****

软 件 工 程 实 验

软件测试需求规格说明书

基于Scapy的分析与扩展

Version 1.9

实 验 小 组 B组

小 组 成 员 陈鸿超（SY1806214）

李铎坤（SY1806219）

刘 颖（SY1806418）

袁梦阳（BY1806157）

编制时间： 2019年5月

版本变更历史

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 提交日期 | 编制人 | 修改说明 | 审核人 | 版本说明 |
| v1.9 | 2019/5/28 | 刘颖 | 根据A组意见修改文档 |  |  |
| v1.8 | 2019/5/24 | 袁梦阳 | 根据C组意见6、7修改文档 | 刘颖 |  |
| v1.7 | 2019/5/24 | 陈鸿超 | 根据C组意见修改文档 | 袁梦阳 |  |
| v1.6 | 2019/5/21 | 陈鸿超 | 规范文档格式 | 李铎坤 | 自查修改 |
| v1.5 | 2019/5/21 | 袁梦阳 | 增加了1.3，1.4，1.5，2.1 | 陈鸿超 | 自查修改 |
| v1.4 | 2019/5/21 | 李铎坤 | 增加了单元测试 | 袁梦阳 | 自查修改 |
| v1.3 | 2019/5/21 | 刘颖 | 完善文档 | 李铎坤 | 自查修改 |
| v1.2 | 2019/5/21 | 陈鸿超 | 增加了单元测试 | 刘颖 | 自查修改 |
| v1.1 | 2019/5/20 | 刘颖 | 完善了测试计划 | 陈鸿超 | 自查修改 |
| v1.0 | 2019/5/16 | 刘颖 | 完善部分测试用例 | 陈鸿超 | 初版完成 |
| v0.6 | 2019/5/16 | 袁梦阳 | 增加部分测试用例，修改表格格式 | 刘颖 | 初版 |
| v0.5 | 2019/5/16 | 李铎坤 | 小笔误修改 | 袁梦阳 | 初版 |
| v0.4 | 2019/5/15 | 陈鸿超 | 格式修改与用例编号修改 | 李铎坤 | 初版 |
| v0.3 | 2019/5/15 | 刘颖 | 部分测试用例 | 陈鸿超 | 初版 |
| v0.2 | 2019/5/15 | 李铎坤 | 部分测试用例 | 刘颖 | 初版 |
| v0.1 | 2019/5/14 | 陈鸿超 | 部分测试用例 | 李铎坤 | 初版 |

目录

[版本变更历史 I](#_Toc9368324)

[1 引言 1](#_Toc9368325)

[1.1 测试目的 1](#_Toc9368326)

[1.2 测试背景 1](#_Toc9368327)

[1.3 测试范围 1](#_Toc9368328)

[1.4 参考文献 1](#_Toc9368329)

[2 测试计划 2](#_Toc9368330)

[2.1 测试方法 2](#_Toc9368331)

[2.2 测试环境 2](#_Toc9368332)

[2.3 测试数据获取 3](#_Toc9368333)

[2.4 测试工具 4](#_Toc9368334)

[2.5 测试分工 5](#_Toc9368335)

[3 功能需求测试 6](#_Toc9368336)

[3.1 测试用例对应关系 6](#_Toc9368337)

[3.2 测试用例描述 8](#_Toc9368338)

[4 非功能需求测试 17](#_Toc9368339)

[4.1 测试用例对应关系 17](#_Toc9368340)

[4.2 测试用例描述 17](#_Toc9368341)

[5 总结 19](#_Toc9368342)

# 引言

## 测试目的

本组基于对Scapy的分析，扩展了报文处理的一些新功能，实现了一个更加完善的报文处理工具。

编写此测试需求规格说明书的目的是指导接下来对于所开发系统的测试活动。测试的目的是检查开发的系统是否完成了软件需求规格说明书中所要求的需求，检查所开发的系统是否正确可靠，发现系统中的问题，最后撰写测试报告。

## 测试背景

项目名称：基于Scapy的分析与扩展

测试人员：陈鸿超、刘颖、李铎坤、袁梦阳

开发人员：陈鸿超、李铎坤

## 测试范围

本测试依据软件需求规格说明书与设计文档，对Scapy的功能性需求和非功能性需求进行测试。

对Scapy的功能性需求描述在需求规格说明书的第4章和第7章，其测试用例在本文档第2章，单元测试用例编号0xx，集成测试用例编号1xx。

对Scapy的非功能性需求描述在需求规格说明书的第5章，其测试用例在本文档第3章，用例编号2xx。

## 参考文献

1. 邹欣.构建之法[M].北京.人民邮电出版社,2015:264-296
2. 单元测试[EB/OL].<https://www.liaoxuefeng.com/wiki/897692888725344/953546675792640>
3. 软件工程测试方法[EB/OL]. <https://blog.csdn.net/fightfaith/article/details/47858101>

# 测试计划

## 测试方法

本组基于对Scapy的分析，扩展了报文处理的一些新功能，实现了一个更加完善的报文处理工具。为了进行充分的测试，本组对扩展后的Scapy进行了集成测试和单元测试。

其中，集成测试针对项目中的每一个功能直接制定输入进行测试，发现其中的漏洞。单元测试对扩展功能中单独封装的类与函数进行测试，从代码细节上发现在实现上出现的问题。

## 测试环境

Scapy在不同的运行环境下都有一套相应版本的代码，但由于时间的限制，本项目扩展部分代码只基于Windows+Python3这个版本的Scapy源码进行开发。因此，本次测试也主要在Windows+Python3环境下进行。

Windows下Python3的安装与配置可以参考网上的教程，下面介绍一下扩展后Scapy的安装，步骤如下：

1. 使用pip命令行安装原始的Scapy库，命令行：pip install Scapy
2. 从本组github项中下载扩展后的Scapy源码，网址：<https://github.com/duolk/19TeamB_Scapy/tree/master/1.%E9%A1%B9%E7%9B%AE%E4%BB%A3%E7%A0%81>
3. 使用扩展后的源码覆盖掉pip安装的源码，安装路径：xxx/Python3/Lib/site-packages

在使用Scapy的某些特殊功能时，可能还需要借助其他插件，这时可以根据提示信息下载和安装相应插件。

各测试人员的测试环境如表2.1所示。

表格 1测试人员运行环境

|  |  |
| --- | --- |
| 成员 | 测试环境 |
| 刘颖 | 处理器：Intel Core i5  内存：8GB  磁盘：251GB  操作系统：Mac OS 10.14  Python环境：Python3.7 |
| 陈鸿超 | 处理器：Intel Core i7  内存：16GB  磁盘：1T  操作系统：Windows10  Python环境：Python3.7 |
| 李铎坤 | 处理器：Intel Core i7  内存：16GB  磁盘：1T  操作系统：Windows10  Python环境：Python3.6 |
| 袁梦阳 | 处理器：Intel Core i7  内存：16GB  磁盘：251GB  操作系统：Mac OS 10.14  Python环境：Python3.7 |

## 测试数据获取

在测试时需要用到的主要是pcap报文数据文件，测试人员可以通过借助tcpdump或者Wireshark工具截获网络上的流量，然后指定存储为pcap文件获得。

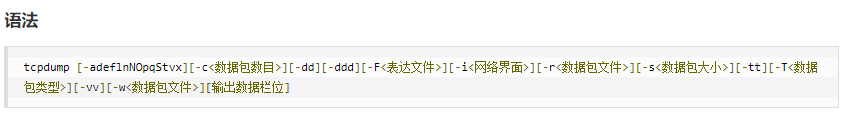


图 2.1tcpdump运行参数

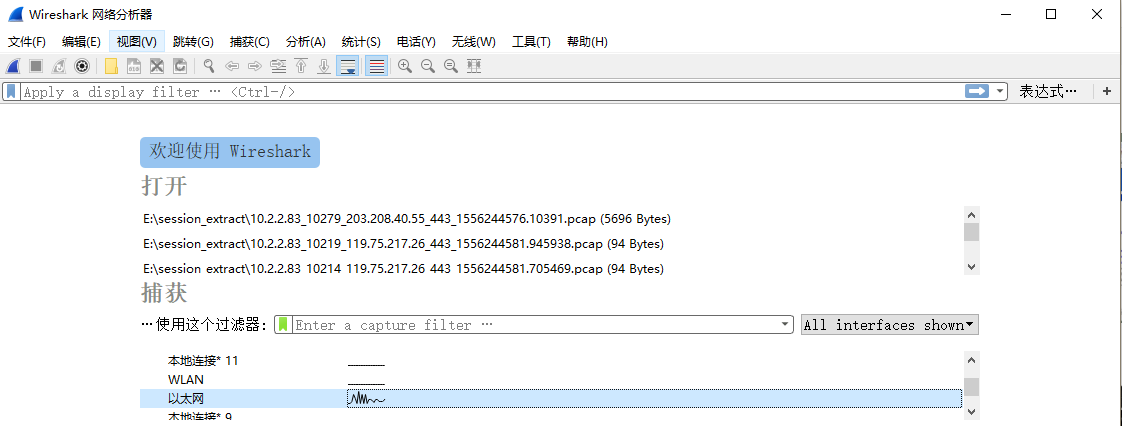


图 2.2Wireshark运行界面

## 测试工具

本测试用到的工具主要有PyCharm、Wireshark。其中，PyCharm是一种Python IDE，带有一整套可以帮助用户在使用Python语言开发时提高其效率的工具，比如调试、语法高亮、Project管理、代码跳转、智能提示、自动完成、单元测试、版本控制。

Wireshark是一个网络封包分析软件。网络封包分析软件的功能是抓取网络封包，并尽可能显示出最为详细的网络封包资料。在对Scapy产生的运行结果进行正确性验证时，测试人员可以使用Wireshark工具，该工具能够读取pcap等格式文件，然后进行详尽的报文展示。

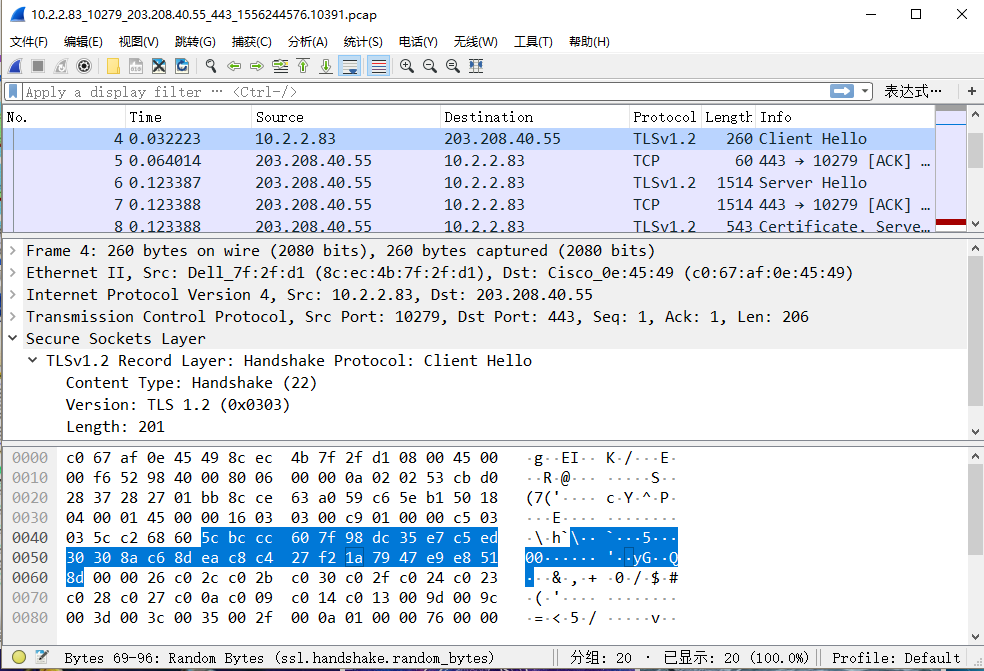


图 2.3Wireshark报文展示页面

## 测试分工

本次测试包括Scapy的原有功能测试和扩展功能测试，共有27个测试用例，测试组成员分工如下：

表格 2 测试分工

|  |  |  |
| --- | --- | --- |
| 成员 | 测试内容 | 测试用例 |
| 陈鸿超 | 测试扩展功能中的文件切分，监听持久化和协议类型获取。 | 编号为001、002、113、114、115、116、117的测试用例 |
| 刘颖 | 测试Scapy原有功能中的端口监听，数据解析，数据发送和数据构造功能。 | 编号为101，102，103，104，111，112的测试用例 |
| 李铎坤 | 测试Scapy的非功能需求中的兼容性，可扩展性，容错性和易用性。 | 编号为003、004、201，202，203，204，205的测试用例 |
| 袁梦阳 | 测试Scapy原有功能中的数据展示，数据导入和数据导出，以及Scapy扩展功能中的报文会话提取。 | 编号为105，106，107，108，109，110，118测试用例 |

# 功能需求测试

## 测试用例对应关系

表格 3功能需求测试用例与需求文档对应表

| **类型** | **功能需求** | **需求文档对应章节** | **测试用例** | **测试点** |
| --- | --- | --- | --- | --- |
| Scapy原有功能 | 端口监听 | 4.2.1 | 用例101端口报文监听测试 | 监听指定或多个端口功能是否正常 |
| 根据BPF过滤报文功能是否正常 |
| 监听指定数量报文功能是否正常 |
| 监听指定时间段内报文功能是否正常 |
| 返回报文数据的核对 |
| 数据解析 | 4.2.2 | 用例102数据报文解析测试 | 返回的协议对象类型及字段值核对 |
| 数据构造 | 4.2.3 | 用例103单层数据报文构造测试 | 完成的单层数据协议对象类型及字段值核对 |
| 用例104多层数据报文堆叠测试 | 堆叠完成的数据协议对象及字段值核对 |
| 数据展示 | 4.2.4 | 用例105数据包字符展示测试 | 控制台输出字符核对 |
| 用例106数据包图形展示测试 | 输出图形文件正确性核对 |
| 数据导入 | 4.2.5 | 用例107 pcap文件读取测试 | 读取指定个数报文功能是否正常 |
| 返回的数据对象值核对 |
| 用例108 16进制编码导入测试 | 返回的数据对象值核对 |
| 数据导出 | 4.2.6 | 用例109 pcap文件导出测试 | pcap报文文件正确性核对 |
| 用例110 16进制编码格式导出测试 | 16进制编码正确性核对 |
| 数据发送 | 4.2.7 | 用例111发送报文测试 | 发送到指定IP地址和链路层协议功能是否正常 |
| 报文成功发送验证 |
| 用例112发送并接收报文测试 | 超时无应答重发功能是否正常 |
| 报文成功发送验证 |
| 接收应答报文验证 |
| 没有应答的报文验证 |
| Scapy扩展功能 | 文件切分 | 7.2.1 | 用例113文件切分功能的兼容模式测试 | 存储方式指定功能，数据切分大小指定功能、文件格式指定功能是否正常 |
| 输出pcap文件正确性验证 |
| 用例114文件切分功能的极速模式测试 | 存储方式指定功能，数据切分大小指定功能是否正常 |
| 输出pcap文件正确性验证 |
| 用例001不解析模式的文件读取功能测试 | 文件头部字段读取验证 |
| 数据块头部读取验证 |
| 数据块块体读取验证 |
| 用例002不解析模式的文件写入功能测试 | 文件头数据写入功能 |
| 报文数据写入功能 |
| 监听持久化 | 7.2.2 | 用例115监听持久化功能的兼容模式测试 | 持久化数据文件的正确性验证 |
| 存储批大小指定功能是否正常 |
| 原有监听功能测试 |
| 用例116监听持久化功能的极速模式测试 | 持久化数据文件的正确性验证 |
| 存储批大小指定功能是否正常 |
| 原有监听功能测试 |
| 协议类型获取 | 7.2.3 | 用例117协议类型获取功能测试 | 待分析类型的协议层数指定功能是否正常 |
| 输出的协议类型核对 |
| 报文会话提取 | 7.2.4 | 用例118会话提取功能测试 | 四元组条件会话过滤功能，会话时间切分模式选择功能是否正常 |
| 切分的小文件正确性核对 |
| 分批处理的大小设置功能是否正常 |
| 用例003 PacketSession类单元测试 | 测试init方法运行是否正常 |
| 测试update方法是否能正确加入报文对象 |
| 测试scan方法能否正确用时间对会话进行截断 |
| 测试save方法是否能正确对会话数据进行导出 |
| 用例004 TestTetradJudge类单元测试 | 测试judge\_ip\_tetrad方法能否对IP对进行过滤 |
| 测试judge\_tetrad方法能否对四元组进行过滤 |

## 测试用例描述

表格 4用例001不解析模式的文件读取功能测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 不解析模式的文件读取功能测试 | | |
| **简要描述** | 本测试主要用于极速模式所使用的不解析模式的文件读取功能能否正常运行 | | |
| **前提和约束** | 安装好扩展后Scapy及其运行环境 | | |
| **测试步骤** | **1** | 准备好待切分的pcap文件 | |
| **2** | 实例化NoAnalysis\_PcapReader()文件解析对象，并传入pcap文件的路径 | |
| **3** | 调用get\_pcap\_head()方法获取文件头字节码数据 | |
| **4** | 调用read\_packet()方法读取数据块块头和块体字节码数据 | |
| **预期结果** | 步骤3 : 返回与pcap文件相应的文件头字节码数据  步骤4 : 返回pcap文件中相应的数据块的块头和块体字节码数据 | | |
| **评价准则** | 返回的字节码数据都与相应pcap文件中的字节码数据相同 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |

表格 5用例002不解析模式的文件写入功能测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 不解析模式的文件写入功能测试 | | |
| **简要描述** | 本测试主要用于极速模式所使用的不解析模式的文件写入功能能否正常运行 | | |
| **前提和约束** | 安装好扩展后Scapy及其运行环境 | | |
| **测试步骤** | **1** | 实例化NoAnalysis\_PcapWriter ()文件写入对象，并传入结果文件的路径 | |
| **2** | 构造文件头字节码字符串，调用\_write\_header()，写入文件头数据 | |
| **3** | 构造数据块字节码字符串元组，调用 \_write\_packet ()，写入数据块 | |
| **预期结果** | 步骤2 :构造的文件头字节码成功写入到结果文件中  步骤3 :构造的数据块字节码成功写入到结果文件中 | | |
| **评价准则** | 结果文件中的字节码数据与构造写入的相同 | | |
| **异常情况** | 文件路径有误 | | 程序提示异常信息，并终止运行 |

表格 6用例003 PacketSession类单元测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | PacketSession类单元测试 | | |
| **简要描述** | 本测试主要用于验证PacketSession类中的方法能否按照期望运行 | | |
| **前提和约束** | 安装好扩展后Scapy及其运行环境 | | |
| **测试步骤** | **1** | 设置参数，实例化PacketSession对象 | |
| **2** | 使用unittest测试模块的assertEqual验证各成员属性初始化是否成功 | |
| **3** | 构造报文与时间实例，传入不同的报文对象和时间参数，使用assertEqual验证update方法是否正确更新了data属性 | |
| **4** | 构造时间实例，传入不同的时间参数，使用assertEqual验证scan方法是否正确处理了data属性 | |
| **5** | 使用assertEqual验证save方法不同模式下，是否正确导出了data属性 | |
| **预期结果** | 步骤2 : 各成员属性正确初始化  步骤3 : update方法正确更新了data属性  步骤4 : scan方法正确处理了data属性  步骤5 : save方法正确导出了data属性 | | |
| **异常情况** | 文件路径有误 | | 程序提示异常信息，并终止运行 |

表格 7用例004 TestTetradJudge类单元测试

|  |  |  |
| --- | --- | --- |
| **名称** | TestTetradJudge类单元测试 | |
| **简要描述** | 本测试主要用于验证TetradJudge类中的方法能否按照期望运行 | |
| **前提和约束** | 安装好扩展后Scapy及其运行环境 | |
| **测试步骤** | **1** | 导入TetradJudge类 |
| **2** | 设置不同组合的IP过滤条件和IP对，使用unittest测试模块的assertEqual验证judge\_ip\_tetrad能否正确匹配过滤条件与IP对数据 |
| **3** | 设置不同组合的四元组过滤条件和四元组，使用unittest测试模块的assertEqual验证judge\_tetrad能否正确匹配过滤条件四元组与四元组数据 |
| **预期结果** | 步骤2 : 各组合输入下能够正常返回True或False  步骤3 : 各组合输入下能够正常返回True或False | |

表格 8用例101端口报文监听测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 端口报文监听测试 | | |
| **简要描述** | 本测试用例主要测试Scapy的端口监听功能，包括四个方面：抓取流量包，设置监听参数，设置停止监听条件和核对返回报文数据。 | | |
| **前提和约束** | 正确配置Python环境、安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 在sniff函数中配置iface参数，设置嗅探器所要嗅探的网卡，接受返回的数据包。 | |
| **3** | 在sniff函数中配置filter参数设置过滤规则。filter的规则使用BPF语法，可以限制抓取报文的IP等信息。 | |
| **4** | 在sniff函数中设置count参数的值，以限定嗅探包的数目。 | |
| **5** | 在sniff函数中设置stop\_filter，传入自定义的函数，当满足函数要求时Scapy停止嗅探。 | |
| 6 | 将以上几个步骤中嗅探到的报文打印出来以进行核对。 | |
| **预期结果** | 步骤2 :设置iface参数嗅探到的报文与iface的设置一致。  步骤3 :设置filter参数嗅探到的报文符合设置的BPF规则  步骤4 :设置count参数嗅探到的报文数量与count一致  步骤5 :设置stop\_filter参数嗅探到的数据包只有最后一个报文符合自定义函数的条件 | | |
| **评价准则** | 监听到的报文与参数设置情况一致 | | |
| **异常情况** | iface参数设置有误 | | 输出错误信息提示，并停止运行 |

表格 9用例102数据报文解析测试

|  |  |  |
| --- | --- | --- |
| **名称** | 数据报文解析测试 | |
| **简要描述** | 本测试用例检查Scapy是否能正确解析pcap文件 | |
| **前提和约束** | 正确配置Python环境、安装Scapy包、格式正确的pcap文件，安装Wireshark | |
| **测试步骤** | **1** | 在Python代码中导入Scapy |
| **2** | 利用Scapy的rdpcap函数读入pcap文件 |
| **3** | 利用repo函数得到数据包的规范化字符串 |
| **4** | 将解析后的报文内容打印出来 |
| **5** | 在Wireshark中打开pcap文件，并与Scapy的解析结果进行对比 |
| **预期结果** | Scapy解析后的报文与Wireshark中的报文各个字段的值都相同 | |
| **评价准则** | 解析报文的结果与Wireshark中的一致 | |

表格 10用例103单层数据报文构造测试

|  |  |  |
| --- | --- | --- |
| **名称** | 单层数据报文构造测试 | |
| **简要描述** | 本测试用例测试Scapy构造单层报文的正确性 | |
| **前提和约束** | 正确配置Python环境、安装Scapy包 | |
| **测试步骤** | **1** | 在Python代码中导入Scapy |
| **2** | 构造TCP、IP等类型的报文，并指定des，scr等字段 |
| **3** | 通过pack.show()方法查看构造的报文 |
| **预期结果** | 构造的报文字段与设定一致 | |
| **评价准则** | 实际结果与预期结果一致 | |

表格 11用例104多层数据报文构造测试

|  |  |  |
| --- | --- | --- |
| **名称** | 多层数据报文构造测试 | |
| **简要描述** | 本测试用例测试Scapy构造多层报文的正确性 | |
| **前提和约束** | 正确配置Python环境、安装Scapy包 | |
| **测试步骤** | **1** | 在Python代码中导入Scapy |
| **2** | 使用“/”操作符构造TCP、IP等类型堆叠的报文，可以单独指定每个类型报文的des，scr等字段 |
| **3** | 通过pack.show()方法查看构造的报文 |
| **预期结果** | 构造的报文字段与设定一致，堆叠方式与设定一致 | |
| **评价准则** | 实际结果与预期结果一致 | |

表格 12用例105数据包字符展示测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 数据包字符展示测试 | | |
| **简要描述** | 本测试验证开发人员是否可以按照要求导出数据包的字符展示结果。 | | |
| **前提和约束** | 正确配置Python环境、正确安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| 2 | 利用Scapy的rdpcap函数读入待测试pcap文件 | |
| **3** | 调用报文数据的show方法显示数据的字符展示 | |
| **预期结果** | 输出报文数据包的字符展示 | | |
| **评价准则** | 报文字符展示与Wireshark解析结果一致且完整，即为正确。 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |
| 报文数据有误 | | 在会影响程序正常执行的情况下提示异常信息，并终止运行 |

表格 13用例106 数据包图形展示测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 数据包图形展示测试 | | |
| **简要描述** | 本测试验证开发人员是否可以按照要求导出数据包的图形展示PDF。 | | |
| **前提和约束** | 正确配置Python环境、正确安装Scapy和PyX包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 利用Scapy的rdpcap函数读入待测试pcap文件 | |
| **3** | 设定layer\_shift参数 | |
| **4** | 调用pdfdump函数生成PDF | |
| **预期结果** | 正确导出报文数据包的图形展示 | | |
| **评价准则** | 报文图形展示内容与Wireshark解析结果一致且完整，即为正确。 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |
| 报文数据有误 | | 在会影响程序正常执行的情况下提示异常信息，并终止运行 |

表格 14用例107 pcap文件读取测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | pcap文件读取测试 | | |
| **简要描述** | 本测试验证开发人员是否可以正确读入pcap文件。 | | |
| **前提和约束** | 正确配置Python环境、正确安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 设置待读入文件存储位置、读取报文数量 | |
| **3** | 利用Scapy的rdpcap函数读入待测试pcap文件 | |
| **4** | 调用报文数据的show方法显示数据的字符展示 | |
| **预期结果** | 正确读入预期数量的报文数据 | | |
| **评价准则** | 读入后的pcap包数据展示结果与Wireshark打开的结果相同即为正确，同时计算是否读入了指定数量的报文。 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |

表格 15用例108 16进制编码导入测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 16进制编码导入测试 | | |
| **简要描述** | 本测试验证开发人员是否可以按照要求以16进制编码格式导入报文数据。 | | |
| **前提和约束** | 正确配置Python环境、正确安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 利用Scapy的rdpcap函数读入待测试pcap文件 | |
| **3** | 调用报文数据的show方法显示原始数据的字符展示 | |
| 4 | 调用str函数将报文数据转换为16进制格式 | |
| **5** | 调用报文数据的show方法显示16进制转化出的数据的字符展示 | |
| **预期结果** | 正确地将16进制编码格式的报文数据读入为Scapy解析格式 | | |
| **评价准则** | 步骤3与步骤5所得结果相同 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |

表格 16用例109 pcap文件导出测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | pcap文件导出测试 | | |
| **简要描述** | 本测试验证开发人员是否可以正确导出pcap文件 | | |
| **前提和约束** | 正确配置Python环境、正确安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 利用Scapy的rdpcap函数读入待测试pcap文件 | |
| **3** | 调用wrpcap函数导出pcap文件 | |
| **预期结果** | 正确导出pcap文件 | | |
| **评价准则** | 导出后的pcap包数据与原始数据在Wireshark中打开的结果相同。 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |

表格 17用例110 16进制编码格式导出测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 16进制编码格式导出测试 | | |
| **简要描述** | 本测试验证开发人员是否可以导出正确的16进制编码格式的报文数据。 | | |
| **前提和约束** | 正确配置Python环境、正确安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 利用Scapy的rdpcap函数读入待测试pcap文件 | |
| **3** | 调用str函数将报文数据转换为16进制格式 | |
| **4** | print输出转换后结果 | |
| **预期结果** | 正确导出16进制格式的报文数据 | | |
| **评价准则** | 与Wireshark中16进制结果作对比，相同 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |

表格 18用例111发送报文测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 发送报文测试 | | |
| **简要描述** | 本测试用例测试Scapy发送报文的正确性 | | |
| **前提和约束** | 正确配置Python环境、安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 构造网络层报文，并作为参数传入send函数 | |
| **3** | 构造数据链路层报文，并作为参数传入sendp函数，同时设置iface参数指定发送数据包的网卡。 | |
| **4** | 分别执行send和sendp函数 | |
| **预期结果** | 1. 运行send()函数后，IDE会显示成功发送一个数据包 2. 运行sendp()函数后，IDE会显示成功发送一个数据包 | | |
| **评价准则** | 实际结果与预期结果一致 | | |
| **异常情况** | iface参数设置有误 | | 输出错误提示信息，并停止运行 |
| 报文构造有误 | | 输出错误提示信息，并停止运行 |

表格 19用例112发送并接收报文测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 发送并接收报文测试 | | |
| **简要描述** | 本测试用例测试Scapy发送并接收报文的正确性 | | |
| **前提和约束** | 正确配置Python环境、安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 构造网络层报文，报文的目的地址设置为一个不可达的IP。将报文作为参数传入sr函数，并通过timeout和retry配置超时时间和重传次数。 | |
| **3** | 构造网络报文，并通过变量ans,unasns接受其返回值。然后通过通过两个变量的summary()方法显示收到返回值的报文和没有收到返回值的报文。 | |
| **4** | 分别执行2和3中的操作 | |
| **预期结果** | 1. 执行2中的操作后，可以看到Scapy不断尝试发报文，尝试的次数为retry中配置的次数，并最终显示报文未送达，接收到0个返回值。 2. 调用ans变量的summary方法后显示出接收到返回值的报文，调用unans变量的summary方法后显示出未收到返回值的报文。 | | |
| **评价准则** | 实际结果与预期结果一致 | | |
| **异常情况** | iface参数设置有误 | | 输出错误提示信息，并停止运行 |
| 报文构造有误 | | 输出错误提示信息，并停止运行 |

表格 20用例113文件切分功能的兼容模式测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 文件切分功能的兼容模式测试 | | |
| **简要描述** | 本测试主要用于验证pcap文件切分功能的兼容模式能否正常运行 | | |
| **前提和约束** | 安装好扩展后Scapy及其运行环境 | | |
| **测试步骤** | **1** | 准备好待切分的pcap文件 | |
| **2** | 设置基本参数，包括监听模式、数据路径、结果路径、批大小，测试基本切分功能 | |
| **3** | 再设置文件名前缀参数，测试结果命名功能 | |
| **4** | 再设置链路层类型、存储类型参数，测试兼容模式下的自定义文件格式功能 | |
| **预期结果** | 步骤2 : 结果目录下产生切分好的pcap文件  步骤3 : 结果目录下产生切分好的、指定文件名前缀的pcap文件  步骤4 : 结果目录下产生切分好的、指定格式的pcap文件 | | |
| **评价准则** | 1. 切分后的pcap文件个数、名称、文件中的报文个数、格式与设置的参数一致 2. 切分后的pcap文件中的报文内容与切分前一致 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |
| 报文数据有误 | | 在会影响程序正常执行的情况下提示异常信息，并终止运行 |

表格 21用例114文件切分功能的极速模式测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 文件切分功能的极速模式测试 | | |
| **简要描述** | 本测试主要用于验证pcap文件切分功能的极速模式能否正常运行 | | |
| **前提和约束** | 安装好扩展后Scapy及其运行环境 | | |
| **测试步骤** | **1** | 准备好待切分的pcap文件 | |
| **2** | 设置基本参数，包括监听模式、数据路径、结果路径、批大小，测试基本切分功能 | |
| **3** | 设置文件名前缀参数，测试结果命名功能 | |
| **预期结果** | 步骤2 : 结果目录下产生切分好的pcap文件  步骤3 : 结果目录下产生切分好的、指定文件名前缀的pcap文件 | | |
| **评价准则** | 1. 切分后的pcap文件个数、名称、文件中的报文个数、格式与设置的参数一致 2. 切分后的pcap文件中的报文内容与切分前一致 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |
| 报文数据有误 | | 在会影响程序正常执行的情况下提示异常信息，并终止运行 |

表格 22用例115监听持久化功能的兼容模式测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 监听持久化功能的兼容模式测试 | | |
| **简要描述** | 本测试主要用于验证监听持久化功能的兼容模式能否正常运行 | | |
| **前提和约束** | 1. 安装好扩展后Scapy及其运行环境 2. 确保运行环境的设备和网络正常 | | |
| **测试步骤** | **1** | 设置基本运行参数，包括监听模式、结果路径、批大小 | |
| **2** | 设置停止监听参数，测试不同的停止监听功能 | |
| **3** | 设置文件名前缀参数，测试结果命名功能 | |
| **4** | 设置端口参数，测试指定监听端口功能 | |
| **5** | 设置报文筛选条件，测试筛选报文功能 | |
| **6** | 打印出监听到的报文，测试监听到的报文是否被解析 | |
| **预期结果** | 步骤2 : 按照停止条件停止监听，并在结果目录下存储了监听到的报文数据文件  步骤3 : 结果目录下产生了指定文件名前缀的pcap文件  步骤4 : 结果文件中的报文数据来自于指定硬件端口  步骤5 : 结果文件中的报文数据符合筛选规则  步骤6 : 打印出的报文是Scapy已经解析后的格式 | | |
| **评价准则** | 1. 监听结果文件中的报文数据符合监听时设置的各参数要求 | | |
| **异常情况** | 监听到的报文数据有问题，无法正常解析 | | 输出错误日志，然后继续监听 |

表格 23用例116监听持久化功能的极速模式测试

|  |  |  |
| --- | --- | --- |
| **名称** | 监听持久化功能的极速模式测试 | |
| **简要描述** | 本测试主要用于验证监听持久化功能的极速模式能否正常运行 | |
| **前提和约束** | 1. 安装好扩展后Scapy及其运行环境 2. 确保运行环境的设备和网络正常 | |
| **测试步骤** | **1** | 设置基本运行参数，包扩监听模式、结果路径、批大小 |
| **2** | 设置停止监听参数，测试不同的停止监听功能 |
| **3** | 设置文件名前缀参数，测试结果命名功能 |
| **4** | 设置端口参数，测试指定监听端口功能 |
| **5** | 设置报文筛选条件，测试筛选报文功能 |
| **6** | 打印出监听到的报文，测试监听到的报文是否按照自定义格式处理 |
| **预期结果** | 步骤2 : 按照停止条件停止监听，并在结果目录下存储了监听到的报文数据文件  步骤3 : 结果目录下产生了指定文件名前缀的pcap文件  步骤4 : 结果文件中的报文数据来自于指定硬件端口  步骤5 : 结果文件中的报文数据符合筛选规则  步骤6 : 打印出的报文是自定义的字典格式 | |
| **评价准则** | 1. 监听结果文件中的报文数据符合监听时设置的各参数要求 | |

表格 24用例117协议类型获取功能测试

|  |  |  |
| --- | --- | --- |
| **名称** | 协议类型获取功能测试 | |
| **简要描述** | 本测试主要用于验证协议类型获取功能能否正常运行 | |
| **前提和约束** | 1. 安装好扩展后Scapy及其运行环境 | |
| **测试步骤** | **1** | 准备好包含多种报文数据的pcap文件 |
| **2** | 使用Scapy本身的文件读取功能读取并解析报文数据 |
| **3** | 调用协议类型获取功能输出报文所有层协议类型、最高层可识别协议类型、指定层的协议类型 |
| **预期结果** | 能够正确输出Scapy解析后报文的指定协议信息 | |
| **评价准则** | 1. 输出的协议信息与Wireshark中各报文的协议信息一致 | |

表格 25用例118 会话提取功能测试

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 会话提取功能测试 | | |
| **简要描述** | 本测试验证开发人员是否可以正确进行会话提取。主要测试包括四元组条件会话过滤功能，会话时间切分模式选择功能是否正常、切分的小文件正确性核对、分批处理的大小设置功能是否正常。 | | |
| **前提和约束** | 正确配置Python环境、正确安装Scapy包 | | |
| **测试步骤** | **1** | 在Python代码中导入Scapy | |
| **2** | 实例化SessionExtractor()类 | |
| **3** | 调用SessionExtractor()类中run方法，其中要设定待提取文件路径、会话文件输出路径、分批读入报文个数、存储文件前缀、四元组过滤器、会话切分时间阈值、会话切分模式、信息显示级别参数。即可提取出会话文件。   1. 改变会话过滤器参数，测试过滤功能。 2. 改变切分模式，测试切分模式选择功能是否正常。 3. 改变分批读入报文个数参数，测试分批处理功能是否正常。 | |
| **预期结果** | 按照设定要求正确提取目标文件中的会话。 | | |
| **评价准则** | 与Wireshark中解析结果作对比，判断会话是否正确提取 | | |
| **异常情况** | 文件格式有误 | | 程序提示可能的异常信息，并终止运行 |

# 非功能需求测试

## 测试用例对应关系

表格 26 非功能需求测试用例与需求文档对应表

|  |  |  |
| --- | --- | --- |
| **非功能需求** | **需求文档对应章节** | **测试用例** |
| 兼容性 | 5.1 | 用例201操作系统兼容性测试 |
| 用例202Python版本兼容性测试 |
| 可扩展性 | 5.2 | 用例203新协议扩展性测试 |
| 容错性 | 5.3 | 用例204非法数据解析测试 |
| 易用性 | 5.4 | 用例205交互模式函数调用测试 |

## 测试用例描述

表格 27用例201操作系统兼容性测试

|  |  |  |
| --- | --- | --- |
| **名称** | 操作系统兼容性 | |
| **简要描述** | 本测试用例用于验证Scapy工具库是否能够运行于不同的操作系统上（Windows，Linux等）上，即在不同系统上Scapy各个基础功能模块是否可以按照预期方式执行，是否具备操作系统无关性。 | |
| **前提和约束** | 目标操作系统上已安装Python环境和Scapy工具库，准备好测试数据。 | |
| **测试步骤** | **1** | 新建Python脚本，在其中编写依次调用各个主要功能模块对测试数据进行处理并输出结果的代码 |
| **2** | 在不同的系统下，执行该Python代码，并记录其输出结果 |
| **3** | 将各系统下的输出结果和预期结果进行对比 |
| **预期结果** | 不同系统下，执行没有出现运行时错误，且各输出结果和预期输出一致。 | |
| **评价准则** | 输出结果若为控制台字符串形式或普通文件，则进行字符串或内容对比，若为输出报文文件，则使用Wireshark打开后进行对应报文逐个比较。 | |

表格 28 用例202Python版本兼容性测试

|  |  |  |
| --- | --- | --- |
| **名称** | Python版本兼容性 | |
| **简要描述** | 本测试用例用于验证Scapy工具库是否提供了能运行于要求的不同版本Python环境上的代码（Python2.7+，Python3.4+），即Scapy工具库是否提供了Python2/3环境下的支持，以适应实际复杂的生产环境。 | |
| **前提和约束** | 目标操作系统上已安装Anaconda环境，并以此创建了要求的不同版本Python虚拟环境（2.7，3.4，…，3.7） | |
| **测试步骤** | **1** | 在不同虚拟环境下，执行pip install Scapy命令安装Scapy工具库 |
| **2** | 安装完成后，运行虚拟环境Python解释器，执行import Scapy.all as Scapy |
| **3** | 运行Scapy控制台工具 |
| **预期结果** | 不同版本环境下，执行Scapy库导入成功，控制台运行成功 | |
| **评价准则** | Scapy能够在不同版本环境下导入，并能正常运行控制台工具 | |

表格 29用例203新协议扩展性测试

|  |  |  |
| --- | --- | --- |
| **名称** | 对于新协议的扩展性 | |
| **简要描述** | 本测试用例用于验证基于Scapy的分析与扩展项目的最终产品是否具有对于新协议的扩展性，即是否能够在尽量少修改项目代码的基础上完成对一个全新协议的支持。 | |
| **前提和约束** | Scapy正常运行所需要的环境均已配置好，且准备好待添加的新协议字段格式。 | |
| **测试步骤** | **1** | Python代码中创建新协议类，继承自Packet父类，并依据新协议格式定义字段名称、类型及内容 |
| **2** | 使用bind\_layers函数将新协议类和已存在的协议层进行绑定（例如将新协议插入在TCP层的payload中） |
| **3** | 使用Scapy数据构造模块构造出包含该新协议的报文对象 |
| **4** | 使用数据存储模块将报文对象存储为pcap文件 |
| **5** | 使用数据导入模块导入该pcap文件为报文对象 |
| **6** | 对比直接构造的报文对象和导入的报文对象 |
| **预期结果** | 整个过程中，Scapy可以正常构造、存储，导入和解析包含该新协议的报文，且前后的报文对象一致，对该新协议的扩展无需修改Scapy原本的项目代码。 | |
| **评价准则** | 使用Scapy.ls功能函数打印报文对象的所有字段，并逐个进行比对 | |

表格 30用例204非法数据解析测试

|  |  |  |
| --- | --- | --- |
| **名称** | 非法数据解析 | |
| **简要描述** | 本测试用例用于验证基于Scapy的分析与扩展项目的最终产品是否能够处理非法的数据报文，即对于包含非法字段或者非法的协议层是否进行原始保留处理，将其封装入Raw类型对象中。 | |
| **前提和约束** | Scapy正常运行所需要的环境均已配置好，且准备好包含非法内容的数据报文。 | |
| **测试步骤** | **1** | 调用数据导入和解析模块对非法数据报文文件进行导入和解析 |
| **2** | 调用解析后报文对象的show()方法查看解析的各层协议类型 |
| **3** | 将得到的协议类型和数据文件的真实情况进行对比 |
| **预期结果** | 导入和解析过程中没有出现运行时错误，且从包含非法数据的协议层向上的数据部分被封装为Raw协议层类型 | |
| **评价准则** | 使用Wireshark打开原始非法数据文件，将其与show()方法返回结果进行逐层对比，Wireshark未识别的部分对应报文对象的Raw层 | |

表格 31用例205交互模式函数调用测试

|  |  |  |
| --- | --- | --- |
| **名称** | 交互模式函数调用 | |
| **简要描述** | 本测试用例用于验证基于Scapy的分析与扩展项目的最终产品是否能成功进入交互模式，并调用各个功能函数进行处理。 | |
| **前提和约束** | Scapy正常运行所需要的环境均已配置完毕 | |
| **测试步骤** | **1** | 在命令行下输入命令Scapy，进入Scapy交互模式 |
| **2** | 使用a=IP(ttl=10) Ether()/IP()/IP()/UDP()等类似命令进行packet创建或进行packet堆叠操作 |
| **3** | 使用a=rdpcap("/spare/captures/isakmp.cap")类似命令读取pcap文件，使用wrpcap写入pcap文件 |
| **4** | 使用pdfdump，psdump进行报文可视化展示 |
| **5** | 类似的调用Scapy中其他的功能函数（数据监听与发送，扩展部分功能函数等）进行报文处理 |
| **6** | 将各条命令执行结果和import导入方式函数执行结果进行对比 |
| **预期结果** | 在交互模式下各个功能函数完成了与库导入形式下相同的操作 | |
| **评价准则** | 相同的输入下，各个功能函数的返回对象、输出文件或者交互显示结果在交互模式下和库导入模式下相同 | |

# 总结

本组的测试计划一共包含了测试用例27个，其中单元测试共4个，集成测试共23个。其中单元测试针对的是本组扩展功能的基础单元函数，集成测试针对所有需求规格说明书中涉及到的功能需求以及非功能需求。