**郑州大学软件与应用科技学院**

**工程实践实习（实训）总结报告**



学生学号： 20137740467

学生姓名： 赵晓宁

专 业： 软件测试

班 级： 4班

企业导师： 兰景宏

实训（实习）公司： 北京卫达科技有限公司

2017年 5月 15日

**说明**

1.实习（实训）结束之前，每个学生都必须认真撰写《工程实践实习（实训）总结报告》。通过撰写实习（实训）总结报告，系统地回顾和总结实习（实训）的全过程，将实践性教学的感性认识升华到一定的理论高度，从而提高实习（实训）效果。

2. 实习（实训）总结报告要求条理清晰，内容详尽，数据准确。字数不少于3000字。

3.实习（实训）总结报告的质量反映了实习（实训）的质量，它是实习（实训）成绩评定的主要依据之一。应在规定时间内将此报告上交。不交实习（实训）报告者不得参加实习（实训）成绩评定。

4．封面中的“实习（实训）单位”必须写单位的全名，必须写上企业指导教师姓名。

5．“前言”部分：“实习（实训）背景”可简介实习（实训）目的等内容；“实习（实训）环境”可包括实习（实训）单位全称（中英文）、地址、实习（实训）单位性质、规模、简介、所在部门、该部门主要工作、指导教师安排等内容；“实习（实训）过程”概述实习（实训）各阶段所从事的主要工作等。

6.“实习（实训）内容”部分：属报告的主要部分。“概述”包括项目介绍、本人从事的工作等；“相关技术”包括与项目相关的理论基础，项目开发方法、开发工具、开发环境等关键技术的介绍；“系统分析”包括对整个项目的介绍分析及本人工作内容的详细分析，如业务分析、功能分析（可使用用例图、活动图来描述）、可行性分析等；“系统设计”包括总体设计和详细设计，总体设计包括系统架构设计、功能模块划分等，详细设计要围绕本人工作内容展开，包括功能模块详细设计、类和对象的设计、动态模型设计（时序图、状态图、协作图等）、算法设计、数据库设计等；“系统实现”也要围绕本人工作内容展开，从编码实现角度论述相应功能模块的实现细节，并展示自己所完成的主要成果及实际应用情况等。可通过“程序流程图”、“关键代码”和“界面”进行直观论述。“系统测试”包括测试方案设计、测试用例和测试结果、最终的测试结论或评价等。

7． “总结”部分：实习感悟及个人收获，实习总结，其中“其它意见”可对学院课程设置、教学内容、实习（实训）安排等方面提出自己的意见或建议，也可对实习（实训）单位的各个方面提出自己的意见。

# 一、前言

## 1.1 实习（实训）背景

经过了大学四年软件技术专业的理论进修，使我们软件技术专业的基础知识有了根本掌握。我们即将离开大学校园，作为大学毕业生，心中想得更多的是如何去做好自己专业发展、如何更好的去完成以后工作中每一个任务。

## 1.2 实习（实训）环境

实习期间，我在实习单位的的研发中心(部门)工作，研发中心主要从事于产品的研发。我被安排在该部门的一个小组工作，该部门有经理1名，主管1名。

## 1.3实习（实训）过程

本人参与软件技术岗位的日常工作，参与组织制定单位软件技术岗位发展规划和年度工作计 划（包括年度经费使用计划，仪器设备申购计划等），并协助同事组织实施和检查执行情况。协助主管领导科学管理，贯彻、实施有关规章制度。确定自己在软件技术专业岗位的工 作职责与任务，定期进修和业务相关的知识，不断提高业务水平和工作能力。 在工作过程，跟同事一起通过与客户的洽谈，现场勘察，尽可能多地了解客户从事的职 业、喜好、业主要求的使用功能和追求的风格等。努力提高客户建立良好关系能力，给客户量身打造设计方案。

# 二、实习（实训）单位（岗位）简介

## 2.1实习（实训）时间

2016年10月至2017年1月。

## 2.2实习（实训）单位（岗位）简介

北京卫达科技有限公司（VEDA）全球首创“智能动态防御”（AI Dynamic Defence）技术，颠覆传统网络安全理念、打破原有网络安全防御被动格局、引领新型网络安全防御技术发展方向。 VEDA总部位于北京市朝阳区，下设西安、成都和郑州三个研发中心，是国家高新技术企业、中关村高新技术企业，通过了ISO-9001-2015、国军标质量管理体系认证、武器装备科研生产单位保密资格认证。致力于成为全球领先的网络安全技术服务提供商。

# 三、实习（实训）内容

## 3.1概述

在实习期间本人完成了一个沙箱系统的项目。

## 3.2相关技术

动态分析是对恶意代码的行为进行分析，静态分析是将可执行文件以二进制形式打开，根据pe结构中所定义的规范找到可执行文件的代码块，数据块，导入表，导出表等信息，将这些信息静态的从二进制文件中取出展示给分析者，让分析者可以看到它们有哪些可疑的操作。有些可执行文件加密之后，如果只使用静态分析是不能看到它们的可疑操作的，只有在运行时它们才会进行那些有害的操作。而动态分析则是将可执行文件在真实的系统或者沙箱中运行，记录其进程之间的调用关系以及调用了哪些函数，该可执行文件对磁盘的操作以及该可执行文件运行时的流量等信息。

## 3.3系统分析

该系统需要让用户可以通过restful api或者web界面提交恶意代码样本至主节点的数据库中，调度系统将会为每个任务分配其请求的资源（虚拟机的类型，版本以及网络条件等），当样本的数量足够多时可以将它们负载均衡到集群里面每个节点上进行分析，并将结果返回到主节点。需要为用户提供的功能包括提交任务，注册节点，删除节点，获取任务状态，获取任务列表，查看任务详细信息获取节点信息等功能。

## 3.4系统设计

系统的运行分为两部分。首先是从节点的启动，在系统开机后首先需要运行virtualbox虚拟机创建vboxnet0虚拟网卡。然后运行cuckoo.py文件，该文件启动之后会创建服务器，加载各个分析模块，获取该节点当前可用的客户机，并周期性的查询数据库的tasks表，取出所有的任务并筛选出status为pending的任务，如果有处于等待状态的任务则取出该任务，并准备好该任务所需要的条件（将样本文件，分析所需要的python脚本和dll动态链接库打包成一个zip文件）然后开启虚拟机，恢复该虚拟机之前保存的快照（该快照运行了一个agent.py脚本创建了一个服务器，调度程序会去连接该服务器并将打包好的文件上传至虚拟机，然后该脚本将收到的zip压缩文件解压到之前配置的目录。），虚拟机启动之后该进程会发送指令运行各个模块（包括模拟鼠标点击，截图等），并让虚拟机启动样本文件并注入之前准备好的动态链接库（该动态链接库会hook一些系统敏感的函数,当测试样本调用这些函数时它会记录这些函数的调用情况,并连接agent.py创建的命名管道将收集的的信息发送至agent进程），agent进程会连接cuckoo.py文件创建的服务器并将收集到的结果实时传递给它，最后由它将结果存储至mongodb和磁盘。最后还需要启动utils/api.py它会创建一个服务器来供主节点连接为主节点服务。

然后是主节点的启动，在主节点的系统启动需要启动四个服务。第一个是web服务。Web服务采用python django框架，用户需运行web/mange.py文件来启动服务。第二个是供用户在控制台使用restful api提交任务的服务它采用flask框架实现，对用户提供了节点注册，节点删除，获取节点的信息，提交任务，获取任务状态，列出所有任务等功能。需要运行distribute/app.py来启动。第三个是调度服务，用户需运行distribute/instance.py文件来启动调度服务，该服务包括三部分：分配任务，设置节点状态，监控每个可用的节点。

## 3.5系统实现

主节点restful api使用python flask框架设计，主要包括：

任务提交

节点注册

节点删除

获取节点的信息

提交任务

获取任务状态

列出所有任务

从节点restful api使用python flask框架设计，主要包括：

创建任务

提供此节点任务列表

提供此节点某个任务的状态

提供任务报告

提供任务的pcap包

提供此节点状态

提供此节点的客户机信息

## 3.6系统测试

系统测试是对系统的组装和验证的测试。系统测试是整个产品系统的测试。目的是验证系统是否满足要求规范，并确定其与要求不一致或矛盾的位置，以便提出更完善的程序。系统测试发现问题后，尝试找出错误的原因和位置，然后进行更正。这是基于黑盒类测试的整体系统要求，应该覆盖系统的所有组件。测试对象不仅包括要测试的软件，还包括软件依赖的硬件，外围设备甚至包括某些数据，一些支持软件及其接口。

表3-1 测试用例表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 功能模块 | 测试用例 | 测试结果 |
| 1 | Restful api任务提交 | 用例： curl http://localhost:9003/api/task -F file=@calc.exe | 测试结果：成功添加任务 |
| 2 | Restful api节点注册 | 用例：curl http://localhost:9003/api/node -F name=cuckoo1 -F url=http://192.168.16.102:8090/ | 测试结果：成功注册节点 |
| 3 | Restful api节点删除 | 用例： curl -XDELETE http://localhost:9003/api/node/cuckoo1 | 测试结果：成功删除该节点 |
| 4 | Restful api获取节点信息 | 用例：curl http://localhost:9003/api/node/cuckoo1 | 测试结果：成功获取该节点信息 |
| 5 | Restful api获取任务状态 | 用例：curl http://localhost:9003/api/task/1 | 测试结果：成功获取id对应的任务状态 |
| 6 | 从节点Restful api创建任务（文件） | 用例：curl http://192.168.16.102:8090/ tasks/create/file  data = dict(  tid=task["id"],  package=task["package"],  timeout=task["timeout"],  priority=task["priority"],  options=task["options"],  machine=task["machine"],  platform=task["platform"],  tags=task["tags"],  custom=task["custom"],  owner=task["owner"],  memory=task["memory"],  clock=task["clock"],  enforce\_timeout=task["enforce\_timeout"],  ) | 测试结果：成功在此节点创建任务（文件） |
| 7 | 从节点Restful api提供此节点任务列表 | 用例：curl http://192.168.16.102:8090/ tasks/ tasks/ list  params=dict(status=status) | 测试结果：成功获取从节点任务列表 |
| 8 | 从节点Restful api提供此节点某任务物状态 | 用例：curl http://192.168.16.102:8090/tasks/view/ <int:task\_id> | 测试结果：成功获取从节点对应id的任务状态 |
| 9 | 从节点Restful api提供任务报告 | 用例：curl http://192.168.16.102:8090 / tasks/ report/<int:task\_id> | 测试结果：成功获取此节点上对应id的任务报告 |
| 10 | 从节点Restful api提供任务的pcap包 | 用例：curl http://192.168.16.102:8090/ pcap/ get/<int:task\_id> | 测试结果：成功获取此节点上对应id任务的pcap包 |
| 11 | 从节点Restful api提供此节点的状态 | 用例：curl  http://192.168.16.102:8090//cuckoo/status | 测试结果：成功获取此节点的当前状态 |
| 12 | 从节点Restful api提供此节点的客户机信息 | 用例：curl http://192.168.16.102:8090//machines/list | 测试结果：成功获取此节点上所有的客户机信息 |
| 13 | 从节点Restful api创建任务（url） | 用例：curl http://192.168.16.102:8090/ tasks/create/url  data = dict(  tid=task["id"],  package=task["package"],  timeout=task["timeout"],  priority=task["priority"],  options=task["options"],  machine=task["machine"],  platform=task["platform"],  tags=task["tags"],  custom=task["custom"],  owner=task["owner"],  memory=task["memory"],  clock=task["clock"],  enforce\_timeout=task["enforce\_timeout"],  url=task["path"],  ) | 测试结果：成功获取此在节点上创建url任务 |

# 四、实习(实训）总结

## 4.1实习（实训）体会

在实习的那段时间，让我体会到从工作中再拾起书本的困难性。每天较早就要上班工作，晚上较晚才下班回宿舍，深感疲惫，很难有精力能再静下心来看书。这更让人珍惜在学校的时光。

此次毕业实习，我学会了运用所学知识解决处理简单问题的方法与技巧，学会了与员工同事相处沟通的有效方法途径。积累了处理有关人际关系问题的经验方法。同时我体验到了社会工作的艰苦性，通过实习，让我在社会中磨练了下自己，也锻炼了意志力，训练了自己的动手操作能力，提升了自己的实践技能。积累了社会工作的简单经验，为以后工作也打下了一点基础。

## 4.2其他意见

尽管在学校认真学习了专业知识，但是当前所掌握的知识面不够广，尚不能轻松胜任软件技术专业岗位工作，因此，尽管在不久的将来走上工作岗位，但我应该将所从事的工作看作是新的学习的开始，只是在实践中学习，才会掌握更多专业知识和技能。

# 五、实习评价

|  |
| --- |
| **企业导师评定意见：** |
| **企业指导老师成绩评定（百分制）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  A（优秀90分以上）、B（良好80-89分）、C（中等70-79分）、D（及格60-69）、F（不及格60分以下）    实习公司盖章：  企业导师签字：  年 月 日 |