ET Distribution Firewall

Acceptance Test

测试者：张智卓

文档编写者：张智卓

测试时间：2005 年 11 月

基本功能测试

主程序--服务端：

ID	动作	期待的结果	通过 / 失败
2.1	双击快捷方式	是否出现登陆界面？	通过
2.2	选择系统管理员并输入管理员名称和密码，点击进入	是否可以检查管理员密码？	通过
		是否可以进入管理员界面？	通过
2.3	选择“管理”菜单下的管理在线用户	是否出现在线用户列表？	通过
2.4	点击“添加”按钮	是否出现添加黑名单对话框？	通过
2.5	填入黑名单资料，点击确定	是否正确添加黑名单资料？	通过
		是否可以检查黑名单资料各项的输入是否符合规范？	通过
2.6	选择列表中一项，点击“修改”按钮	是否出现修改对话框？	通过
2.7	修改某些资料，点击确定	是否可以保存修改结果？	通过
		是否检查资料各项的输入规范？	通过
2.8	选择列表中一项，点击“删除”按钮	是否正确删除资料？	通过
2.9	选择“管理”菜单下的“报警参数设置”	是否出现参数设置对话框？	通过
2.10	选择“添加管理员”	否正确添加管理员资料？	通过
2.11	设置报警时间，并点击确定	结果是否正确保存并起作用？	通过
2.12	选择“电子邮件报警”，点击“管理联系人”	是否会出现联系人列表？	通过
2.13	选择列表中的一项，点击添加按钮	右边是否会出现添加了的联系人的资料？	通过
2.14	选择一个联系人，填写报	是否可以发送邮件到该联系人信	通过

	警内容，点击“测试”按钮	箱中？	
	选择“短信报警”，点击“管理联系人”	是否会出现联系人列表？	通过
	选择列表中的一项，点击添加按钮	右边是否会出现添加了的联系人的资料？	通过
	选择联系人，点击“测试”	是否可以将短信发到该联系人手机上？	通过
	同时选择多个联系人，点击“测试”	是否可以将短信发给多个联系人？	通过
	选择“.NET Alert”，填入参数，点击“预览”	是否可以看到预览消息？	通过
	选择“管理”菜单里的“传感器管理”	是否出现传感器管理对话框？	通过
	点击“添加”按钮	是否能够显示添加传感器对话框？	通过
	填入传感器参数，点击确定	是否正确保存传感器参数？	通过
	选择列表中的一项，点击“修改”按钮	是否出现修改传感器对话框？	通过
	修改传感器的参数，并点击“确定”	是否正确修改传感器的对话框？	通过
	选择列表中的一项，点击“删除”按钮	是否正确删除该传感器的资料？	通过
	点击“启动”按钮	是否出现“采集端”对话框？	通过
	输入传感器规定的 ID 号，点击“连接”	动态曲线图上是否出现一条红色的曲线？	通过
		曲线图下方的列表里是否列出了传感器和相应池塘的各项资料？	通过
	继续连接其他传感器	动态曲线图上是否出现不同颜色的曲线？	通过
		是否最多连接 8 个传感器？	通过
	选择一个已连接的传感器，点击“断开”	动态曲线图上是否相应的曲线会消失	通过
	升高水温	动态曲线图上是否显示相应的变化？	通过
		相应池塘的状态是否由安全变为危险？	通过
		是否出现蜂鸣器报警对话框并听到峰鸣声？	通过
		是否出现邮件报警对话框，并在相应的油箱收到报警通知？	通过
		是否出现短信报警对话框，并有短	通过

		信发送到对应的手机？	
		是否出现.net alert 报警对话框，并通过 MSN 发送报警内容？	通过
	点击“停止”按钮	动态曲线图是否清空？	通过
	点击“改速”按钮	是否出现改速对话框？	通过
	拖动速度的标尺，由低到高	观察动态曲线图的速度是否有相应的变化？	通过
	通过状态窗体查看客户状态	是否能得到状态列表	通过
		是否能正确显示图像	通过
		是否能正确关闭图像	通过
	点击“添加规则”	是否能正确显示	通过
		是否能写入规则格式	通过
	点击“添加策略插件”	能否正确显示插件信息	通过
		能否加载插件	通过
		能否弹出结果对话框	通过
	点击“插件编译”	能否通过动态编译生成 dll	通过
		能否正确加载 DLL	通过
	点击“查看日志”	能否正确显示登陆管理情况	通过
	用 ASP.NET 查看	能否正确登陆	通过
		能否查看各个列表	通过
		能否进行修改和更新	通过
		能否进行删除	通过

主程序—客户端：

ID	动作	期待的结果	通过 / 失败
3.1	观察各个动态曲线图	是否有图像显示	通过
		观察动态曲线图中是否有相应的变化	通过
	观察第一页“安全状态”	是否正确显示“安全等级”	通过
		是否正确显示“连接状态”	通过
	选择第二页“网络状态”	是否正确显示各个正在监听状态的进程	通过

		能否刷新进程	通过
		能否结束进程	通过
	选择菜单栏“日志”察看”	观察是否能正确显示入侵事件	通过
	选择第三页“应用规则”	能否正确显示所有询问过的规则	通过
		能否禁止某一程序通信	通过
		能否删除规则	通过
		能否添加规则	通过
		能否修改规则	通过
	选择“IP 规则”	能否选择 IP 规则	通过
		能否取消 IP 规则	通过
		IP 规则是否起作用	通过
	选择“基本选项”	能否正确显示现在安全级别	通过
		能否修改级别	通过
		能否添加 IP 规则	通过
		添加后是否起作用	通过
		能否设置开机启动	通过
	选择“高级设置”	能否显示所有误用检测类别	通过
		能否进行类别的选择	通过
		能否打开实验环境	通过
		打开实验环境后确定防火墙是否关闭	通过
	选择“插件设置”	能否正确显示上次的设置	通过
		能否改变组数和时间的设置	通过
		能否改变插件	通过
		能否正确加载插件	通过
		能否正确加载并显示统计选项	通过
		能否选择统计选项	通过
		选择后能否在列表中正确显示	通过
		能否取消选择	通过
	选择“插件编译”	能否编辑文本	通过
		能否正确加载	通过
	选择菜单栏的“帮助”	选择“升级规则”能否成功与服务器通信	通过
		选择“升级黑名单”能否成功与服务器通信	通过
		选择“关于 ET 小组”能否成功显示相关信息	通过
	观测托盘图标	能否正确显示安全状态	通过
		能否用右键弹出选项	通过
		能否退出	通过
		能否返回主程序	通过

重点功能测试：

1、 状态检测对“拒绝服务攻击“的防御

测试工具	测试强度	测试结果（是否通过）
udpflood	**3000/sec**	通过
synflood	**3000/sec**	通过
icmpflood	**3000/sec**	通过

2、 误用检测对蠕虫特征的检测的效率

蠕虫名称	测试次数	有效检验次数
slammer	**20**	**19**
Redcode2	**20**	**18**

3、 基于统计模型的异常及检测的实验总结

采集总时间	状态变量个数	创建状态总数	攻击测试样本数	检验效率
5Hours	**28**	**98**	**34**	**40%**
8Hours	**28**	**87**	**34**	**58%**

14Hours	**28**	**65**	**34**	**74%**