实验七OpenVAS系统实现漏洞扫描

实验介绍

OpenVAS是开放式漏洞评估系统，也可以说它是一个包含着相关工具的网络扫描器。其核心部件是一个服务器，包括一套网络漏洞测试程序，可以检测远程系统和应用程序中的安全问题。其官方网址为：http://www.openvas.org/

OpenVAS 是结构可分为三层：客户层、服务层和数据层，如图：

**1.** 客户层

客户层主要是向用户提供使用接口，它有三种接入方式：Shell命令行方式(OpenVAS CLI)、浏览器方式(Greenbone Security Assistant，服务端口为9392或443)和图形化界面的方式(Greenbone Security Desktop)

**2.** 服务层

服务层分为三个部分：OpenVAS Scanner、OpenVAS Manager和OpenVAS Administrator。

OpenVAS Scanner 提供交流协议OTP (OpenVAS Transfer Protocol)，该协议允许控制扫描的执行。

OpenVAS Manager是把易攻击性扫描和易攻击性解决方案管理集合起来的中心服务。它通过OTP(OpenVAS Transfer Protocol)控制Scanner，并且向用户提供基于XML、无状态的OMP(OpenVAS Management Protocol)用于浏览器方式的接口。它还控制着一个集中存储配置信息和所有扫描结果的SQL数据库(基于sqlite)。

OpenVAS Administrator 是一个命令行工具，或者说是一个完全服务的事务处理后台，它提供OAP(OpenVAS Administration Protocol)用于用户接口，其主要任务是用户管理(user management)和馈送管理(feed management)。

**3.** 数据层

数据层包含两个部分：网络易攻击性测试集(NVT‘s)和一个集中存储配置信息和所有扫描结果的SQL数据库。

实验内容

学习掌握并实现网络安全技术，在Linux系统中配置OpenVAS系统并实现漏洞扫描。

1. 在一台计算机上，基于Linux系统调试配置OpenVAS系统，包括扫描引擎和管理中心的配置。实现管理中心向扫描引擎下发任务、状态上报等管理工作，扫描引擎执行对指定系统的漏洞扫描任务。

2. 实现分布式部署OpenVAS系统，在多台计算机上实现配置管理中心和多个扫描引擎，一个管理中心可控制三个以上扫描引擎完成扫描任务。

3. 对OpenVAS系统的plugin（特征库）的语法进行描述和解析。基于对plugin的语法理解基础上，模拟实现一个plugin。

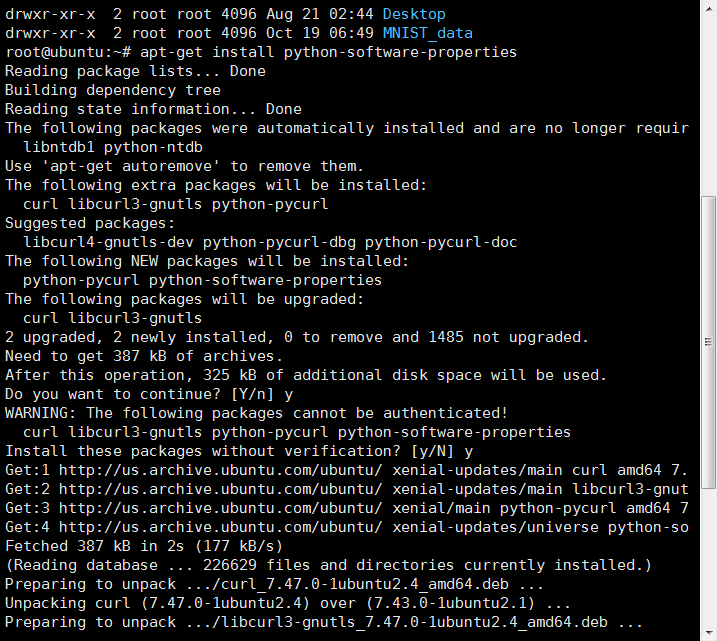
4. 2人组成一组，各组人员自由组合，协商任务分配，避免出现小组间互相抄袭。每人必须承担系统实现的一部分，最终一组完成一个项目。

实验要求

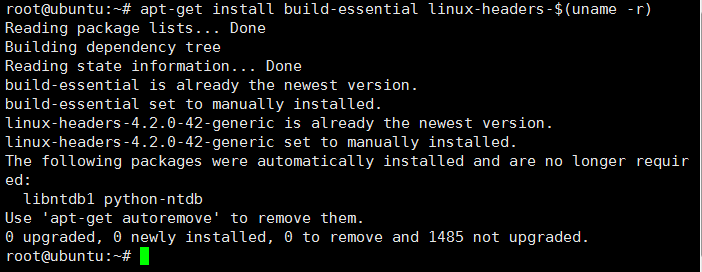
**1.** 安装**OpenVAS**

1) 安装各种依赖包

*sudo apt-get install python-software-properties*

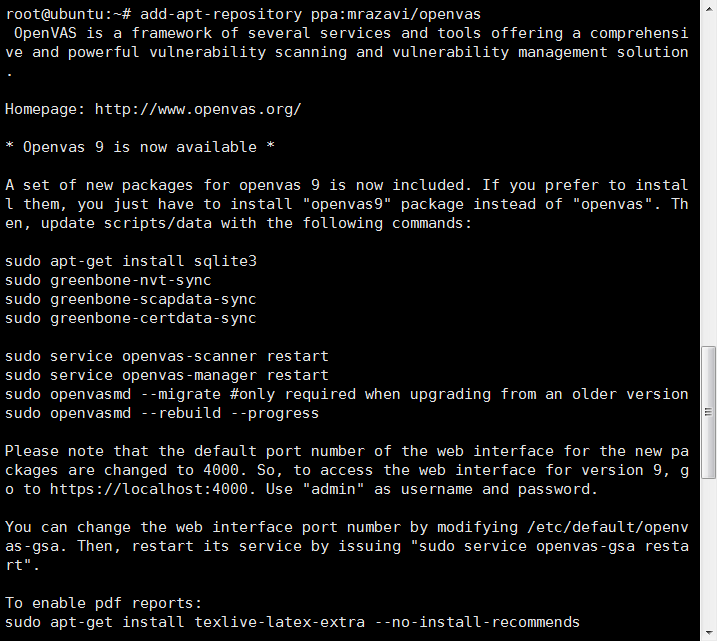


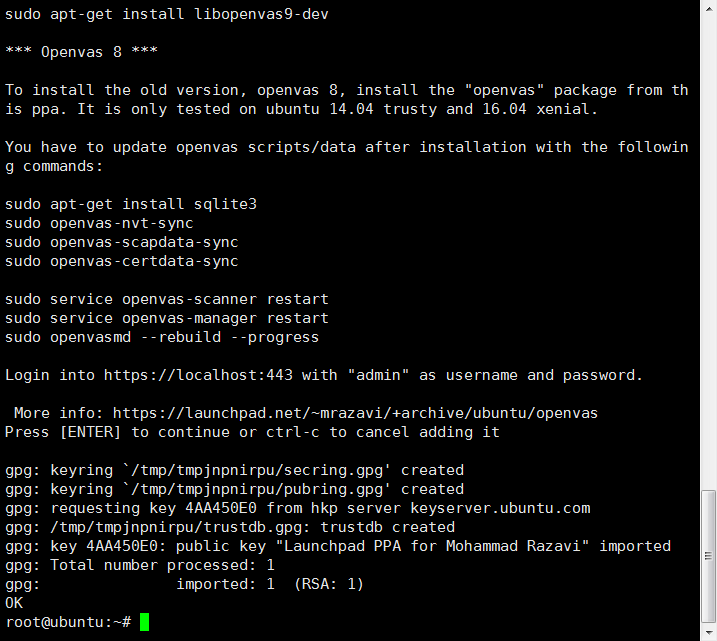
*sudo apt-get install build-essential linux-headers-$(uname -r)*



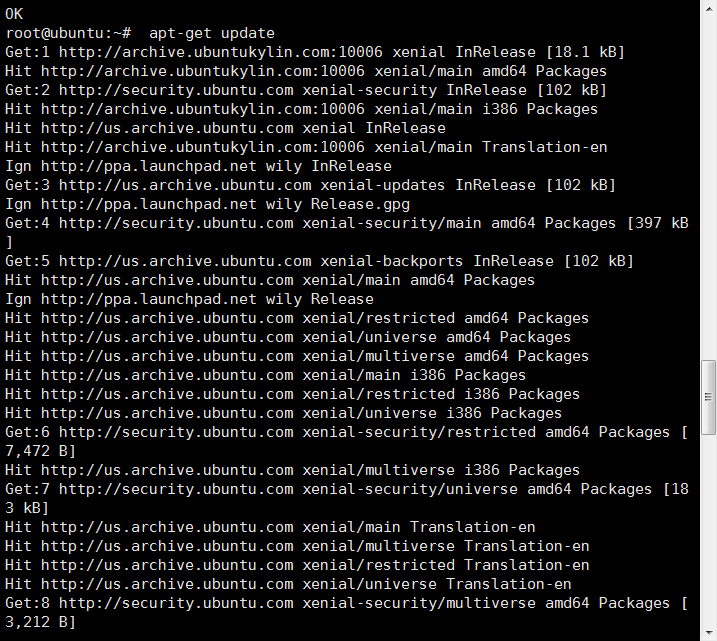
2) 添加repository

*sudo add-apt-repository ppa:mrazavi/openvas*





*sudo apt-get update*



3) 安装openvas

*sudo apt-get install openvas9*

*sudo apt-get install sqlite3*

4) 同步漏洞数据/OpenVAS脚本（下载时间比较长）

*sudo greenbone-nvt-sync sudo greenbone-scapdata-sync sudo greenbone-certdata-sync*

5) 重启扫描器和管理器

*sudo service openvas-scanner restart*

*sudo service openvas-manager restart*

*sudo openvasmd --rebuild --progress*



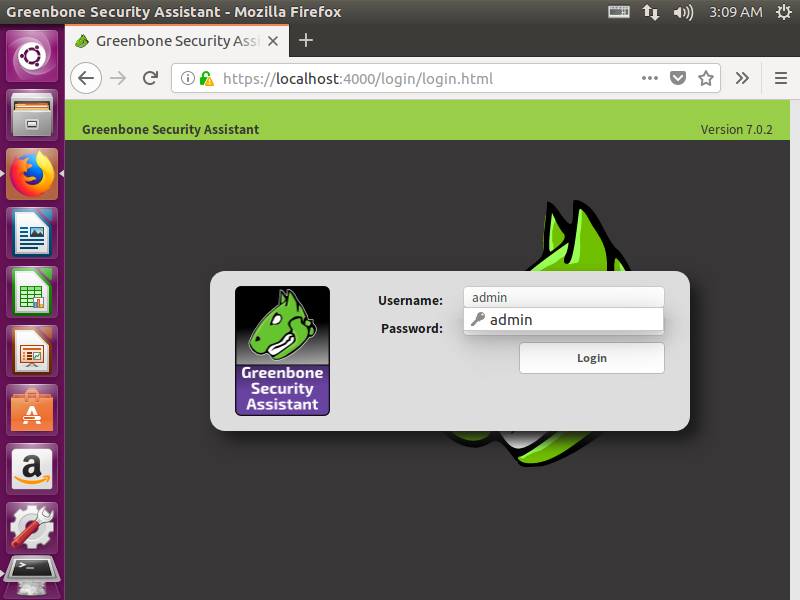
6) 配置可生成PDF报告

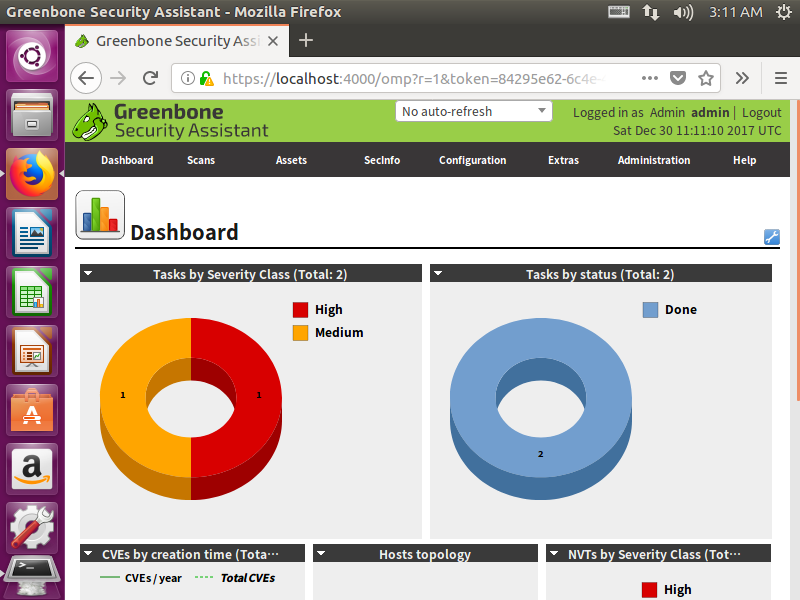
*sudo apt-get install texlive-latex-extra --no-install-recommends*

7) 安装openvas-nasl

*sudo apt-get install libopenvas9-dev*

8) 打开浏览器，访问https://localhost:4000。输入用户名/密码，初始化均为admin。进入OpenVAS主界面。





**2.** 扫描任务

