**中国科学院信息工程研究所**

**网络协议漏洞分析测试平台实施方案**

上海豌豆信息技术有限公司

2016年3月

# 概述

中科院网络协议漏洞分析测试平台主要由四个部分组成，包括：虚拟化测试云子平台、数据分析子平台、自动化漏洞测试子平台、Fuzzing测试子平台、技术培养学习子平台。

虚拟化测试云子平台，整个项目以EasyCloud私有云为基础，对数据分析子平台、自动化漏洞测试子平台、Fuzzing测试子平台、技术培养学习子平台进行集成，要实现完整的网络协议漏洞验证和分析过程，最终可以输出对某个网络服务软件或系统的漏洞分析报告。

一个典型的测试场景是：发现某系统存在安全问题，将该系统（服务器／虚拟机）接入到测试平台。首先，使用自动化漏洞测试子平台对该系统进行漏洞扫描，发现系统内已经允许的系统或第三方网络服务（FTP、SMTP、RTP等）是否存在已知漏洞，并将扫描结果保存；第二，如果没有发现已知漏洞，使用Fuzzing测试子平台对系统或第三方网络服务进行Fuzzing测试，并将检测结果保存；第三，上述测试过程中，数据分析子平台要能够收集测试过程中的网络协议、syslog日志、snmp日志，收集的网络协议要能够保存为pcap格式（EasyScapy），并能够将被测试主机的性能数据做采集，数据分析子平台会根据收集到的各项报告数据，生成最终版报告。

自动化漏洞扫描子平台，采用Nessus扫描软件，通过Nessus对外开放的Web API接口，自动调用界面上的扫描选项，并可以通过API接口自动扫描和输出XML格式的扫描报告。

Fuzzing测试子平台，采用Peach Fuzzer模糊测试框架，Peach Fuzzer支持通过XML格式自定义网络协议或文件格式，通过编写Peach Fuzzer的XML测试规则，实现FTP、SMTP、流媒体等协议的Fuzzing测试规则。

数据分析子平台，采用现在研发的EasyScapy模块，提供协议数据包的抓取和停止功能；能够调用zibbix的数据接口，抓取测试主机上的性能数据，并能够将数据包显示在页面。

技术培养学习子平台，采用EasyLabs v1.0版本，主要是集成漏洞案例到该学习子平台，需要集成的漏洞案例可包括：Windows RPC协议漏洞、邮件协议漏洞、FTP协议漏洞、IE浏览器漏洞、文件格式漏洞等25个以上常见测试场景。每个漏洞案例需要包含：漏洞环境、漏洞测试工具、漏洞说明（即：实验步骤），上述案例的录入类似实验课程的录入。

# 平台说明

中科院网络协议漏洞分析测试平台采用ATCA大机器为运行的硬件平台，共包括4块硬件主板（即4台服务器）和1块网络交换板。

由于整个平台涉及到子平台之间数据的共享和维护，建议采用共享存储方式部署统一的存储空间，即：虚拟机原始镜像、虚拟机镜像、Nessus扫描结果、Fuzzing模糊测试结果、Pcap抓包结果、性能监控结果，均应统一存储到固定的位置，这个位置的数据可以供平台内的应用程序访问，以便于做数据的集成和处理，并最终生成整合的报告。

由于需要考虑到各子系统间网络的互联互通，建议对网络访问进行统一的规划和处理，即：漏洞扫描子平台运行的Nessus扫描服务，可以访问系统内的任意网络主机；Fuzzing模糊测试子平台运行的测试虚拟机，可以规定访问的IP地址范围，并能够进行分布式Fuzzing测试；Pcap抓包数据分析，需要能够访问到任意网络主机的数据；EasyLabs学习系统需要对外提供访问服务。

在平台上进行测试的系统或网络软件，一个完整的流程如下：

1. 自动化漏洞扫描子平台，允许新建一个扫描任务（唯一标识，可以与测试项目关联），可输入要扫描的IP地址，可以查看当前扫描是否完成；扫描完成时可以将扫描结果导出到共享存储空间，即：可以在新建测试项目下生成扫描任务的结果文件。
2. Fuzzing测试子平台，显示已经部署好的支持FTP／SMTP／流媒体协议（RTP）的Fuzzing测试虚拟机，测试虚拟机分为已经配置好peach测试规则的测试虚拟机和被测虚拟机，被测虚拟机可以按虚拟机模板按需创建Windows和Linux虚拟机，并通过调整测试规则中的被测虚拟机IP地址，可以发起1台或多台测试用虚拟机，对被测主机实施分布式测试。测试完成后，可以通过同步脚本将测试结果同步到共享目录（唯一标识，可以与测试项目关联）。
3. 数据分析子平台，允许新建一个抓包分析任务（唯一标识，可以与测试项目关联），可以将抓包数据保存到共享存储空间，并能够调用API接口显示抓包结果；具有规则库功能，可以根据规则库分析已有数据包，按规则查找数据包中存在问题的协议数据。（按先前的项目需求，协议分析最关键的功能是可以分析第三方网络流量中存在的协议漏洞或潜在攻击，但这个很难实现，目前主要是以使用漏洞规则库中的检查pcap文件中存在的潜在攻击）（需要具有规则库功能，可以将新发现的漏洞触发规则录入到规则库内）
4. 收集以上测试项目下保存下的测试结果，进行统一分析后生成统一的报告，并可以将报告导出为PDF格式。

# 技术路线

网络协议漏洞分析测试平台由五个子平台构成，分别是：虚拟化测试云子平台、数据分析子平台、自动化漏洞测试子平台、Fuzzing测试子平台、技术培养学习子平台。

平台总架构图如下：

*网络协议漏洞分析测试平台总架构图*

虚拟化测试云子平台，负责实现测试环境的创建与统一管理。通过虚拟化的方式将被测应用或产品的服务器、网络架构、客户端等基础设备进行模拟仿真，从而让网络协议漏洞分析测试可以在来自于实际环境的复现场景中进行。虚拟化测试云子平台通过虚拟化技术实现各种测试场景的保存和重复利用，节省了测试流程中环境布置的时间与人力投入，简化并加快了协议漏洞分析与发现的过程。虚拟化测试云子平台负责对外提供接入与输出接口，接入接口供物理设备或第三方网络接入云虚拟化网络；输出接口对外输出虚拟化设备的基础信息与虚拟环境的网络流量。

数据分析子平台负责对各基础设备间进行数据的采集监测，再通过数据分析模块的处理，形成协议分析、流量分析流程，最终通过可视化进行协议、流量的标准化展示。数据分析子平台通过内置的测试流程设定文档和PCAP流量记录，辅助测试结果的技术分析，并将所有重要信息自动收集打包到一个原理性报告中，必要时可将该包发送给第三方进行自动重现与测试结果验证。

自动化漏洞测试子平台，负责实现应用和产品的自动化漏洞测试，挖掘发现已知漏洞，并通过数据分析模块进行漏洞的原理研究。自动化漏洞测试子平台通过采用多个分析测试模块（并联）联用的多路分流设计方案，可以实现对网络级、报文级、应用级的网络漏洞综合分析，确保测试过程全面、可靠。自动化漏洞测试平台可以进行第三方漏洞扫描产品接入，并可以将第三方漏洞扫描产品测试结果融入自动化漏洞测试平台，形成已有技术手段的充分利用。

Fuzzing模糊测试子平台运行于虚拟化测试云平台之上，在无法通过已知手段对漏洞进行挖掘研究的情况下，对应用或产品进行Fuzzing模糊测试，进一步挖掘未知漏洞或安全隐患。Fuzzing模糊测试子平台通过制订模糊测试方法对SMTP、FTP、RTP等常见应用层协议进行Fuzzing测试；同时也可以基于网络协议数据分块特性，具备对未知协议的一定Fuzzing测试能力。Fuzzing模糊测试子平台应支持基于应用的、基于协议的测试。

技术培养学习子平台用于将整个网络协议漏洞分析测试平台相关的业务知识与应用流程进行体系化培训，让新接触的人员能够快速掌握整个业务流程，并能够提高相关漏洞分析技术水平。技术培养学习子平台也支持在网络协议漏洞分析测试平台使用过程中产生的自有技术或经验积累可以通过课程的方式分享延续给其他人员，从而达到知识积累沉淀的目的。

# 实施方案

## 虚拟化测试云子平台

以EasyCloud系统为基础，综合考虑各系统之间的数据共享和网络访问功能，采用共享存储方式统一部署存储空间，采用统一的网络访问控制，保证内部各子平台之间的网络通讯。

目前考虑到的部署方式为：

1. 将虚拟机原始镜像、虚拟机镜像、Nessus扫描结果、Fuzzing测试结果、pcap抓包结果、性能监控结果，应统一存储到固定的位置，这个位置的数据可以供平台内的应用程序访问，以便于数据的集中处理和生成整合报告。
2. 建议将网络设置为各系统之间的互联互通，以便于子平台之间的相互访问。
3. 网络交换机（网络板卡）需要预留外部设备接入的接口，以便于后续使用。
4. 需要考虑Nessus是安装到虚拟机？还是安装到物理机？
5. 需要考虑EasyScapy安装到什么位置？以便于能够对测试过程进行抓包分析。
6. 需要考虑zabbix监控安装到什么位置？以便于获取到系统性能和log日志。

## 自动化漏洞测试子平台

自动化漏洞测试子平台主要是通过在界面上输入扫描IP地址、选择扫描策略，调用Nessus官方提供的REST API接口，自动对目标进行漏洞扫描，并可以在扫描完成后，通过界面上的选项将扫描结果导出到共享存储目录。

Nessus官方提供的API接口已经具备上述功能，可根据实际情况进行功能调整，具体可参考：<https://github.com/tenable/nessrest>。

界面上需要具有的功能：

1. 新建任务按钮，打开新建任务对话框，可以输入扫描IP、选择扫描规则；
2. 启动／停止／删除扫描任务按钮，与API接口对接，实现扫描任务的启动／停止／删除功能；
3. 扫描任务列表，显示当前扫描的IP地址／扫描状态（扫描中／已完成），最右侧有~~同步报告按钮、~~导出报告按钮，报告可同步到共享目录；（报告同步后要在数据库做记录，以便于后续报告的整合。）；具有导出报告功能，可以将报告导出为html／csv等Nessus支持的报告格式；
4. 扫描策略制订，扫描策略预先查看Nessus下定制的扫描策略ID，将扫描策略重新录入一份到该系统，方便在新建任务时直接使用；可以预先在Nessus定制Windows／Linux等系统扫描策略，并在策略中加入对常用网络服务的支持（FTP／SMTP／流媒体等）。

备用方案：

1. 新建扫描任务在Nessus中配置和运行，扫描策略也在Nessus中制订；整个扫描过程由Nessus完成。
2. 界面上有扫描任务列表，显示当前扫描的名称、IP、状态、时间等信息，最右侧有~~同步报告按钮、~~导出报告按钮，报告可同步到共享目录（报告同步后要在数据库做记录，以便于后续报告的整合。）；具有导出报告功能，可以将报告导出为html／csv等Nessus支持的报告格式。

补充方案：

需要具有其他渗透测试工具，部署安装有Metasploit、OWASP ZAP等工具的虚拟机，可以安装1台Kali Linux虚拟机，集成多款渗透测试工具，该虚拟机可以访问所有网络，以便于对其他系统进行测试。

## Fuzzing模糊测试子平台

Fuzzing模糊测试子平台主要由配置好Peach测试规则的多台虚拟机组成，按照支持的默认协议，分别配置支持FTP／SMTP／RTP协议的Fuzzing模糊测试虚拟机，启动虚拟机后即为已经配置好Peach测试规则。

该功能类似“云主机”功能的复制，主要是需求如下：

1. 制订Peach的FTP／SMTP／RTP协议测试规则的3台虚拟机，虚拟机内需要有命令使用的详细说明文档，指导测试人员启动命令进行测试。（即：安装了Peach测试工具的虚拟机，此处的虚拟机为Fuzz虚拟机）
2. 按被测软件的测试环境要求，可以自己调用需要创建何种类型的云主机，并部署为被测软件环境（即：安装了需要进行测试的网络服务软件），安装被测软件的云主机，能够访问共享目录，并将待安装软件同步到该云主机进行安装部署。
3. 上述两个步骤完成后，运行步骤1的测试虚拟机，对步骤2的被测虚拟机进行测试。
4. 注：步骤1的测试虚拟机可复制后开启多个，以实现分布式并行测试的需求。（可以使用EasyCloud内的云镜像功能，复制多个测试用虚拟机）

## 数据分析子平台

数据分析子平台是整合其他几个平台数据的系统，也是该项目中最难实现的部分，主要具备以下几项需求：

1. ~~可收集zabbix采集的设备数据，并采用可视化方式展示在监控范围内的系统性能；（可使用pyzabbix）~~使用现有研发的性能接口
2. 具备数据抓包分析功能，可使用EasyScapy模块的功能，显示当前的抓包数据，并能够对抓包数据管理和分析，实现可视化效果；（功能类似pcap-analyzer）
3. 具备漏洞规则管理功能，可以录入漏洞规则，包括对漏洞规则的增删改查；
4. 具备数据包分析功能，可以将平台本身通过EasyScapy抓取的数据包、第三方导入的数据包，与漏洞规则进行匹配查询，通过数据包分析功能能够发现数据协议中存在的安全漏洞；（可通过分析HTTP协议，识别出SQL注入和XSS跨站的漏洞规则；可根据录入的漏洞规则，在数据包中查找出具有该规则的协议数据）
5. 具有报告整合功能，可以将漏洞扫描、fuzzing测试、协议分析、性能监控等数据进行定制化报告的输出，定制化报告可选择漏洞扫描项目、fuzzing测试项目、协议分析项目等，并按需求定制报告。（报告整合需要综合考虑各类报告的内容和可选项，应该有一个可定制报告的选项页面）

## 技术培养学习子平台

技术培养学习子平台，采用EasyLabs v1.0版本，主要是集成漏洞案例到该学习子平台，需要集成的漏洞案例可包括：Windows RPC协议漏洞、邮件协议漏洞、FTP协议漏洞、IE浏览器漏洞、文件格式漏洞等25个以上常见测试场景。每个漏洞案例需要包含：漏洞环境、漏洞测试工具、漏洞说明（即：实验步骤），上述案例的录入类似实验课程的录入。

其他课程包含的内容有：测试详细流程文档、场景中漏洞隐患的原理介绍、整个网络协议漏洞分析测试平台的使用流程教学课程。