Nessus 使用说明

1. 硬件需求

一台 linux 机器作为服务器端，一台 Windows 机器作为客户端。
如果 linux 使用比较熟，也可以不使用 windows 作为客户端，直接使用 linux 下的客户端。（此文档暂不对这部分进行说明）

2. NESSUS 的安装

UNIX 系统服务器端需要编译然后才可以使用，推荐使用 linux 作为服务器。

如技术条件允许，推荐先安装最新版本的 NMAP（端口扫描工具）、Hydra（口令破解工具）、Nikto（cgi 漏洞扫描工具），并增添到 PATH$路径里。Nessus 安装的时候会自动识别这些已安装的外部程序，并集成这些程序来增强 Nessus 的功能。此部不是必须。

下面以 Redhat linux AS 3.0 系统安装 Nessus-2.0.10a 为例进行说明。

最近版本的 Nessus 下载地址
http://ftp.nessus.org/nessus/nessus-2.0.10a/
http://ftp.nessus.org/nessus/nessus-2.0.10a/src/为 Nessus 的 4 个源代码包。
http://ftp.nessus.org/nessus/nessus-2.0.10a/nessus-installer/为 Nessus 的自动编译安装脚本。

服务器安装有两种方式，一种需要对 4 个源代码包分别手工进行编译，比较麻烦，推荐使用自动安装脚本。
安装之前要确认机器上安装了 gcc 和 sharutils（需要使用里面的 uudecode），可以从系统安装盘里面找。

成为（su）root 用户或使用 root 用户进行登陆。
下载 http://ftp.nessus.org/nessus/nessus-2.0.10a/nessus-installer/nessus-installer.sh，并运行之（./nessus-installer.sh）；或直接 lynx -source http://install.nessus.org | sh 。

3. 服务器端软件配置

Nessus 安装之后首先需要添加 Nessus 用户，运行
nessus-adduser
会提示几个问题，回答即可，注意认证手段有证书验证和密码验证两种。为了方便推荐选用“PASS”密码验证。规则定义“RULES”可以限制用户的访问的 IP 等，一般置空按“ctrl+d”推出即可。

下一步需要制作服务器端与客户端之间加密通讯的需要的证书。运行
nessus-mkcert
一般全部默认回车即可。

4. 漏洞库插件升级

升级前请确认 IP 及 DNS 配置情况，即保证 Nessus 服务器可以访问外网。运行 nessus-update-plugins
升级漏洞库，注意可能要等一段时间。
如果 Nessus 服务器在内网不能连接外网，也可以手工下载漏洞库然后复制到漏洞库文件夹。此不详述。

5. 运行服务器守护进程

当 Nessus 安装、升级都结束以后，确认自己是 root 用户，运行 nessusd –D。

6. 安装客户端软件

nesuss 服务器端自带了客户端连接软件,如果 linux 上安装了 GTK，则 Nessus-installer.sh 脚本会自

动编译出图形界面的 Nessus 客户端。
推荐的是使用 windows 版的 Nessus 客户端 NessusWX，下载地址
http://Nessuswx.Nessus.org/archive/Nessuswx-1.4.4.zip

运行程序后点击 Communications,Server Name 填入 Nessus 服务器 IP 地址，端口默认 1241 即可。
Encryption 选择默认的 TLSv1。Authentication 选择 Authentication by pass（假设前一步服务端配置的时候选择使用密码认证）Login 和 Password 填入前一步 Nessus 服务端配置的时候增添的用户名和密码。

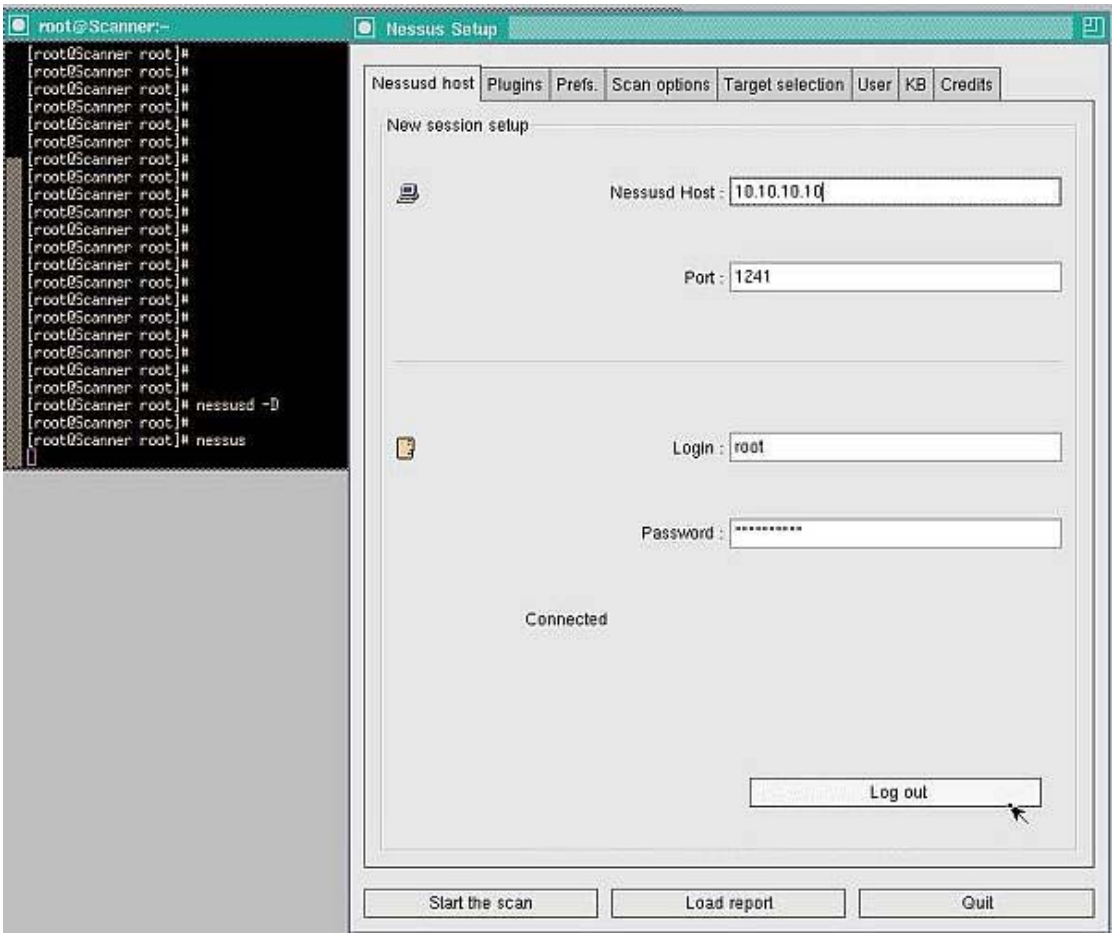

Figure 1: Starting the Nessus server and connecting with the Unix GUI

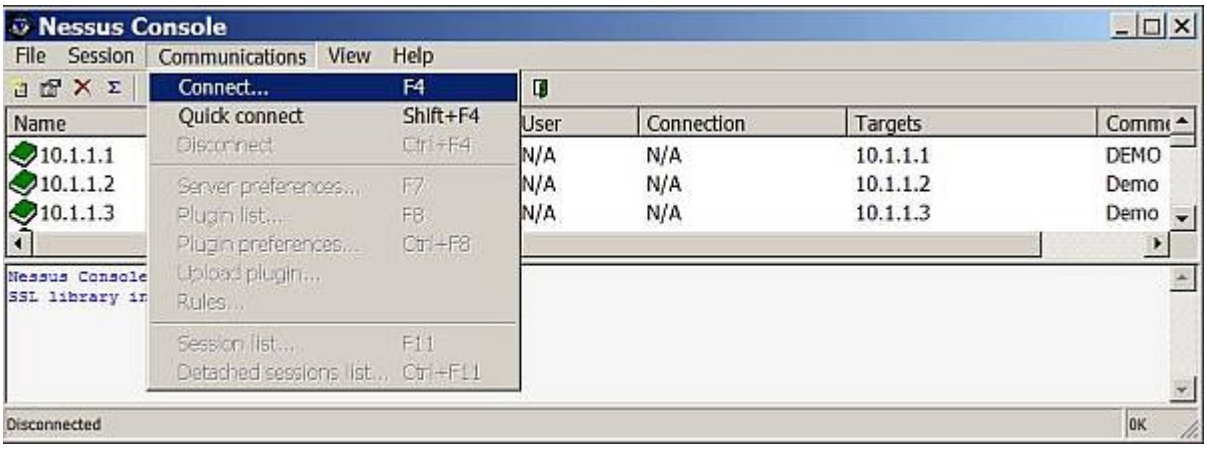

Figure 2: Connecting to the Nessus server with NessusWX (Windows Client)

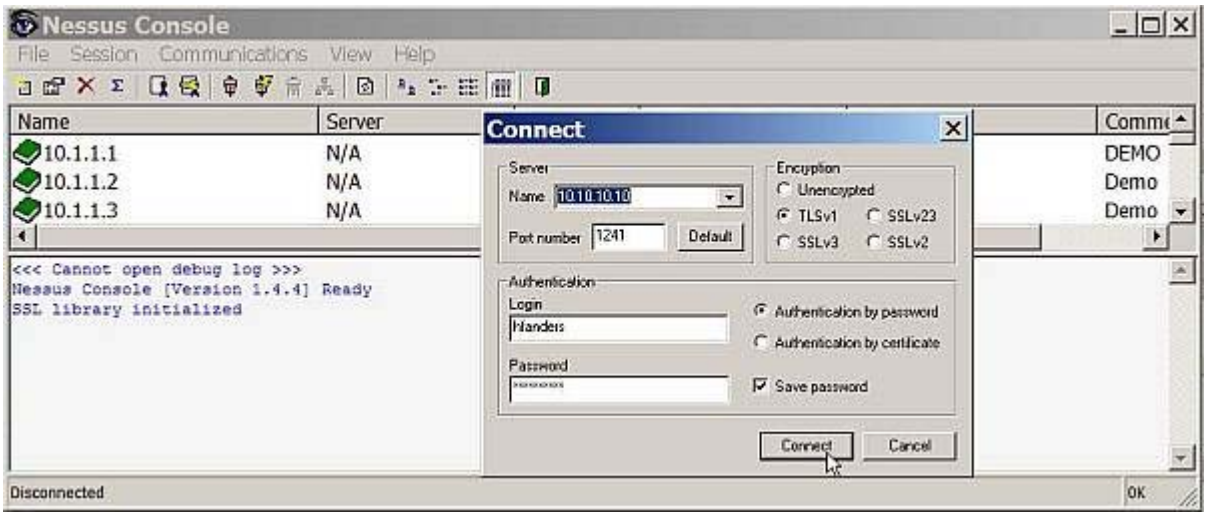

Figure 3: Enter in the server IP and the login and password setup with nessus_adduser

7. 使用 Nessus

7.1. 插件选择（重要）

Nessus 的插件已经有相应的分类，其中包括了部分危险的、拒绝服务类策略。在扫描前一定要对拒绝服务类策略进行去除。比较简单的方法是选择“Enable Non-Dos”。
如果想提高扫描速度或是想针对主机选择使用的插件，也可以单独进行选择。

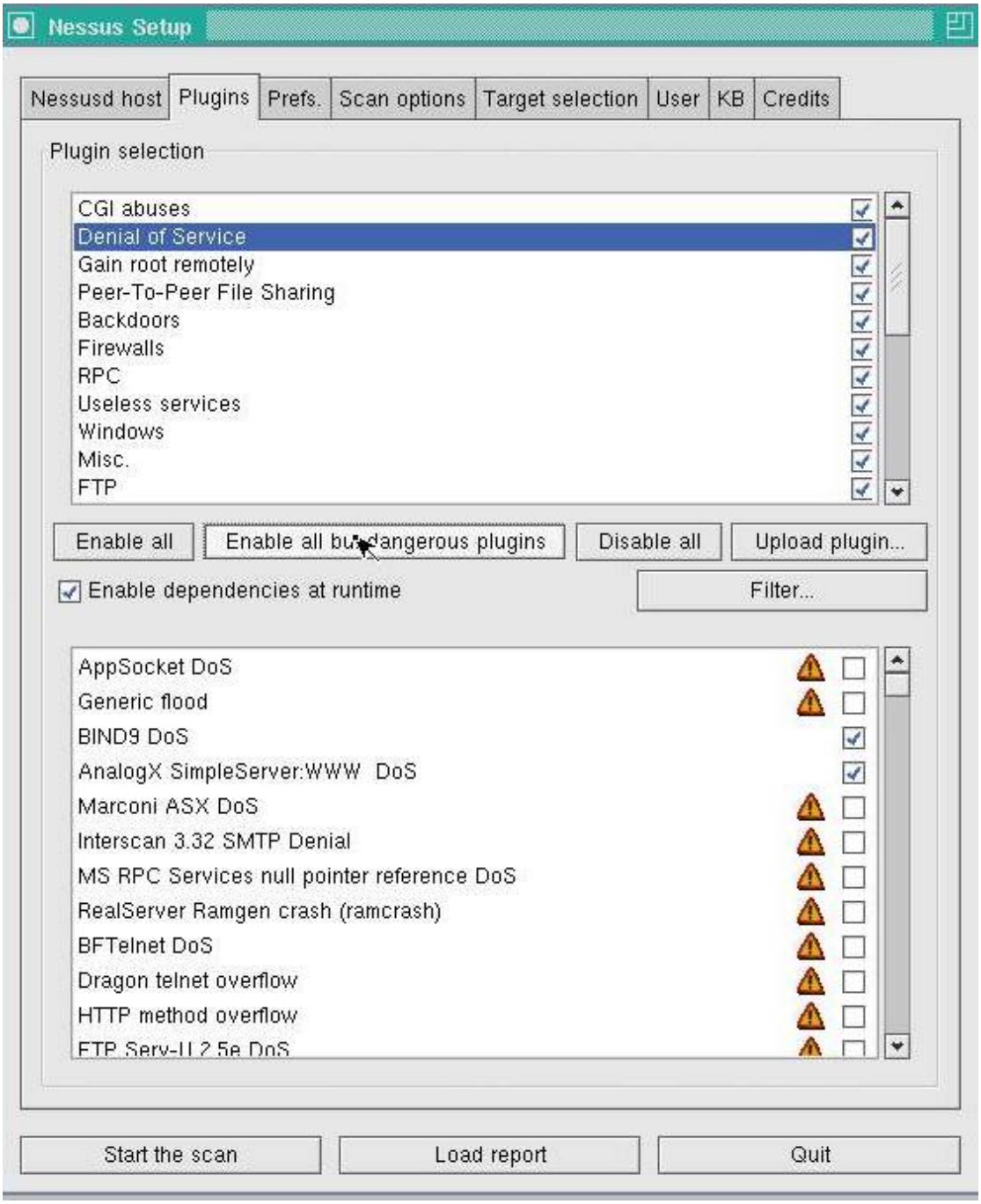

Figure 4: Enabling all but dangerous plugins with the Unix Nessus GUI

Figure 5: Selecting plug-ins with the Windows NessusWX Client

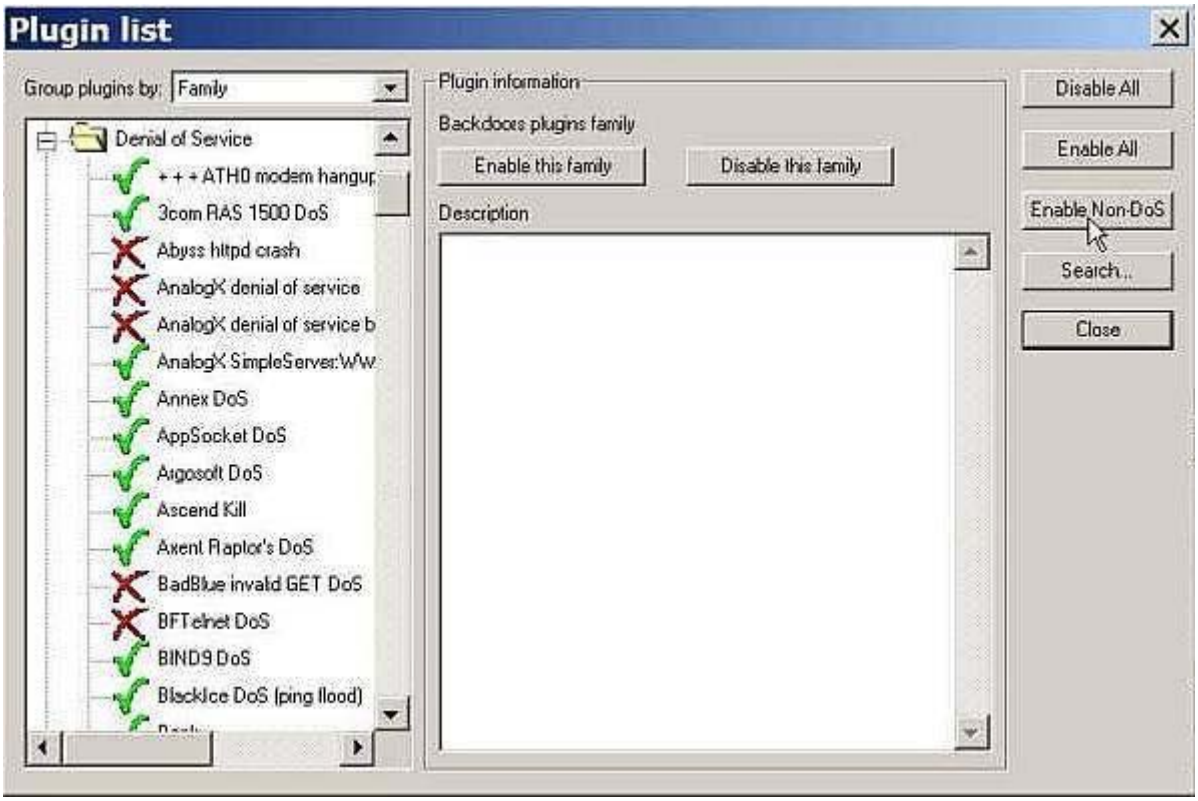

Figure 6: Enabling non-dangerous plug-ins with the Windows NessusWX Client

7.2. 选项部分的配置

最大同时扫描主机数和每主机线程数不能选的太大，目的是尽量减小扫描对网络和主机的影响。推荐同时扫描主机 5 台，每主机扫描线程 10。

主要的扫描选项如下

Enable plugin dependencies ——Nessus 在某个插件所依赖的插件没有激活的情况下不会运行。这个选项会自动激活插件之间的依赖关系。（NASL 脚本间相互是有关联的，比如一个脚本先获取服务的版本，另一个脚本再根据服务版本进行其他检测。如果打乱了脚本的执行顺序可能会影响扫描结果，但也由于脚本间不需要互相等待，会节省扫描时间。）推荐选择。

Do rever DNS lookups —— 做 DNS 反向解析，即由 IP 地址反向解析 DNS 名。

Safe checks —— 禁止掉危险的插件检测，只进行被动的如 banners 中的版本的检测，而不进行真正的溢出攻击。这样可能会造成误报，但是会避免扫描造成的服务器故障。推荐选择。

Optimize the test ——默认情况下，Nessus 在端口服务没有识别的情况下也会运行插件对默认端口进行检测。这个选项会加快测试的速度，但是可能会导致漏报。推荐选择。

Resolve unknown services —— 分析未知服务，对“Well-known services list”列表之外的端口进行服务分析。推荐不选。

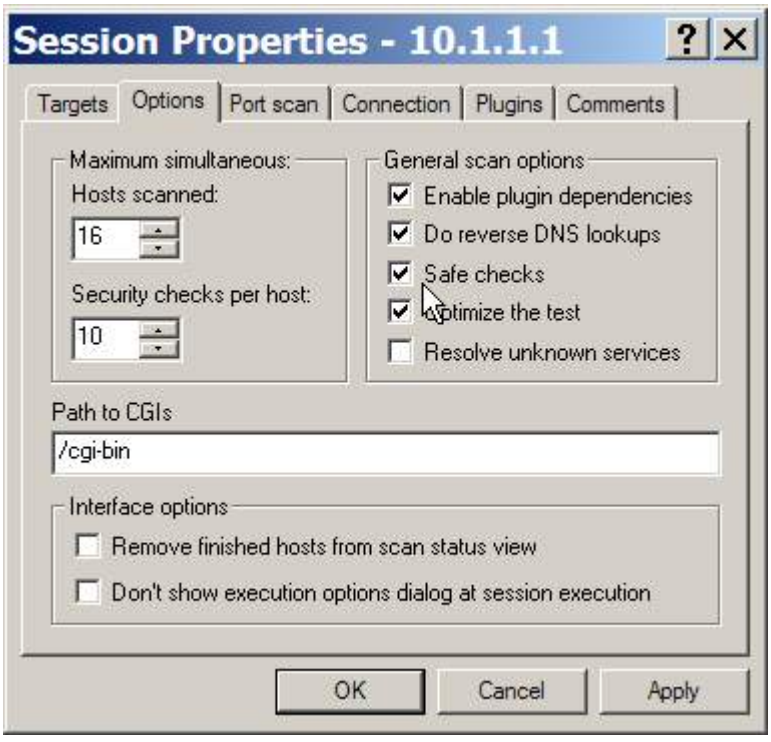

Figure 7: Choosing Safe Checks

7.3. 端口扫描的配置

考虑到扫描的速度，推荐的端口扫描的范围为 1-1024。
如果主机或网络已经过滤了 ICMP，则必须把“Ping the remote host”选项 Disable，否则 PING 不通 Nessus 就不会进行扫描。
另为了保证被扫描主机扫描时的稳定性，推荐把“SYN Scan” Enable。而“tcp connect() scan” Disable。（部分网络设备、主机和应用对大量的端口全连接比较敏感、容易出现问题）。
其他选项一般均可以 Disable。

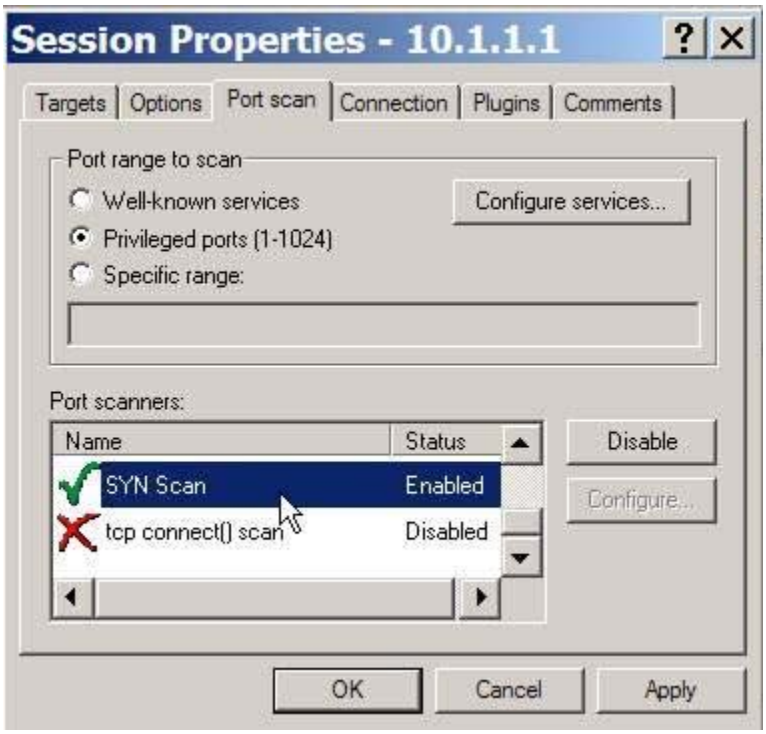

Figure 8: Configuring the internal SYN scan for a simple port scan on NessusWX

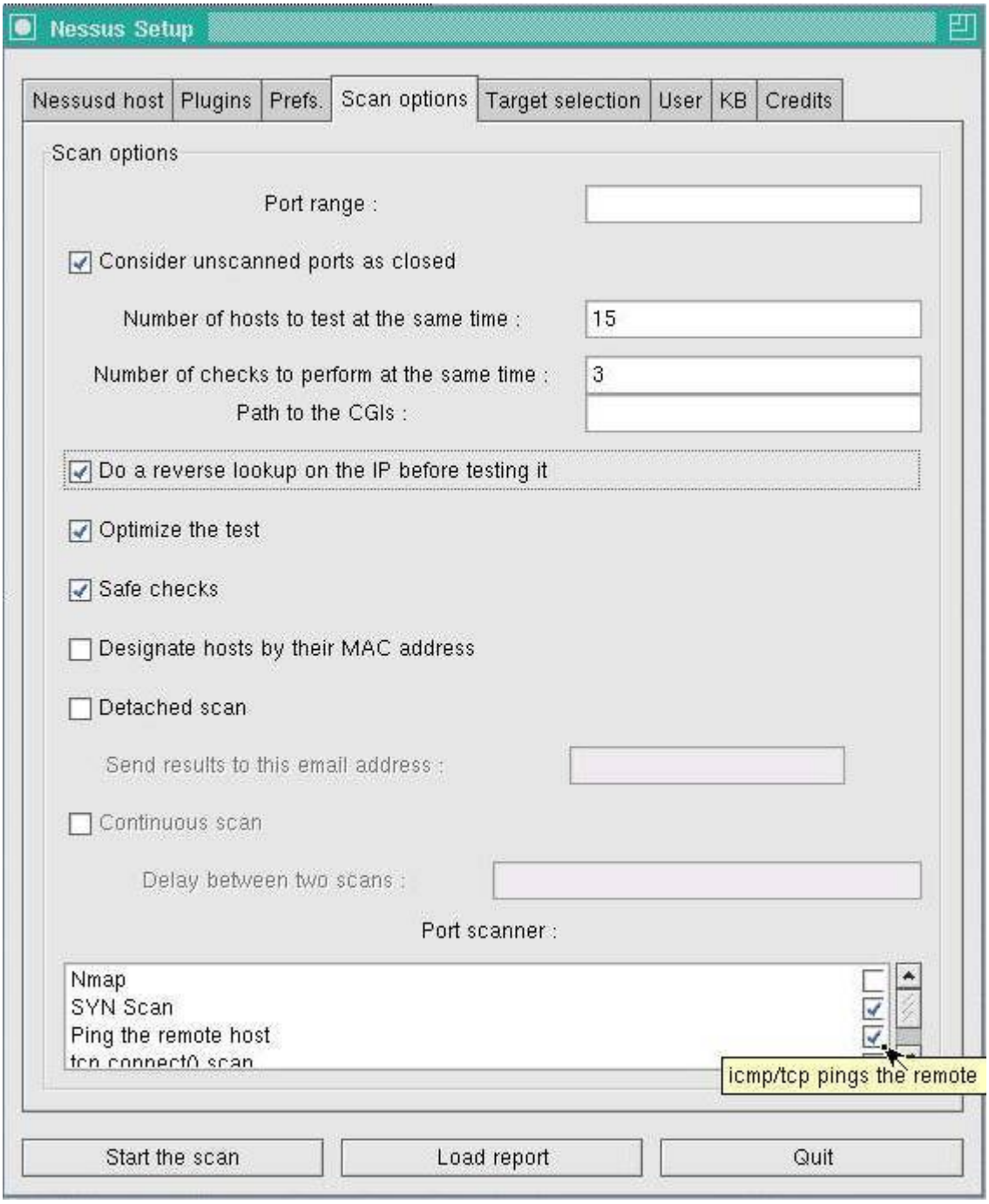

Figure 9: Configuring the internal SYN scan for a simple port scan on the Unix Client

7.4. 扫描对象的输入

扫描对象可以以单个主机/子网/IP 段的形式添加。
另外也支持直接到入文本格式的 IP 列表（Import），推荐使用此种方式，可以直接从 excel 的设备列表中复制到文本，然后导入。
有一个小技巧是导入 IP 列表的时候，最后一行一定加一个空行（回车），不然最后一行会被忽略。

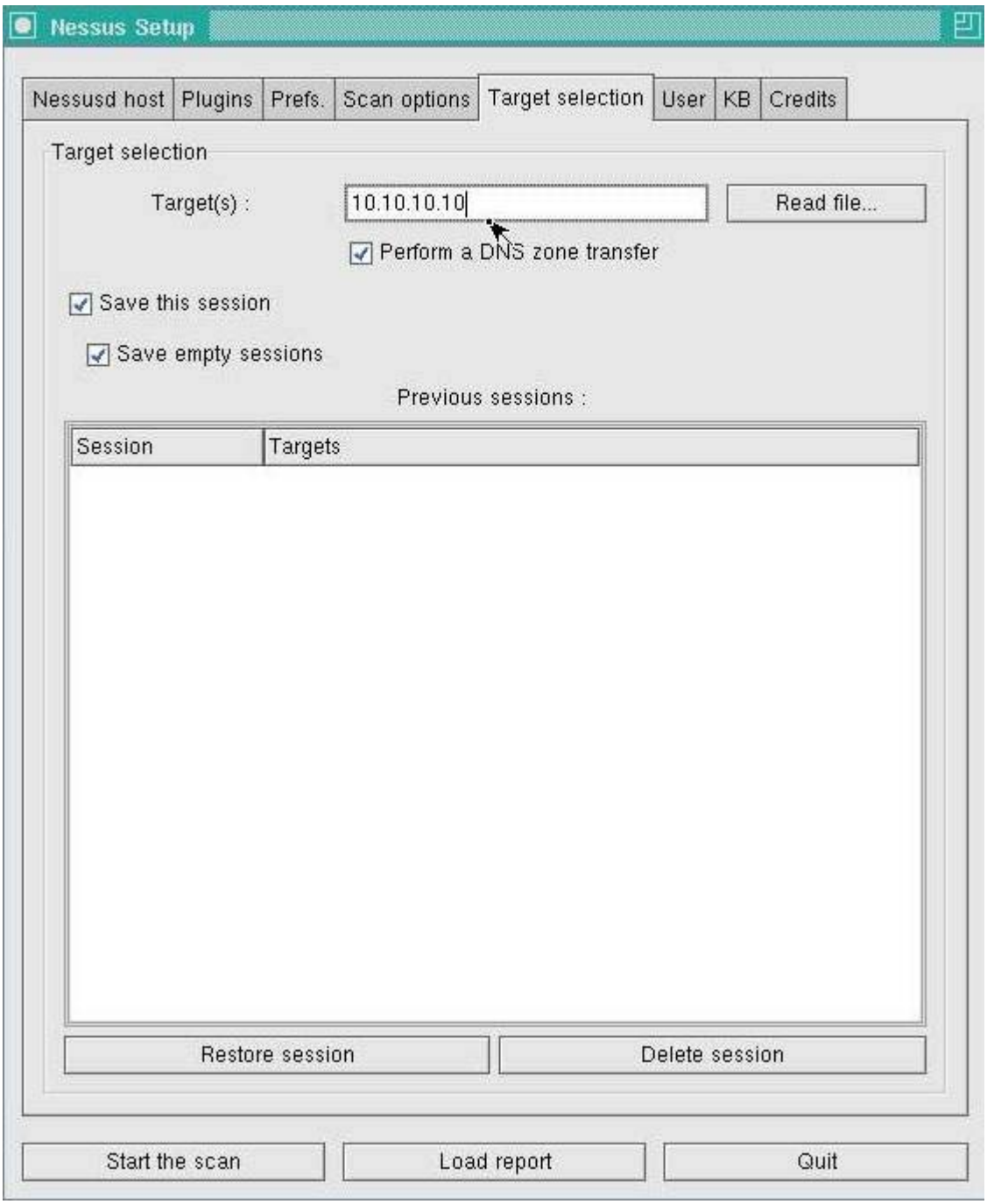

Figure 10: Specifying Targets in the Unix GUI

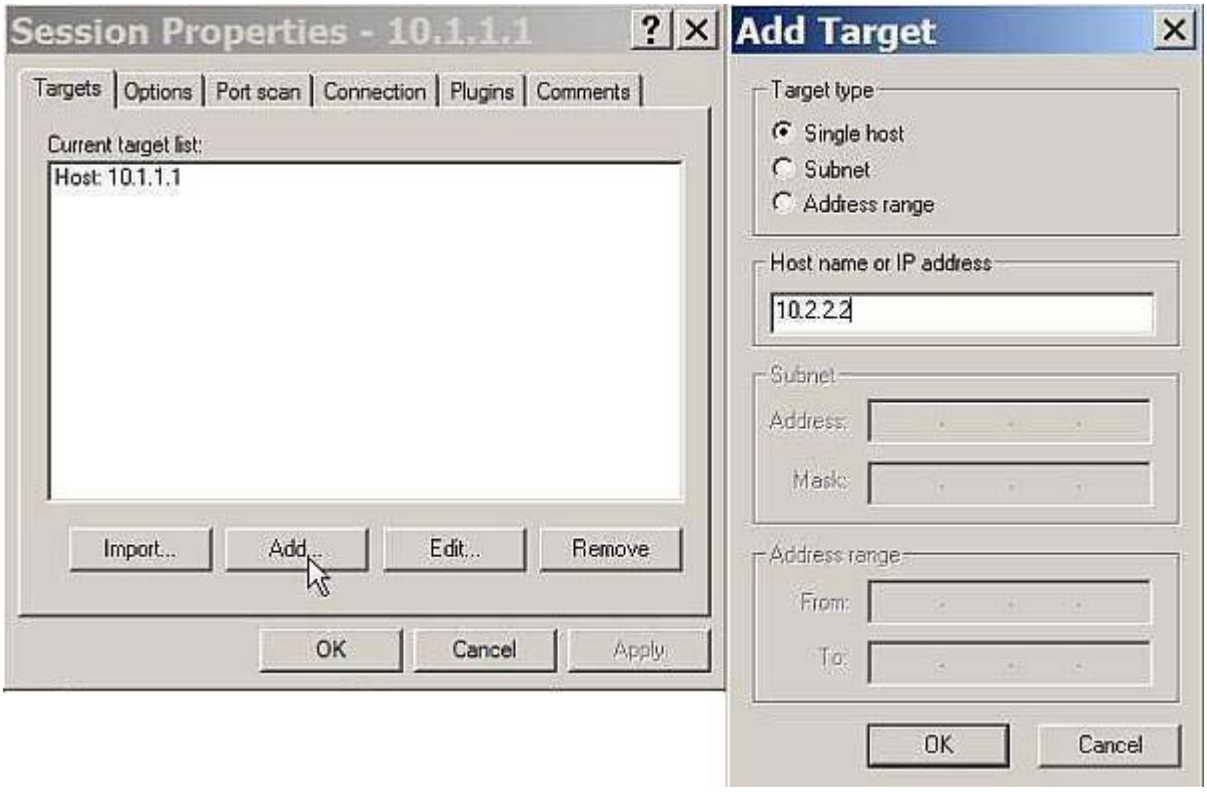

Figure 11: Target Selection in NessusWX

8. 扫描

当扫描选项和扫描对象均配置完毕且确认完毕后（一定要最后确认一下），点击确定。

在主界面双击新建的 Session，或右键点击然后选择 Execute 后会弹出，扫描确认框，其中各项意义如下：

Enable session saving —— 允许保存 session 文件，如果扫描过程中异常退出，可以继续前次的扫描。**（推荐选中）**

Enable KB saving —— 允许保存知识库“*knowledge base，*”可以使插件共享扫描得到的如开放端口、系统类型和其他信息。可以避免重复的扫描行为，节省带宽、时间。**（推荐选中）**

Detached scan —— 分离扫描，允许客户端断开连接在后台进行扫描。此项要求必须选上前面的“Enable KB saving”。这个选项会使客户端不能实时得到扫描进程和结果，“*Continuous scan*”是服务器端进程在扫描结束后重新开始测试。扫描结果可以使用邮件进行发送。“*Delay between scan loops*”定义了重复扫描之间的时间间隔（秒）。**（此项不推荐）**

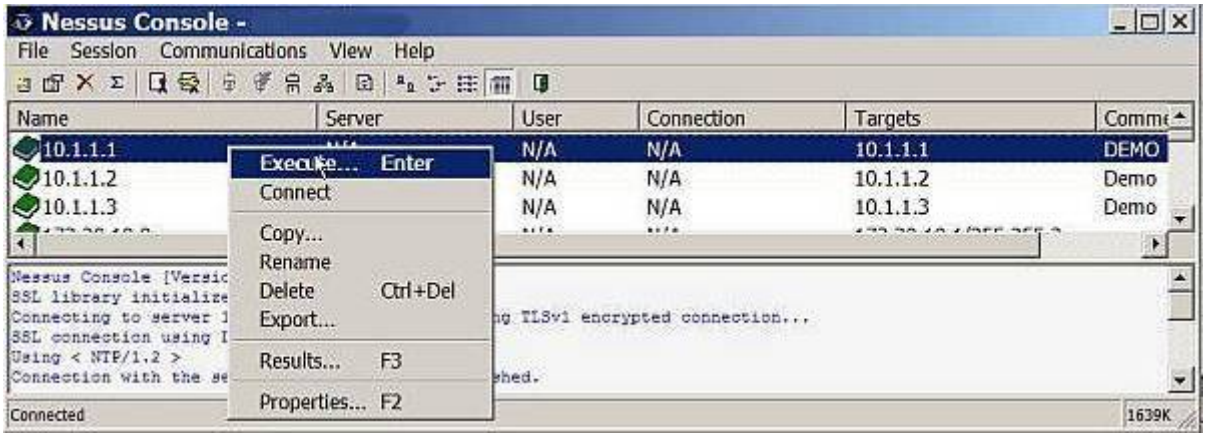

Figure 12: Starting a scan in NessusWX

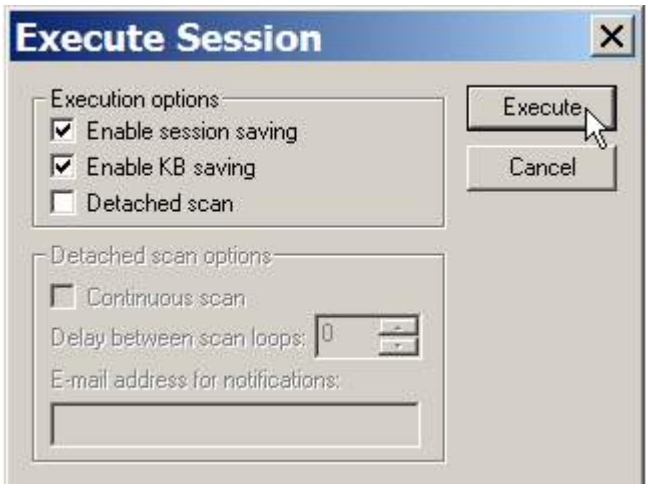

Figure 13: Starting a scan in NessusWX

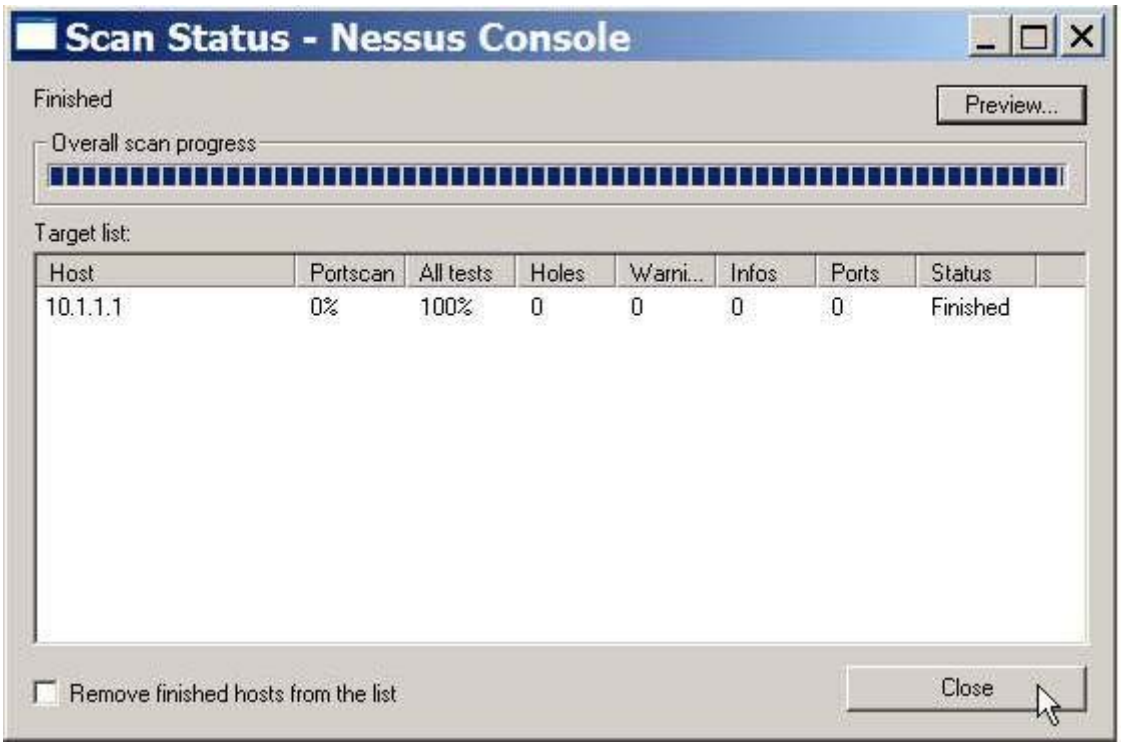

Figure 14: NessusWX scan in Progress

扫描状态栏中会显示扫描的进度，以及发现的漏洞和信息，以及每个主机检测的状态。并可以在扫描未完成进行预览“Preview”。
扫描中可以在此窗口对每个扫描的主机的扫描进行删除停止等操作。

9. 结果的查看和导出

扫描后的结果可以直接点 View 进行查看，并可以对某些误报的进行标记。

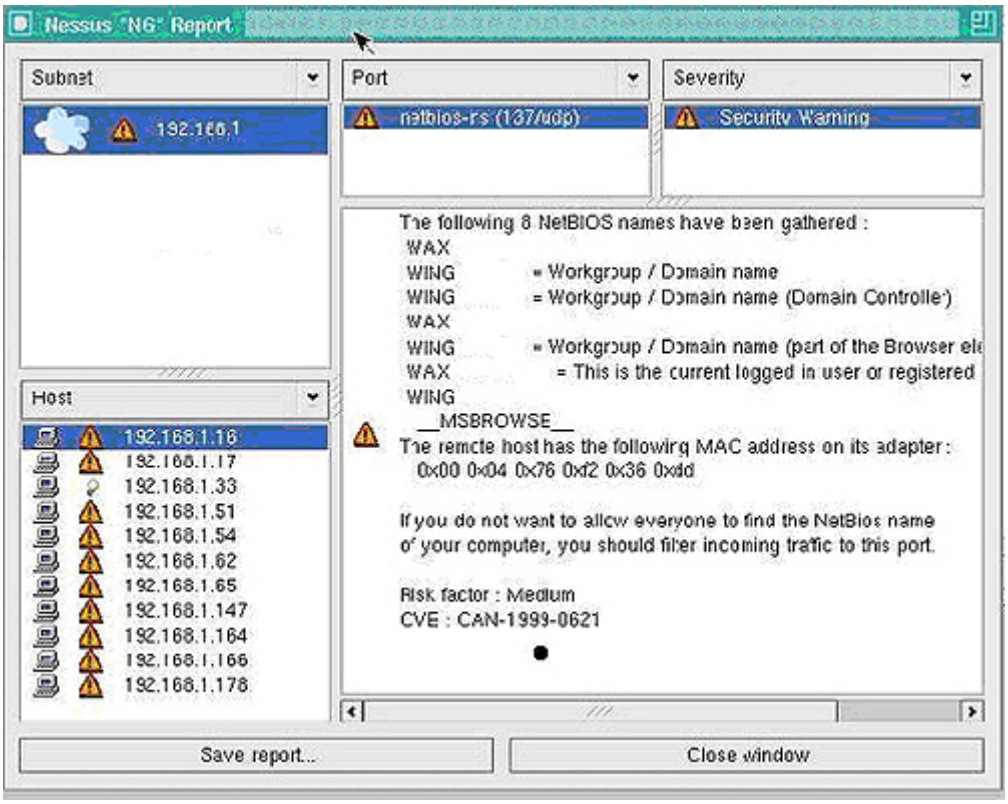

Figure 15: Results are automatically displayed in Nessus GUI.

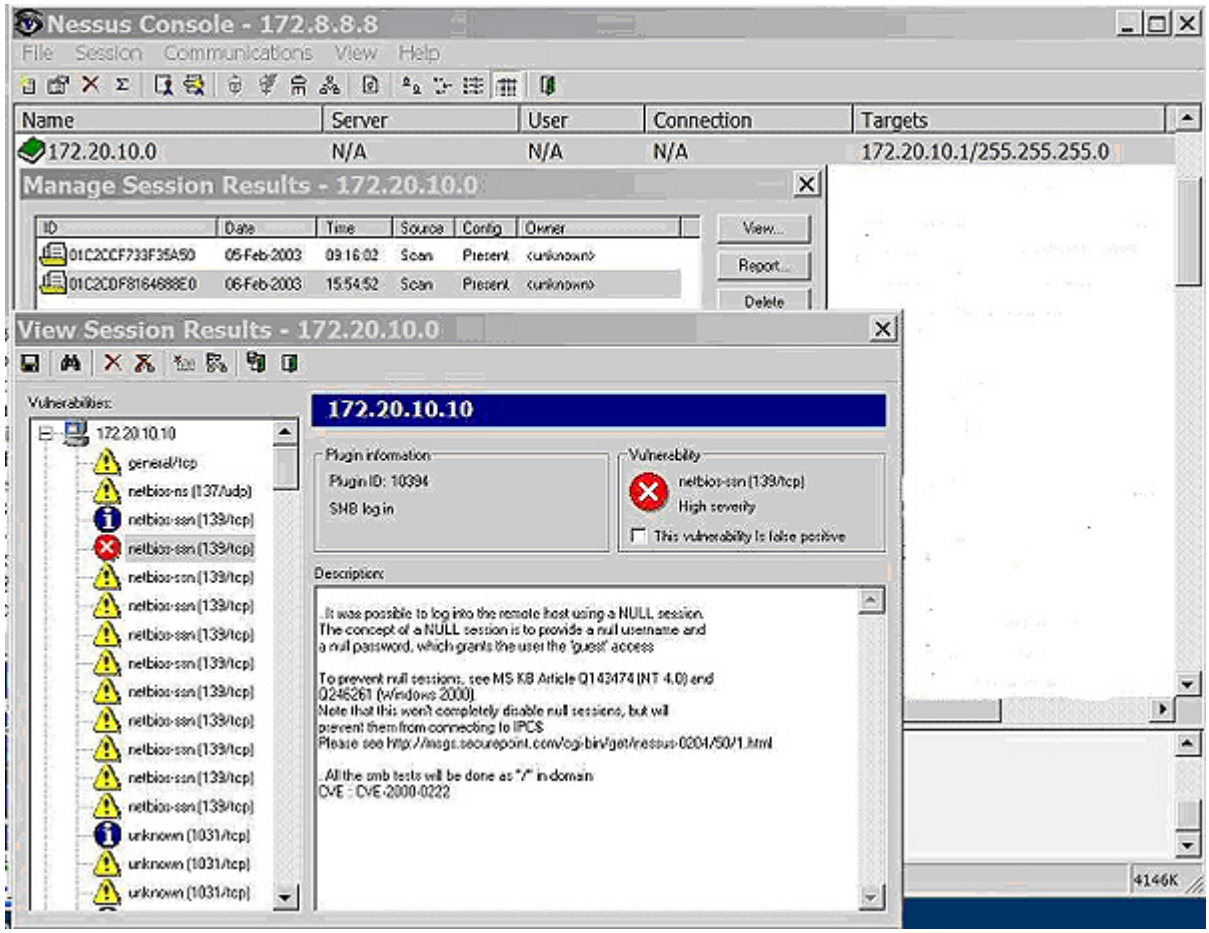

Figure16: Viewing results in NessusWX.

并可以把扫描结果到出为 PDF、Html、CSV 等多种格式。
这里我们选择导出为 CSV 格式（以逗号分隔的数据格式），以方便后期入库分析。

10. 如何降低 Nessus 扫描的风险

如果你的系统比较脆弱，为了尽量减少扫描造成的问题，可以采取如下措施：

10.1. 不进行端口扫描

不使用网络方式扫描端口开放情况，方法如下（不推荐）

- 登陆到系统“guinea-pig”，运行"netstat -a -n --inet"，或是其他命令得到开放 IP 端口（--inet）的数字形式的输出（-n）。
- 将结果至一个文件“guinea-pig”（文件名必须于被扫描的主机名一致）。
- 转换为 nmap 文件格式

netstat2nmap guinea-pig > gp.nmap
（nessus-tools/contrib/netstat2nmap.pl）

- 端口扫描部分只选择“nmap”扫描器，并且在其配置里将“gp.nmap”设置为其结果文件。

或是 SYN 和 TCP Connect()扫描都不选，直接由插件检测。

10.2. 其他选项

选择“safe checks”选项
选择“optimize the test”
不选择“enable dependencies at run time”
删除其他无用的或是危险的插件（plugins）
不选择“Resolve unknown services”
“Plugins”插件配置，服务（Services）“Test SSL based services”选项选择 Known SSL ports 或 None。

10.3. 残余风险

在不选择 SSL 连接尝试后，识别服务仍然比端口扫描更可能造成问题。
一些收集信息插件可能会造成影响，“optimize the test”选项一定程度上降低这种风险。