
全国大学生开源软件技术竞赛

分析设计说明书

学校名称: 新疆农业职业技术学院

项目名称: 网络安全检测与分析

团队组成: 贾登波 赵银波 柴永强

指导教师: 杨功元 罗晓东 傅峰

联系电话: 0994—2334932

电子邮箱: jdb06gw@xjnzy.edu.cn

填报时间: 2008 年 11 月 22 日

网络安全检测与分析

摘要

网络已经深入到每个人的日常生活之中，网络管理员的责任日益重大。如果一个网络管理员缺乏安全防范意识，没有强大的网络安全检测和分析工具，那么他所维护的网络是极其危险的。即使有相关的工具，但是漫长的安装过程和繁琐的配置，使用起来也十分不便。根据网络安全管理需要，我们针对上述情况制作了基于 Linux 平台的网络安全检测和分析 LiveCD 工具光盘，以便更好地帮助网络管理员、网络安全工程师检测、分析和解决网络安全方面的问题。即使网络管理员到一个新的网络环境进行安全相关的工作，只要启动光盘，不用繁琐的安装、配置即可工作。该工具盘具有如下功能：检测服务漏洞、流量监控、网络监听、端口扫描、路由跟踪、网络病毒查杀。

一、背景和应用领域

Linux 操作系统凭借强大的网络功能，优秀的系统性能和出色的安全性和稳定性，赢得了广大服务器客户的亲睐。但是，任何操作系统都不可能绝对的安全，英国的一家网络安全公司对某一个时期内发生的安全攻击事件进行调查表明：在成功的安全攻击中，对 linux 主机攻击的成功次数在不断上升；调查也指出，问题出在网络管理而不是 Linux 系统本身。Linux 系统虽然相对比较安全，但是如果疏于管理、没有正确的配置，也会发生安全相关的问题。

虽然各种 linux 服务器发行版本自带了一些基本的安全检测工具，但是功能和性能都不能满足要求，与专业化的网络安全工具存在一定差距，远远满足不了网络安全工程师的需要，所以很多网络安全工程师还是希望能有一套功能全面、使用方便的安全检测和维护工具。不过，即使有这样的工具，但是漫长的安装过程和繁琐的配置选项，会让许多用户难以使用。

基于以上背景，经过相关调研工作，我们决定设计、制作一款基于 linux 平台的网络安全检测和分析 LiveCD 工具盘，该产品拥有能够全面检测和分析网络安全的功能，并且省去了繁杂的安装和配置过程。可以直接从光盘启动，使用本 LiveCD 提供的网络安全检测、分析工具。该产品主要提供给网络安全工程师、网络工程师使用，也可供一般的网络用户进行网络安全评估。

二、特点和设计思路

1、作品特点

(1) 方便性

整套工具集中在一张普通的 CD 上，可以随身携带。插入光驱即可运行，光盘启动后，只需进行简单网络地址配置即可使用。

(2) 实用性

该产品拥有检测服务漏洞、流量监控、网络监听、端口扫描、路由跟踪、网络病毒查杀等一整套工具，用户可以根据需要选择相应工具进行网络安全的检测和分析。

2、设计思路

解决实际工作遇到的问题，方便用户使用，是我们设计该产品的基础。以用户为中心是我们设计该产品的理念。

在设计该产品时我们主要考虑到如下问题：

(1) 产品操作的方便性

第一，我们在设计时尽最大努力采用直观的图形化界面进行操作，避免让用户使用复杂的命令工作，即使有命令也尽可能简单。

第二，我们在设计时尽最大努力让用户只需要轻轻点击鼠标就可完成相应的操作。强调操作的简洁、实用。

(2) 产品的实用性

该产品在设计时通过调研分析广大用户需求的基础上，精心选用检测服务漏洞、流量监控、网络监听、端口扫描、路由跟踪、网络病毒查杀等不同网络安全领域的工具，让用户可以根据自己的需要游刃有余的选用 LiveCD 提供的工具进行工作。

(3) 产品系统的最优化原则

第一，在制作该产品时最关键的一个问题就是系统的裁剪问题，我们在设计时只安装与该产品功能相关的安装包，多余的包一个都不安装，以保证该系统的最小化。

第二，在工具选用方面，我们采用的原则是功能相同的采用性能更强大、操作更简洁，界面更友好的工具，绝不重复选用。

(4)产品的稳定性

第一，我们在设计该产品时既要考虑系统的最小化，又要避免一味追求系统最小化而引起系统不稳定的问题。

第二，我们在安装工具包时坚决避免因不同软件冲突而使系统不稳定的情况。

三、运行的硬件环境的要求

经过我们在方正、海尔、联想、惠普、华硕等不同品牌的特定系列机型上进行测试，该 Live CD 运行正常，网络安全相关功能性能可靠、稳定。但由于时间有限，没有做到最广泛的测试，一些特殊平台没有经过测试验证。

该 LiveCD 运行计算机硬件要求：PIII(以上) CPU、128M（以上）内存、光驱一部。

四、功能描述

该LiveCD是针对供网络安全工程师以及网络管理人员使用设计的，它可以检测服务器上运行的各种服务，查看网络流量，捕捉不同协议的包，探测不同的端口，路由跟踪和网络病毒查杀。

1、服务扫描

Nessus是用来检测各种服务漏洞的，它可以扫描出上千种服务的安全隐患，其中包括WWW服务、FTP服务、E-MAIL服务等常用服务。

Nikto专门用来检测web服务器，非常专业，扫描结果非常详细。

2、网络流量监控

Ntop可以查看网络流量，它可以细微到某一台计算机的不同协议的数据包所占用的带宽。可以进行局域网各种网络信息的扫描收集，为用户提供各种网络基础信息。

(2) 网络监听

Wireshark是一款功能强大的协议分析和监听软件，可以通过设置相关规则来过滤网络上的数据包。结合交换机端口镜像，可以对整个网络的数据进行捕捉、分析。找出异常的数据包，进行网络病毒定位、故障分析等工作。

(3) 端口扫描

Nmap是一款扫描软件，它最主要的功能是探测本机或远程服务器上开放的服

务和端口。为使用者提供服务器上运行的服务的相关信息，为弥补相关漏洞做准备。

（4）路由跟踪

Traceroute、VisualRoute可以用来进行路由跟踪，定位网络节点故障、分析网络节点故障原因。

（5）网络病毒查杀

我们还设想做网络防火墙和当今流行网络病毒（像现在比较流行的arp病毒）定位、查杀的功能，但由于时间和技术等方面的原因，我们的结果和设想还是有一定的差距的，如果有时间，我们会继续完善。

这套LiveCD是基于RedFlag-Workstation3.0制作，但并不意味着只可以检测linux平台的机器，它完全可以检测使用各种平台的主机，包括采用Windows系列操作系统的主机。

五、工作原理

该产品是对网络安全进行检测和分析，这就要确保该LiveCD启动后，网络能够正常使用，这样才能使用各种安全检测和分析工具。

本LiveCD使用的是通过网络远程检测目标网络或本地主机安全性、脆弱点的技术。通过网络安全扫描，系统管理员能够发现所维护的各种服务器开放的服务，并对其进行漏洞、脆弱性检测。

网络安全扫描技术采用积极的、非破坏性的办法来检验系统是否有可能被攻击崩溃。它利用了一系列的脚本模拟对系统进行攻击的行为，并对结果进行分析。这种技术通常被用来进行模拟攻击实验和安全审计、分析。网络安全扫描技术与防火墙、安全监控系统互相配合就能够为网络提供很高的安全性。

一次完整的网络安全扫描分为3个阶段：

（1）第1阶段：发现目标主机或网络。

（2）第2阶段：发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务以及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。

（3）第3阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。

我们使用了各种网络安全扫描技术，包括有PING扫描（Ping sweep）、操作系统探测（Operating system identification）、如何探测访问控制规则（firewalking）、端口扫描（Port scan）以及漏洞扫描（vulnerability scan）等。这些技术在网络安全扫描的3个阶段中各有体现。

该产品中所有的工具是利用TCP、UDP、ARP等网络协议原理与网络安全风险、威胁特性进行检测和分析工作。其中，Nessus是基于C/S(服务器端和客户端)模式工作的网络漏洞、脆弱性检测工具。Nikto是专业的WEB漏洞扫描工具，其工作需要perl环境。Wireshark是网络数据包捕捉和分析工具，需要PCAP支持。NTOP是网络流量分析，网络信息收集工具。Nmap是Linux下最强大的端口扫描工具。

六、体系结构和关键技术点

1. 体系结构：

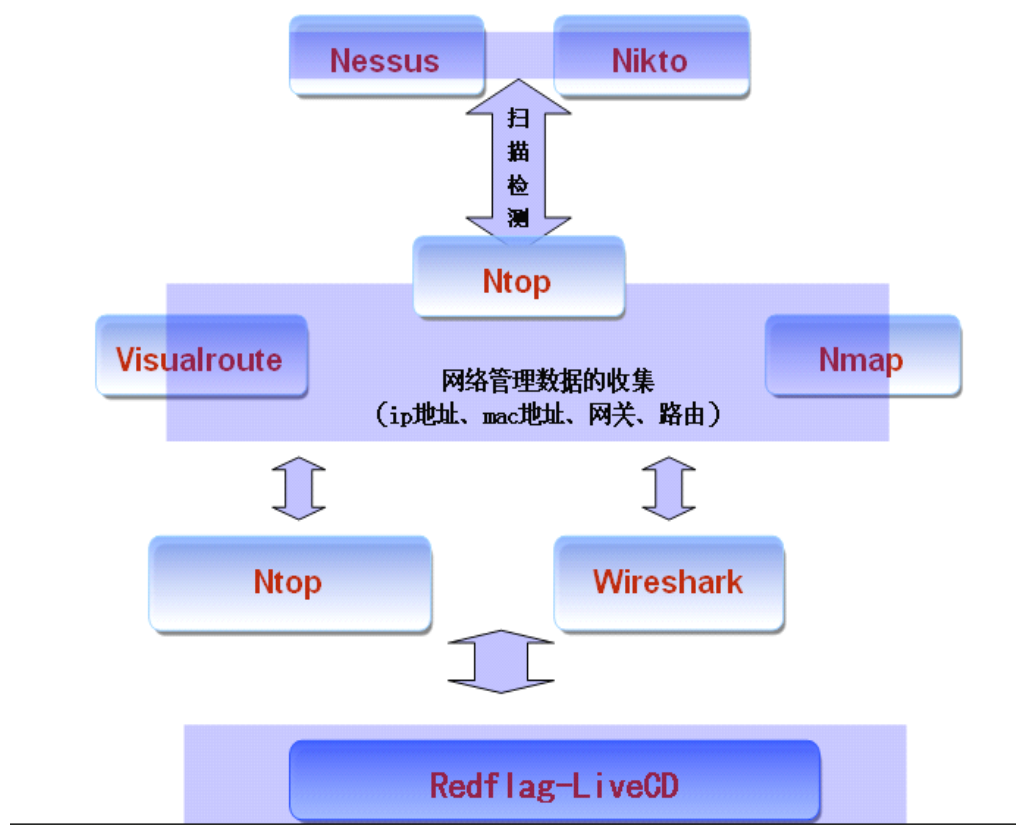


图 1：网络安全检测分析 Live C D 体系结构

2. 关键技术点：

(1) 系统裁减及 live-vcd 的制作

Live C D 系统的裁减过程，即可以是完全安装 Asianux 3.0，进入系统后，再卸载模块；也可以在安装的时候，筛选需要的包，裁减不需要的模块。这两种

方法各有利弊：采用第一种方法，前期工作很少有包依赖关系的困扰，而后期裁减模块时，包依赖关系的问题就会突显出来，很可能一个小小的失误就导致系统的崩溃。采用第二种方法，在安装系统筛选包的过程中，可能会因依赖关系而把不需要的模块也安装上，并且在中间安装工具软件时可能由于依赖关系又装一些其它的软件包，但这种方法在后期可直接进行 CD 封装。我们从自身条件出发，最终采用第二种方法裁减系统包。

由于初期我们对系统包不太了解，所以只能一遍一遍地测试，这种方法虽然很慢，但每一次的测试都使我们更近一步目标。刚开始，我们只能“见名之意”地挑选一些我们需要的包，并利用 Google 进行搜索相关资料。第一次我们做的系统很小，才 800 多兆，这是失败的第一次，因为根本就没有图形化界面。进行第二次安装时，我们静下心来思考，肯定是第一次安装时图形化界面所需的包我们没有选或者没有选全。这次在选包的时候，我们把 kde 完全选择，base-X 完全选择，这次果然有图形界面了但系统要要比第一次庞大得多。前面几次我们就反反复复只为了图形化系统而定制软件包，最后总算找到要有图形界面而必需的最基本包，即 base-X 中的包含 X-org 的软件包。再加上中文支持和浏览器，前面最初安装的图形化系统达到了 1.3G。后来在装我们所选的工具包时，需要有 gcc 环境，我们又不得不重新配置系统。不过，此时，对于我们来说这并不难，我们很容易地在 Development 中找到了 gcc 相关软件包，并且选择了与之有关的 C 函数库。这次安装 tar 包软件基本上没什么问题了，等所有工具安装好之后，想到 gcc 环境已经没有必要了，就决定卸载 gcc，可出现了依赖关系，只卸载了部分 gcc 软件包。就在我们为此发愁的时候，指导老师罗老师来了，他告诉我们，其实我们开始根本没有必要构建 gcc 环境，完全可以在完全安装的系统上安装我们的工具，然后再把安装好的文件复制到我们裁减后的系统上，再简单的设置一下就行。此法给我们节省了很多时间，也避免了许多麻烦。至此，模块裁减算是结束。

(2) live-cd 的封装。按照红旗杯站点上提供的方法，我们封装的 live-cd 根本运行不起来。经过分析，我们想到原因可能是我们系统的问题，站点上提供的方案应该是在完全安装的系统上可以成功，而我们的系统则卸载了很多我们不需要的模块。所以再一次封装，安装 2.6.24 版本的内核的内核时，我们去掉了

参数--nodeps 和--force, 果然如我们猜测的那样, 是我们系统的问题, 报错信息提示了很多依赖包, 根据那些包名, 我们在镜像光盘上找, 最终找到下面这些依赖包: glib2-devel-2.12.3-2.i386.rpm、libdhcp4client-3.0.5-5.1AX.i386.rpm、libdhcp4client-devel-3.0.5-5.1AX.i386.rpm、libdhcp6client-0.10-33.1AX.i386.rpm、libdhcp6client-0.10-33.1AX.i386.rpm、libdhcp-1.17-1.i386.rpm、libdhcp-devel-1.17-1.i386.rpm、libnl-1.0-0.10.pre5.4.i386.rpmlibnl-devel-1.0-0.10.pre5.4.i386.rpm、pkgconfig-0.21-1.i386.rpm、pkgconfig-0.21-1.i386.rpm、glibc-headers-2.5-12.1AX.i386.rpm、glibc-devel-2.5-12.1AX.i386.rpm、e2fsprogs-devel-1.39-8.i386.rpm、e2fsprogs-1.39-8.i386.rpm。这些包安装上之后, 安装新内核就没有问题了, 但封装还是有问题。最后指导老师傅老师给出了解决方案, 原来我们没有装 squashfs 和 aufs 模块, 只有装了这两个模块才能制作 live-cd。这两个模块安装了之后就可以制作了。

(3) 网络安全检测和分析技术。通过对计算机网络或计算机系统内的若干关键点收集信息并对它们进行分析, 从中发现是否有违反安全策略的行为和被攻击的迹象, 发现各种应用程序、服务的漏洞, 以提高系统管理员的安全管理能力, 及时对系统进行安全防范, 及早地发现系统漏洞, 并进行升级补丁。利用网络数据包捕捉工具, 对网络中的数据包进行分析, 发现各种网络攻击行为。例如当前流行的 ARP 欺骗工具, 能够发现并定位发起 ARP 欺骗的计算机, 对其进行处理。利用流量分析工具, 分析网络的流量信息, 发现非法访问和异常流量, 对网络进行监控, 提高网络性能和安全性。

七、功能模块设计

这套LiveCD主要分五大功能:服务扫描、流量监控、数据包捕捉、端口扫描、路由跟踪等。

(一) 服务扫描

服务扫描主要选用了两个工具, 分别是Nessus和Nikto, 这两个工具都有各自不同的用途。

1、Nessus

Nessus是C/S模式结构, 必须安装服务器端和客户端才能使用。首先打开客户端后, 需要用帐号和密码和服务端建立连接(需要提前在服务器端申请帐号);

其次通过服务器端对目标服务器上运行的服务进行安全扫描检测。Nessus功能十分强大，它支持插件功能，一共有两万多个插件，并且不断在更新。支持扫描非常全面，当最后扫描完毕后，会生成一份详细的检测报告，供使用者进行分析、处理。

实例分析：

①双击桌面上的Nessus图标启动它。依次按照提示的步骤进行操作。

②依次打开“File”——“Scan Assistant”来确定扫描目标。

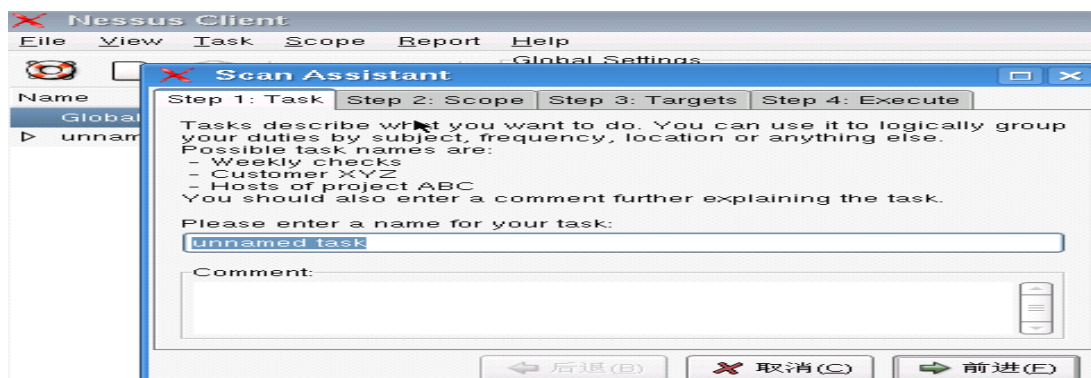


图2：打开Nessus输入扫描任务的名进行扫描

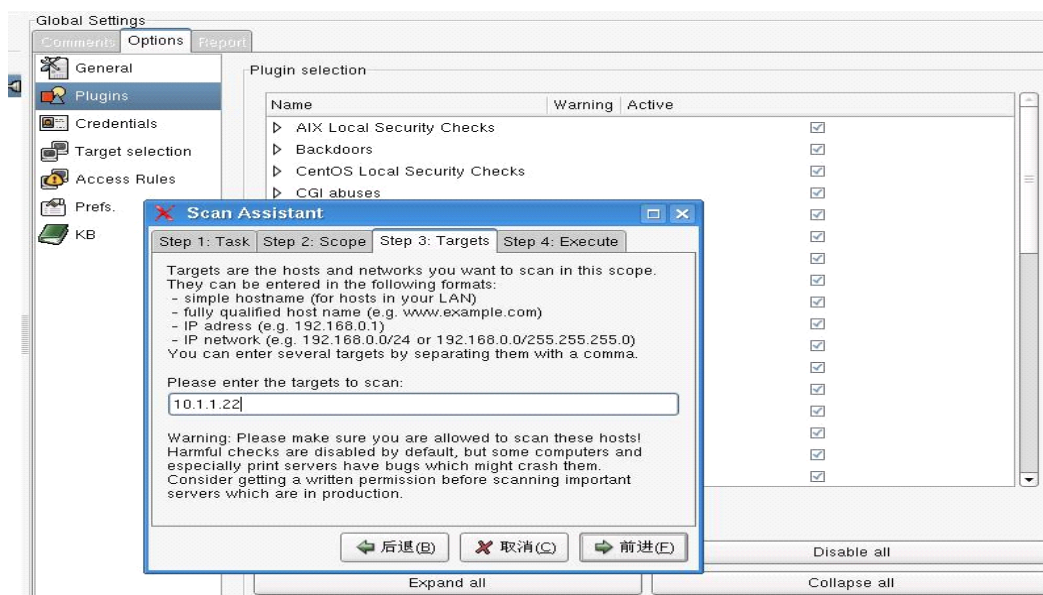


图3：输入扫描目标服务器的名称

③连接Nessus服务器端，输入用户名和密码。



图4：输入用户名和密码

④最后生成检测报告

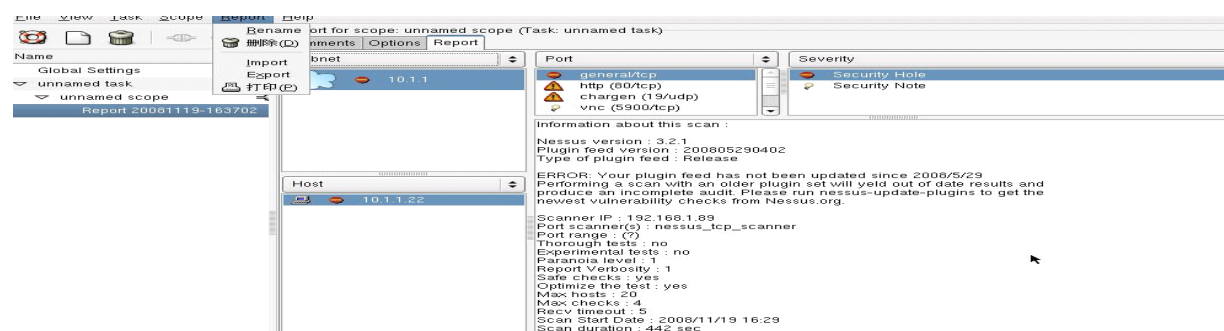


图5：生成检测报告

2、Nikto

Nikto是一款开放源代码的、功能强大的web扫描评估软件，可以扫描指定主机的web类型、主机名、特定的目录、特定的CGI漏洞、返回主机允许的http模式等，可以及时的检测出网站的安全隐患。由于在字符界面下工作，所以用起来不太方便，要加很多的参数。最常用的参数有-h，后接目标服务器IP地址；-p，后接端口名；-o，后接文件名，可以为扫描报告指定一个输出文件。参数很多，可以用--help来查看。

实例分析：

假设要扫描IP为10.1.1.5的WEB服务器，则需在用户终端输入如下内容。

```
[root@localhost nikto]# perl nikto.pl -h 10.1.1.5 -p 80
- Nikto v2.03/2.04
+ Target IP:          10.1.1.5
+ Target Hostname:    10.1.1.5
```

```

+ Target Port:      80
+ Start Time:      2008-11-21 0:44:00
+ Server: Microsoft-IIS/6.0
+ No CGI Directories found (use '-C all' to force check all

```

以上是对web服务器10.1.1.5进行扫描检测的部分摘要，可以看出主机10.1.1.5基于Microsoft-IIS/6.0的web服务器。

也可以使用nikto.sh脚本，按照提示输入扫描目标的IP地址和端口进行扫描，扫描结果会放入同目录下的nikto.txt文档，最后会自动打开该文档供使用者查看。

(二) 流量分析 (Ntop)

Ntop是一款网络流量分析软件，它可以直观的将网络使用情况和每个节点计算机的网络带宽详细地显示出来。Ntop在监测网络数据传输、排除网络故障方面有着不可替代的作用，可以通过分析网络流量来确定网络上存在的各种问题，如瓶颈效应或者性能下降。Ntop 不仅可分析网络流量，而且它还可以记录网络通信的时间和过程，自动的识别网络中的有用信息和你所使用的网络系统。它还可以确定出哪些通信量属于某个特定的网络协议，占主要通信量的是那些主机，各自通信的目标是哪些主机，各主机间数据包传递的时间间隔等。Ntop基于web网页模式来监测网络流量，并且图形直观、简洁，十分容易使用。

实例分析：

①双击桌面上的ntop图标，出现如下界面：

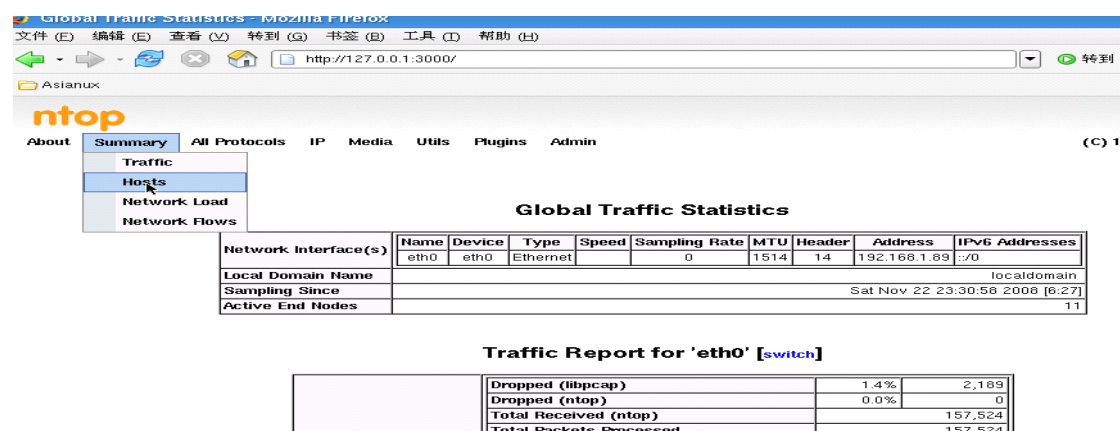


图6: ntop运行界面

②选择summary下的hosts对网络进行监控，(hosts表示显示各台主机的流量

状况，traffic表示整体的网络流量状况，network load表示当前的网络负载，network flow表示整个网络的流量情况）如下图：

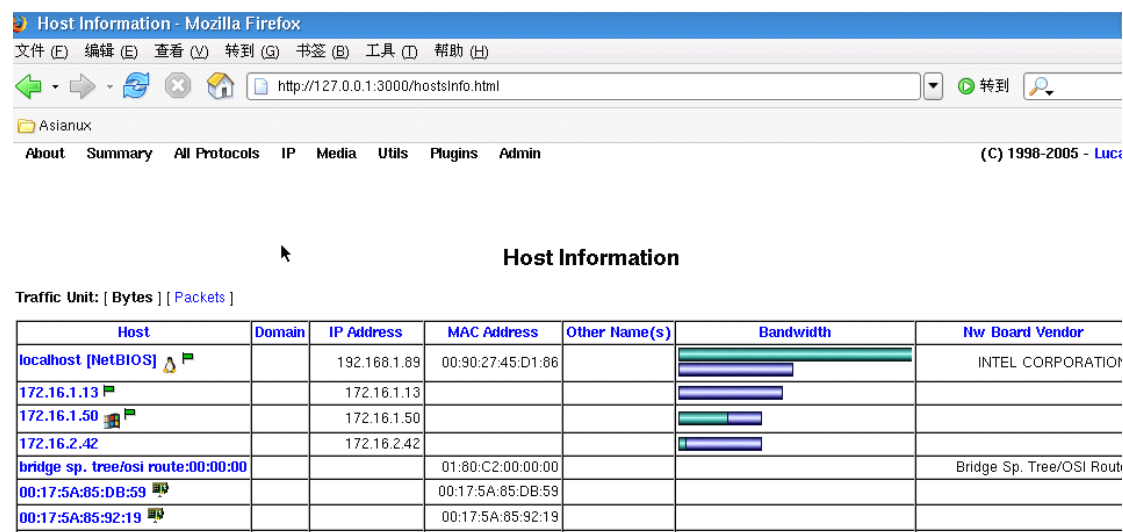


图7：选择summary下的hosts选项进行分析

（三）数据包捕捉分析（Wireshark）

1、wireshark 简介

Wireshark 是一款功能强大的网络协议分析、数据捕获工具，可以在 Linux、Solaris、SGI 等各种平台运行。可以在一个共享的网络环境下对数据包进行捕捉和分析，而且还能够自由地为其增加某些插件以实现额外功能。在用 Wireshark 截获数据包之前，应该为其设置相应的过滤规则，可以只捕获感兴趣的数据包。Wireshark 使用与 Tcpdump 相似的过滤规则，并且可以很方便地存储已经设置好的过滤规则。要为 Wireshark 配置过滤规则，首先单击“Capture”选单，然后选择“CaptureFilters...”菜单项，打开“CaptureFilter”对话框。

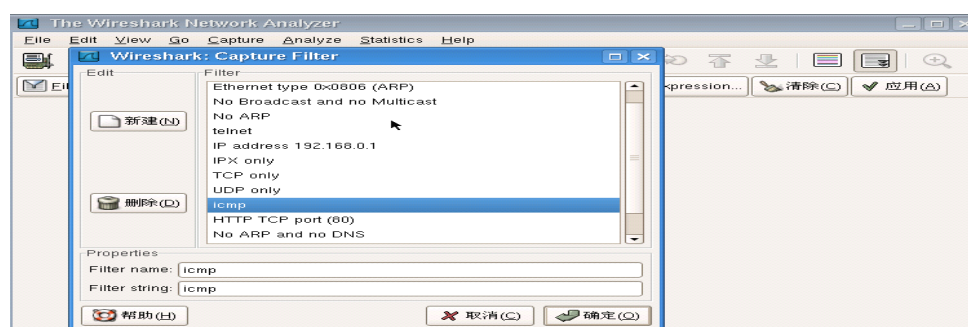


图8：“CaptureFilter”对话框

你可以根据需要设置过滤规则来捕获有用的数据包。过滤规则设置好后，需要选择接口，也就是你要捕捉的那个接口，还是在“Capture”选单里面，第一

项“Interfaces”，确定好后就可以捕捉你感兴趣的包。

No.	Time	Source	Destination	Protocol	Info
8274	174.14202	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8275	174.14230	192.168.1.89	172.16.1.241	TCP	5906 > stgxfws [PSH, ACK]
8276	174.14290	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8277	174.15002	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8278	174.15801	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8279	174.16599	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8280	174.17402	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8281	174.17407	192.168.1.89	172.16.1.241	TCP	5906 > stgxfws [ACK] Seq=1
8282	174.18203	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8283	174.19002	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8284	174.20597	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]
8285	174.21402	172.16.1.241	192.168.1.89	TCP	stgxfws > 5906 [PSH, ACK]

图9: Wireshark扫描结果

2、数据包捕捉分析

Wireshark 可以进行网络数据包的分析、检测，由于现在绝大部分都是交换网络，需要在交换机上配置端口镜像才能捕捉到局域网内的所有数据包进行分析。利用 wireshark，可以查找网络故障、分析病毒传播途径、确定网络病毒位置。

以思科交换机为例，cisco 的端口镜像叫做 SWITCHED PORT ANALYZER，简称 SPAN，创建端口镜像过程如下：

第一步：创建端口镜像源端口

monitor session session_number source interface interface-id [,|-] [both|rx|tx]

(1) session_number, SPAN 会话号，2950、3550 思科系列交换机一般支持的本地 SPAN 最多是 2 个，即 1 或者 2。

(2) interface-id 源端口号，[,|-]源端口接口符号，即被镜像的端口，交换机会把这个端口的流量拷贝一份，可以输入多个端口，多个用“,”隔开，连续的用“-”连接。

(3) [both | rx | tx]，可选项，是指拷贝源端口双向的(both)、仅进入(rx)还是仅发出(tx)的流量，默认是 both。

第二步：创建 SPAN 目的端口

monitor session session_number destination interface interface-id [encapsulation {dot1q [ingress vlan vlan id] | ISL [ingress]} | ingress vlan vlan id]

(1) interface-id 目的端口，在源端口被拷贝的流量会从这个端口发出去，端口号不能被包含在源端口的范围内。

(2)[encapsulation {dot1q | isl}], 可选, 指被从目的端口发出去时是否使用 802.1q 和 isl 封装, 当使用 802.1q 时, 对于本地 VLAN 不进行封装, 其他 VLAN 封装, ISL 则全部封装

第三步: 在 wireshark 中开始捕捉数据包, 设置 filter 针对特定应用进行数据过滤, 完成分析工作。如现在局域网流行的 ARP 攻击, 可以设置 filter 定位 arp 病毒攻击源, 然后进行处理。其 filter 设置如下:

```
arp.opcode=0x2
```

(四) 端口扫描 (Nmap)

Nmap 是一款扫描软件, 它可以对不同的端口和服务进行扫描。根据扫描信息, 可以分析出服务器的安全问题。Nmap 可以扫描一个主机, 也可扫描一个网段 (192.168.2.2/24 或者 192.168.2.*或 192.168.2.1-254), 在实际扫描中, 可以根据不同的需要加上不同的参数。它有图形和文本两种扫描界面。

①图形界面:

双击桌面上的 nmap 会弹出如下窗口

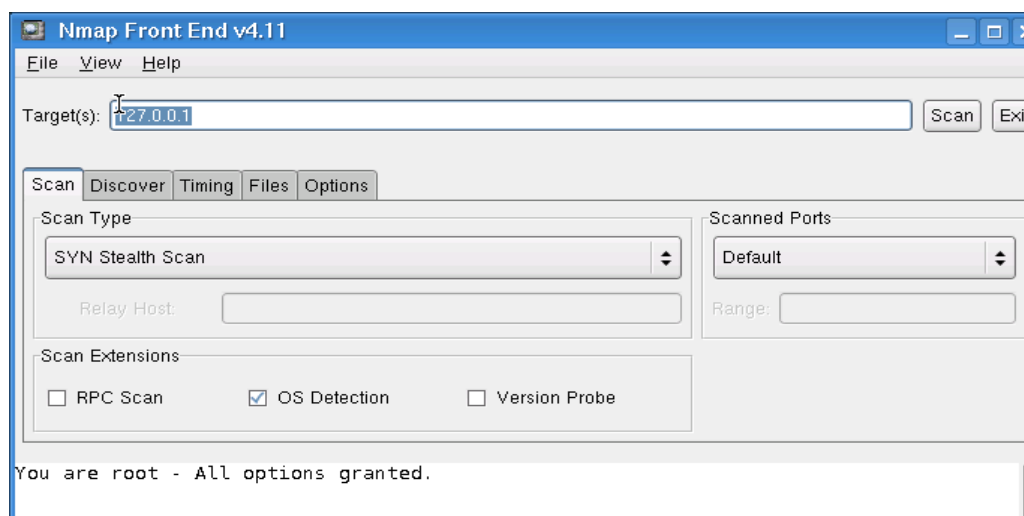


图10: 输入要扫描的主机IP

在 scan 类型中选择你要扫描的类型后, 在 Targets 一栏输入你要扫描的主机 IP 即可。(如果你要扫描一组主机可输入 10.1.1.1-8 这种格式, 如果你要扫描一个网段可输入 10.1.1.0/24 这种格式。) 然后点击 scan 即可进行扫描。

② 文本界面

```
[root@localhost ~]# nmap -sT 192.168.1.89
```

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2008-11-19 12:52
```


CST

Interesting ports on 192.168.1.89:

Not shown: 1660 closed ports

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

22/tcp	open	ssh
--------	------	-----

139/tcp	open	netbios-ssn
---------	------	-------------

445/tcp	open	microsoft-ds
---------	------	--------------

1241/tcp	open	nessus
----------	------	--------

3000/tcp	open	ppp
----------	------	-----

5801/tcp	open	vnc-http-1
----------	------	------------

..... (参数-sT表示基于tcp的扫描方式)

以上只是对测试主机192.168.1.89进行了简单的扫描，可以看到它开启了ftp、nessus等服务。

八、相关技术比较和分析

Windows 系统下的网络安全检测与分析工具类型比较多，操作简洁，简单实用，但是大多数工具只能在 windows 系统下运行，并且大部分是商业软件。对于中小企业、普通网络管理员负担较大。目前，没有哪个系统将不同功能的工具集成到一块，集成到一张光盘，不许安装、配置就能正常使用。

该产品与其他系统相比较，有如下特点：

1、该产品中的工具进行检测和分析的主机不受操作系统的限制，也就是说linux、windows、unix 等操作系统都能被扫描检测。

2、该产品中的工具都是开源的，可以自由传播。网络安全检测和分析功能强大，某些方面设置强于一般商业软件。

3、该产品的集成化比较高，所选工具全面，涵盖网络安全检测和分析的不同方面，但各个工具都是同类型中功能最强大、最容易使用的。

4、所选工具既简单实用，符合网络管理人员的需求；又专业化程度高，符合网络安全工程师的需求。

5、该工具操作简单，不用等待漫长的安装和进行繁杂的配置就能使用，只

需从光盘启动即可。

九、总结

该产品是在调研的基础上,按照网络安全工程师和网络管理员的工作需求制作的。该LiveCD是针对供网络安全工程师以及网络管理人员使用设计的,它可以检测服务器上运行的各种服务,查看网络流量,捕捉不同协议的包,探测不同的端口,路由跟踪和网络病毒查杀。其中关键的技术是系统裁剪和LiveCD的封装技术和网络安全检测和分析技术。该产品的优点有:进行检测和分析的主机不受操作系统的限制;不用等待漫长的安装和进行繁杂的配置就能使用;既简单实用,又符合专业化程度高;工具全面,功能齐全;工具都是开源产品,功能强大能够满足要求。

附录:

(1) 组员信息:

组员	性别	班级	联系方式	分工
贾登波(组长)	男	06 高职网络	597739418@qq.com	方案规划, 系统模块裁减
赵银波	男	06 高职应用	641359778@qq.com	工具软件选择、安装
柴永强	男	07 高职网络	645350192@qq.com	工具软件选择

(2) 软件信息:

我们所选的软件均为开源免费软件,版权归原作者所有。下面为软件的出处。

Wireshark	http://www.wireshark.org
Nikto	http://www.cirt.net/nikto/nikto-current.tar.gz
Nessus(服务器端)	http://www.nessus.org/
Nessus(客户端)	http://www.nessus.org/
Ntop	http://www.ntop.org/

(3) 参考文献

- 【1】《管理员必读》——网络安全第二版 作者:王达 电子工业出版社 2007.6
- 【2】《网络安全实战详解》(企业专供版) 作者:张敏波 电子工业出版社 2008.5
- 【3】《网络安全评估》 作者:麦肯兰勃(美) 中国电力出版社 2006.1