名称，如下图所示。填写相应的信息后，单击【下一步】按钮。

5、弹出【请求文件摘要】窗口，确认后单击【下一步】按钮，接着单击【完成】按钮，完成服务器端证书配置，如下图所示。

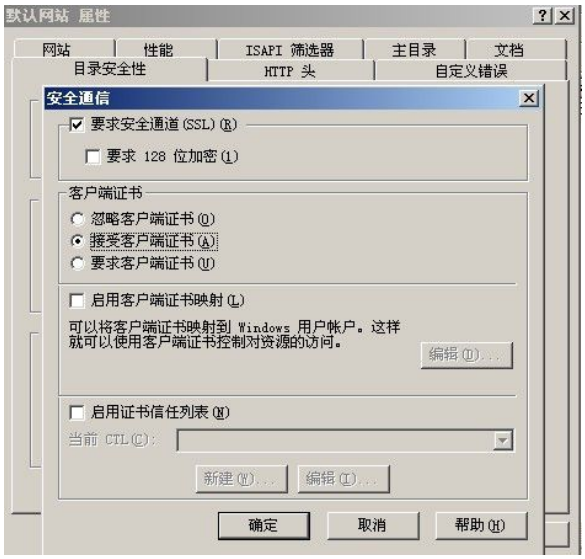
6、打开 IE 浏览器（windows2003 中的），进入证书申请主界面，如下图所示。

7、在出现的网页中选择【高级证书申请】，如图所示，在出现的网页中单击第二个选项【base64 编码】。打开刚才 IIS 证书向导生成的请求文件，（默认路径 C:\certreq.txt），复制并粘贴文件内容到第一个文本框，如下图所示，单击【提交】按钮，转到完成提交后的页面。

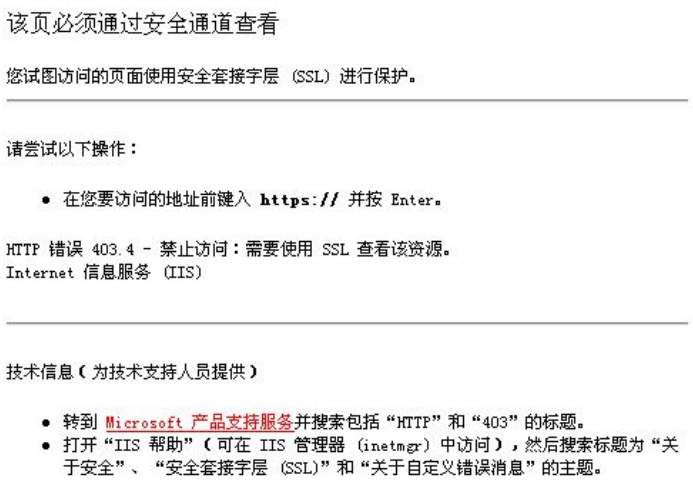
8、回到首页，选择【查看挂起的证书申请状态】，弹出的页面中选择一个已经提交的证书申请，如下图所示。选择【Base 64 编码】，点击【下载证书】，【保存】certnew.cer 文件到桌面。

9、选择【开始】|【程序】|【管理工具】|【IIS（Internet 信息服务）管理器】，在弹出窗口右键单击【默认网站】，弹出的快捷菜单中选择【属性】选项，在弹出窗口内选择【目录安全性】标签，选择【服务器证书】，选择【下一步】，【处理挂起的请求并安装证书】选择【下一步】，【浏览】选择刚才保存的 certnew.cer 文件，如下图所示。【下一步】【下一步】【完成】。

10、还是在【目录安全性】下，选择【安全通信】下的【编辑】，在下如图所示的弹出窗口中选中【要求安全通道（SSL）】复选项，并在【客户端证书】栏中选中【接受客户端证书】复选项，再单击【确定】按钮。返回【目录安全性】面板，单击【应用】按钮及【确定】按钮，完成配置。



11、在 XP 系统打开浏览器，输入服务器 IP 地址，进入证书申请主页面，此时会显示错误信息页面，要求采用 https 的方式连接服务器，如图所示。



12、把 http 改成 https 继续访问，此时浏览器提示你要安装证书，安装完证书后，就可以正常使用了。

13、再次打开 Wireshark，并点击开始抓包的按钮。打开 IE 浏览器，输入网址 https://windows2003 的 IP/?id=1(比如：https://192.168.1.130/?id=1)，然后保存 Wireshark 的抓包结果 2。

14、分析比较抓包结果 1 和抓包结果 2 中，对 IP/?id=1 请求处理的差异。

实验思考

1、查阅相关资料，完成在 Linux 下独立根 CA 的配置及应。

2、对 Wireshark 所抓到的未使用 SSL 连接和使用 SSL 连接的信息，加以对比，看看存在什么差异。

实验报告

1、写出 windows server 2003 下独立根 CA 的配置及应用的过程，将重要的步骤截图并保存。

2、写出 windows server 2003 下基于 Web 的 SSL 连接设置的过程，将重要的步骤截图并保存。

3、回答实验思考中的相关问题。