测试文档

子模块：规则文件管理模块

|  |  |
| --- | --- |
| **测试目标** | 规则文件被正确编译并存入链表 |
| **测试方法** | 1. 将协议名输入本地文件/etc/snort/proto.config 2. 将协议文件放入本地文件夹/etc/snort/regexps 3. 启动snort 4. 查看正则表达式是否被正确载入 |
| **测试结果** | 正则表达式被正确载入   * 后台监控   + 本地正则表达式载入      * + Web端添加的正则表达式载入 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

子模块：连接管理模块

|  |  |
| --- | --- |
| **测试目标** | 连接被正确插入和删除 |
| **测试方法** | 1. 启动snort 2. 客户机进行各种网络行为 3. 观察连接插入删除情况 |
| **测试结果** | 连接被正确插入和删除   * 后台监控   + 连接被正确插入和删除 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.3 子模块：规则匹配模块

|  |  |
| --- | --- |
| **测试目标** | 数据包是否匹配正则表达式 |
| **测试方法** | 1. 启动snort 2. 客户机进行各种网络行为 3. 观察匹配情况 |
| **测试结果** | 数据包匹配正则表达式   * 后台监控   + 数据包被匹配 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

子模块：输出过滤模块

|  |  |
| --- | --- |
| **测试目标** | 数据是否被缓冲并输出 |
| **测试方法** | 1. 启动snort 2. 客户机进行各种网络行为 3. 观察过滤情况 |
| **测试结果** | 连续的数据包被过滤 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

子模块：输出模块

|  |  |
| --- | --- |
| **测试目标** | 数据是否被缓冲并输出 |
| **测试方法** | 1. 启动snort 2. 客户机进行各种网络行为 3. 观察缓冲和输出情况 |
| **测试结果** | 数据包被缓冲并且输出   * 后台监控   + 数据包被缓冲并且输出 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5 主模块：应用层协议匹配模块

4.5.1 验证协议匹配一（QQ2010 Beta 1530）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用QQ协议的主机IP和端口号 |
| **测试方法** | 1. 启动snort 2. 客户机登录QQ 3. 观察输出情况 |
| **测试结果** | 使用QQ的主机被检测到并输出信息到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.2 验证协议匹配二（迷你迅雷3.0 build：3.1.1.58）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用迅雷协议的主机IP和端口号 |
| **测试方法** | 1. 启动snort 2. 客户机登录迅雷   3）观察输出情况 |
| **测试结果** | 使用迅雷的主机被检测到并输出信息到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.3 验证协议匹配三（edonkey 1.1.7）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用edonkey协议的主机IP和端口号 |
| **测试方法** | 1）启动snort  2）客户机登录edonkey  3）观察输出情况 |
| **测试结果** | 使用edonkey的主机被检测到并输出到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.4 验证协议匹配四（windows live messenger版本14.0.8089.726）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用msn协议的主机IP和端口号 |
| **测试方法** | 1）启动snort  2）客户机登录msn  3）观察输出情况 |
| **测试结果** | 使用msn的主机被检测到并输出到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.5 验证协议匹配五（ftp）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用ftp协议的主机IP和端口号 |
| **测试方法** | 1）启动snort  2）客户机登录某个ftp  3）观察输出情况 |
| **测试结果** | 使用ftp的主机被检测到并输出到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.6 验证协议匹配六（http）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用http协议的主机IP和端口号 |
| **测试方法** | 1）启动snort  2）客户机登录浏览器，打开任意网页  3）观察输出情况 |
| **测试结果** | 使用http的主机被检测到并输出到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.7 验证协议匹配七（ssh）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用ssh协议的主机IP和端口号 |
| **测试方法** | 1）启动snort  2）客户机使用ssh  3）观察输出情况 |
| **测试结果** | 使用ssh的主机被检测到并输出到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.8 验证协议匹配八（kugoo build：6.1.18.404）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用kugoo协议的主机IP和端口号 |
| **测试方法** | 1）启动snort  2）客户机使用kugoo  3）观察输出情况 |
| **测试结果** | 使用kugoo的主机被检测到并输出到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.9 验证协议匹配九（dns）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用dns协议的主机IP和端口号 |
| **测试方法** | 1）启动snort  2）客户机使用dns进行地址解析  3）观察输出情况 |
| **测试结果** | 使用dns的主机被检测到并输出到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |

4.5.10 验证协议匹配十（bittorrent 6.4 build 18095）

|  |  |
| --- | --- |
| **测试目标** | 检测出使用bittorrent主机IP和端口号 |
| **测试方法** | 1）启动snort  2）客户机使用bittorrent  3）观察输出情况 |
| **测试结果** | 使用bittorrent的主机被检测到并输出到数据库   * 后台监控 |
| **结果分析** | 测试通过 ； 测试未通过 🞏 |



