**安全测试工具之OpenVAS（Server）**

**一． OpenVAS简介**

　　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。

　　用户需要一种自动测试的方法，并确保正在运行一种最恰当的最新测试。OpenVAS包括一个中央服务器和一个图形化的前端。这个服务器准许用户运行 几种不同的网络漏洞测试（以Nessus攻击脚本语言编写），而且OpenVAS可以经常对其进行更新。OpenVAS所有的代码都符合GPL规范。

**建立架构：**

　　OpenVAS是一个客户端/服务器架构，它由几个组件组成。在服务器上（仅限于Linux），用户需要四个程序包：

　　OpenVAS-Server: 实现基本的扫描功能

　　OpenVAS-Plugins: 一套网络漏洞测试程序

　　OpenVAS-LibNASL 和OpenVAS-Libraries: 实现服务器功能所需要的组件

　　而在客户端上（Windows或Linux均可），用户仅需要OpenVAS客户端。

　　Server Scanner:负责调用各种漏洞检测插件，完成实际的扫描操作

　　Manager:负责分配扫描任务，并根据扫描结果生产评估报告

　　Libraries:负责管理配置信息，用户授权等相关工作

**二． OpenVAS安装**

　　Ubuntu Linux安装OpenVAS为例

　　sudo add-apt-repository ppa:mrazavi/openvas

　　sudo apt-get update

　　sudo apt-get

　　install "openvas"

　　Yes

　　sudo apt-get

　　install sqlite3

　　sudo openvas-nvt-sync

　　sudo openvas-scapdata-sync

　　sudo openvas-certdata-sync

　　sudo service openvas-scanner restart

　　sudo service openvas-manager restart

　　sudo openvasmd --rebuild --progress

　　sudo service openvas-gas restart

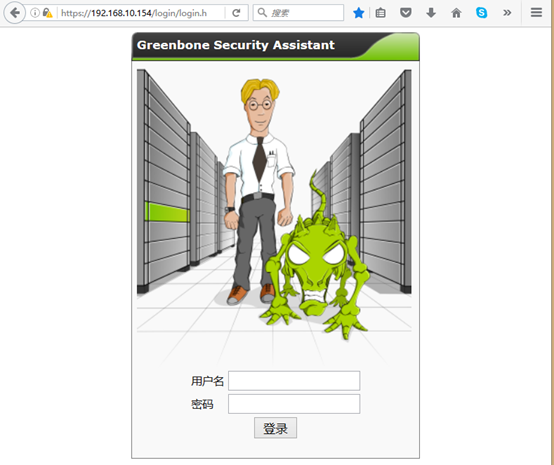
　　这里安装过程需要一点时间，请耐心等待......

**三. OpenVAS使用操作**

　　内部访问地址：https://192.168.10.154/login/login.html

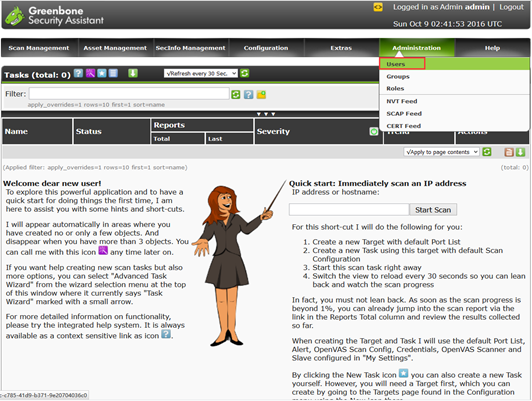
　　外部访问地址：https://openvas.nat123.net/login/login.html

当第一次访问时，可能会出现不安全链接提示，请将此地址添加为安全例外。

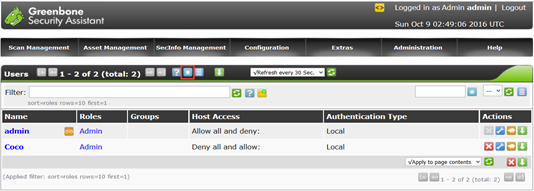


**1.创建用户：**

\*使用ADMIN账号登录系统，看到如下图所示



\*进入Administration>Users如下图所示



　　\*点击上图中图标，进入New User页面，如下图所示

　　填写Login Name和Password

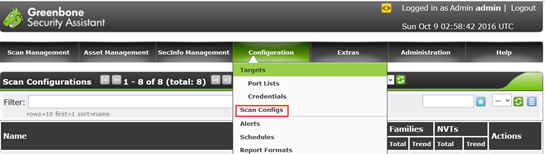
　　选择用户角色（Admin，Guest，Info，Monitor，Observe，User）

点击Create User按钮，新的用户创建完成

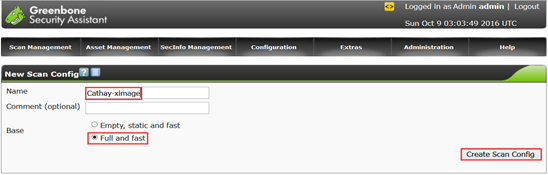


**2.配置Scan Configs**

\*进入Configuration>Scan Configs页面后点击New Scan Config

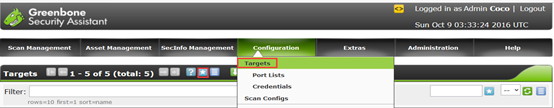


\*New Scan Config:填写Name，选择Base，点击Create Scan Config

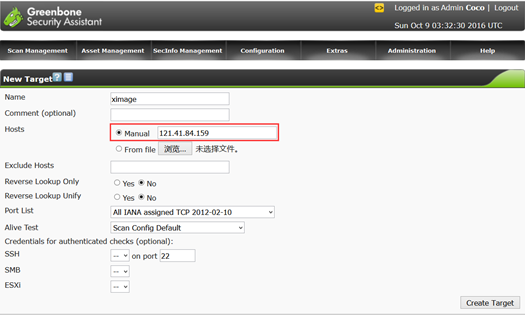


**3. New Target：**

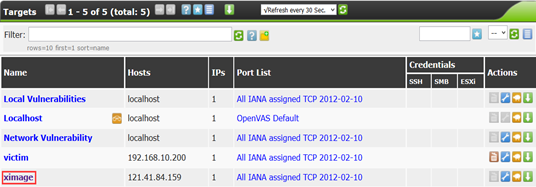
\*进入Configuration>Targets点击进入New Target页面



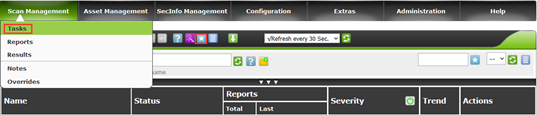
\*这里的Hosts, Manual需要输入\*\*对应的IP地址 121.41.84.159



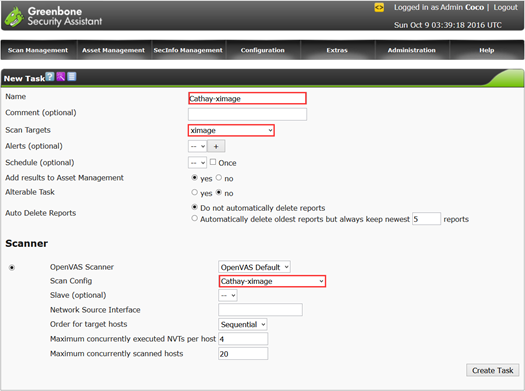
\*创建成功：



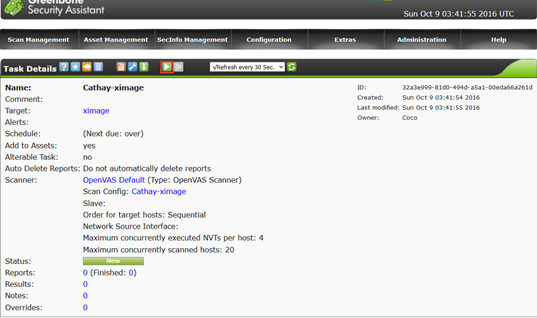
1. **New Task：进入Scan Management>Tasks点击图标New Task**

****

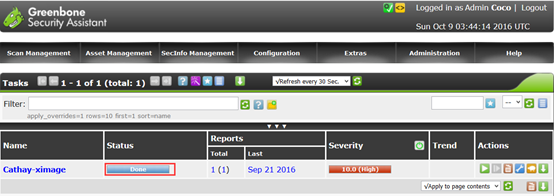
\*填写Name，选择Scan Target（ximage）,选择Scan Config(Cathay-ximage)



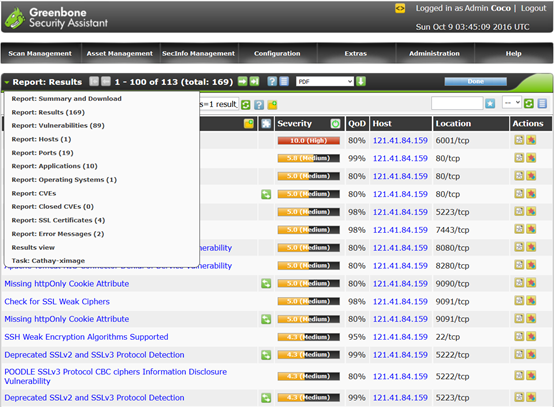
\*Run Task，这里Running的过程需要一段时间，但是在Result数字有变化时可随时查看结果



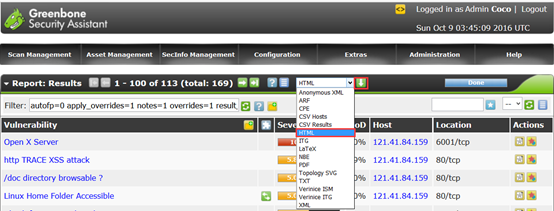
1. **查看结果，当Status为Done是代表已经扫描完毕**



\*点击Done查看结果，如下图所示



\*导出扫描结果报告，可以选择适合的类型下载报告



\*导出Report如下图所示

