是如何汇报它们的扫描结果的，即使得出你的网络只有低的安全问题，你也不应该沾沾自喜。一名优秀的黑客可以从很小的缺陷入手给系统造成致命的破坏。

Symantec NetRecon

如图 3-19 所示，NetRecon 是最先为 Windows NT 网络设计的网络扫描产品之一。NetRecon 像其他扫描程序一样可以发现网络中的各种元素，处理本单元中讨论的各种问题，包括密码检查。NetRecon 可以比较准确地模拟各种攻击，NetRecon 的界面由 3 个窗格组成。对象窗口允许你查看每个扫描对象，通过单击可以展开目录结构。通过扫描网络，图形窗口显示低、中、高的风险等级。状态栏显示扫描的进程，你可以对网络进行深度扫描，当然这种扫描会耗费大量的时间。例如，广泛的扫描会花费两天的时间。

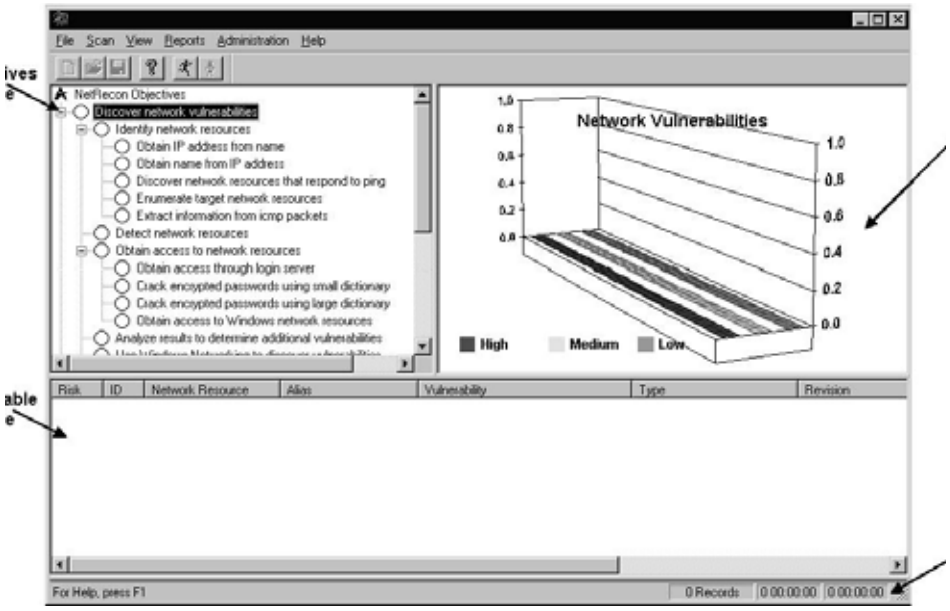

图 3-19 NetRecon 的界面

漏洞数据库和对象列表

在 NetRecon 中以一些漏洞列表作为侦查数据库，可以将该列表理解为攻击指纹，但是该名词通常被用于入侵检测系统程序中。如果你持有 NetRecon 的授权，便可以从 symantec 的 Web 站点(http://www.symantec.com)升级这个漏洞列表,通过 Reports view Vulnerability Descriptions 菜单，可以查看相关漏洞的描述。

下面列出 NetRecon 扫描出的系统漏洞：

- Finger 服务漏洞

- Game Over(远程管理访问攻击)
- 未授权注销禁止
- 服务漏洞，包括 SMTP、DNS、FTP、HTTP、SOCKS 代理和低的 send mail 补丁等级。

大多数网络扫描程序，如 NetRecon，包含了事先定义好的对象列表。通过选择 Reports、View Objective Descriptions，可以查看在 NetRecon 中已经配置好的当前对象列表。

Network Associates CyberCop Scanner

CyberCop Scanner 是 Network Associates 的产品，该公司的产品还包括 SnifferBasic(前身是 NetXRay)和其他网络管理软件，像 NetRecon 一样，CyberCop Scanner 是一个主机级别的审核程序。与 Axent 的产品一样，CyberCop 也把各种漏洞分类为低、中、高 3 个等级。

CyberCop scannes 不是网络扫描程序，它是入侵监测系统程序，能够对黑客活动进行监视，提供报警功能，还能惩罚黑客。你将在本教程中学习一些入侵检测系统程序。

实验 3-7：部署 eEye Retina

在本实验中，我们将学习在 Windows 2000 里安装 eEye Retina，然后对教室里的主机进行扫描。具体操作如下：

1. 从教师处获得 eEye Retina。
2. 从 C:\Lab Files\Lesson 2\eEye Retina folder 获得 eEye Retina。
3. 双击安装文件（**retinademo.exe**），按照安装向导进行安装。
4. 通过**开始|程序|Retina Retina** 打开应用程序。
5. Retina 的主界面会出现在屏幕上。
6. 打开 **File Save**，在根目录下用你的名字保存当前会话。
7. 打开 **Edit|IP Range**，输入所在网络的 IP，单击 **add**。
8. 单击 **Scanner** 图标。任务栏会显示 **Scanner**。现在，单击 **Start** 按钮，开始扫描。

9. 扫描结束时，屏幕会很突出地显示类似于图 3-20 的报告。

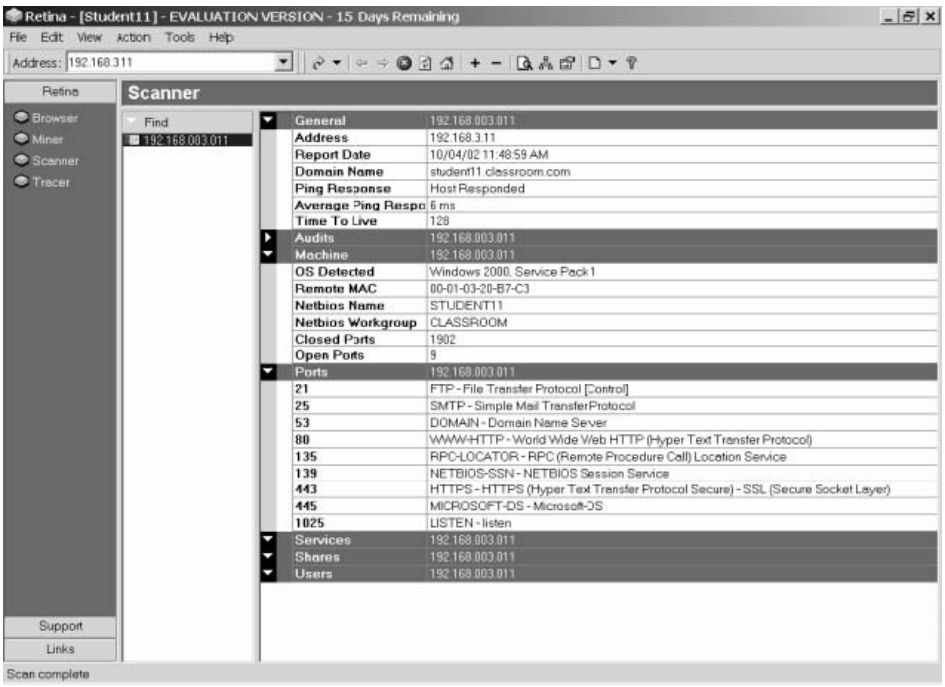

图 3-20 查看 Retina 扫描结果

10. 一般的，Retina 会报告第一个被扫描的系统。单击图标查看脆弱性报告，它们是以 IP 地址进行排列的，你可以查看详细各台主机的脆弱性报告。Retina 会给你提供远程主机的一般信息，还会提供给你系统的脆弱性，就像一份详细的审核报告。你也可以查看远程主机开放的端口和提供的服务。当你查看完第一台主机后，单击左面板上的下一个 IP 地址就可以继续查看，你能查看 Retina 所有能发现的系统。

11. 如果可能，让你的搭档启动到 Linux 并重新启动你的 Retina，对你搭档的系统进行扫描。对比一下从一个操作系统到另一个操作系统，它的脆弱性是如何变化的。

12. 打开 **Tools Polices** 并选择 **Force Scan**，Retina 将会对你搭档的计算机进行暴力破解。对你搭档的计算机重新进行扫描看看 Retina 能侦测到什么。

13. Retina 的 **Miner** 特点允许你扫描 Web 服务器的脆弱性。

14. 最后，使用 Retina 的 **Tracer** 特点，在你和远程主机之间实施 traceroute。它的浏览特点类似于 Web 浏览器，更像 IE 浏览器。