

网络安全检测和分析产品说明书

这套LiveCD主要用来帮助网络安全工程师和网络管理员检测和分析网络中的安全漏洞。分五大功能:服务扫描、流量监控、数据包捕捉分析、端口扫描等。

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，这里已申请好了账户为root，密码是123456）；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，它仅插件就两万多个，扫描非常全面；最后扫描完毕后，会生成一份分类详细的检测报告。

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。

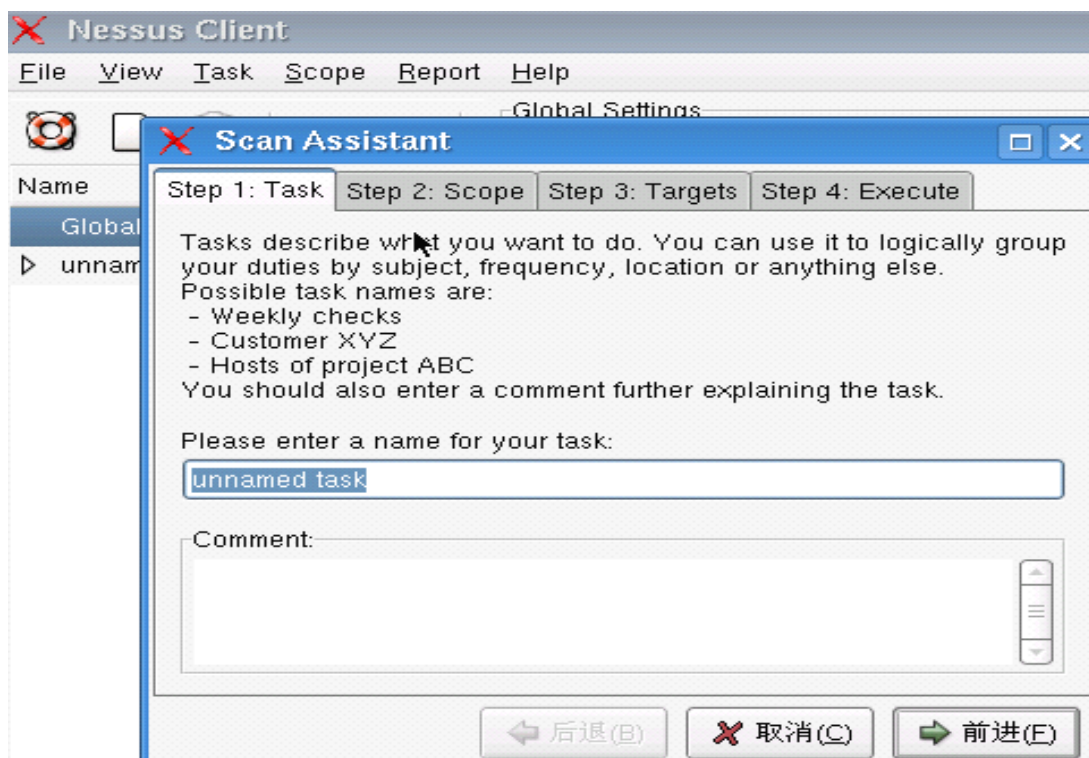


图1 输入扫描任务的名称

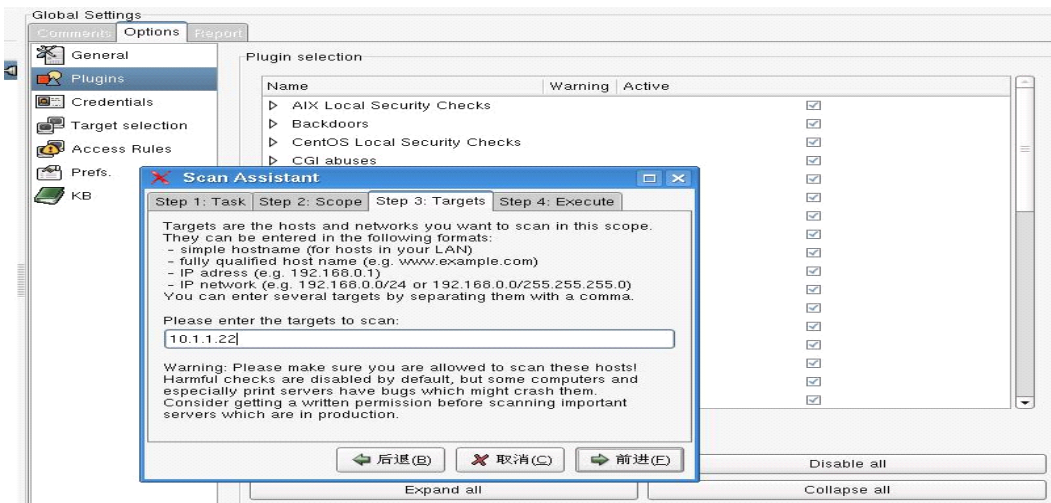


图2 输入扫描目标服务器的名称

③连接Nessus服务器端。

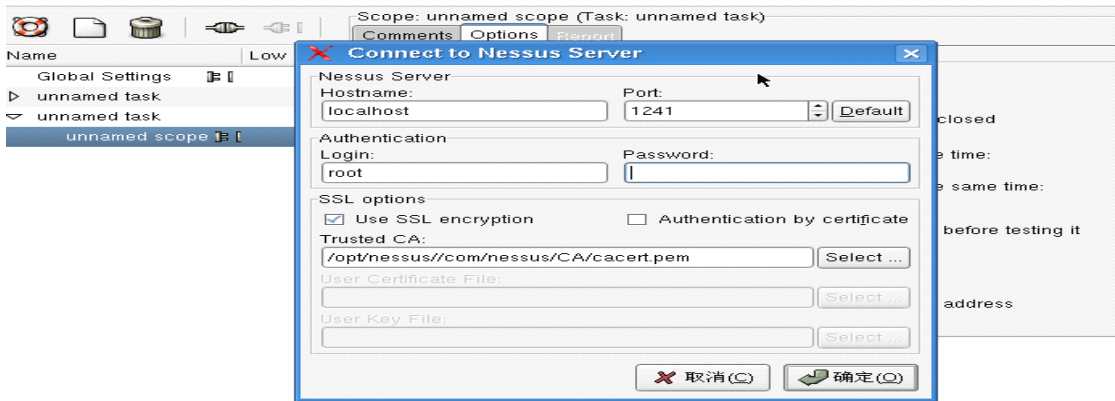


图3 输入验证信息

④生成检测报告

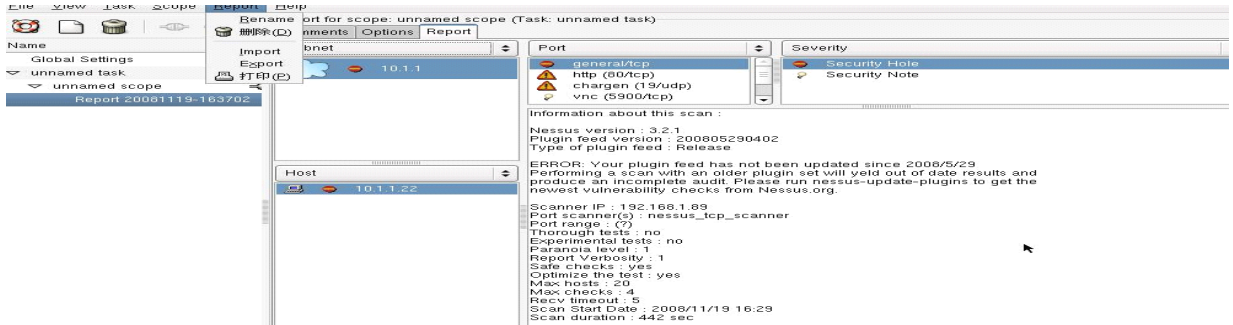


图4 生成检测报告

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。

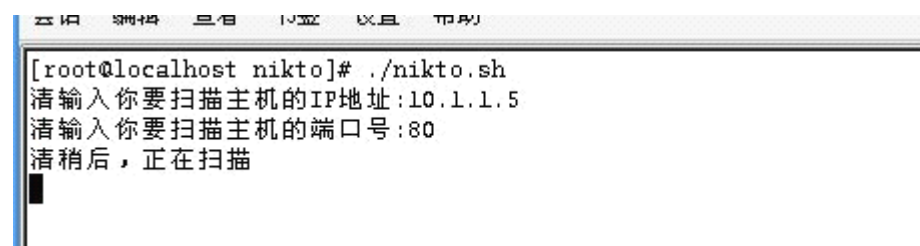
实例分析：

双击桌面上的Nikto图标，会进入nikto所在的目录，用命令ls查看。

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。对于上面这条命令，你可以直接用./nikto.sh来执行，当然对于其它复杂的命令，还需要自己输入命令和参数。



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，并且有直观分析图，非常容易使用。

实例分析：

①双击桌面上的ntop图标，出现如下界面：

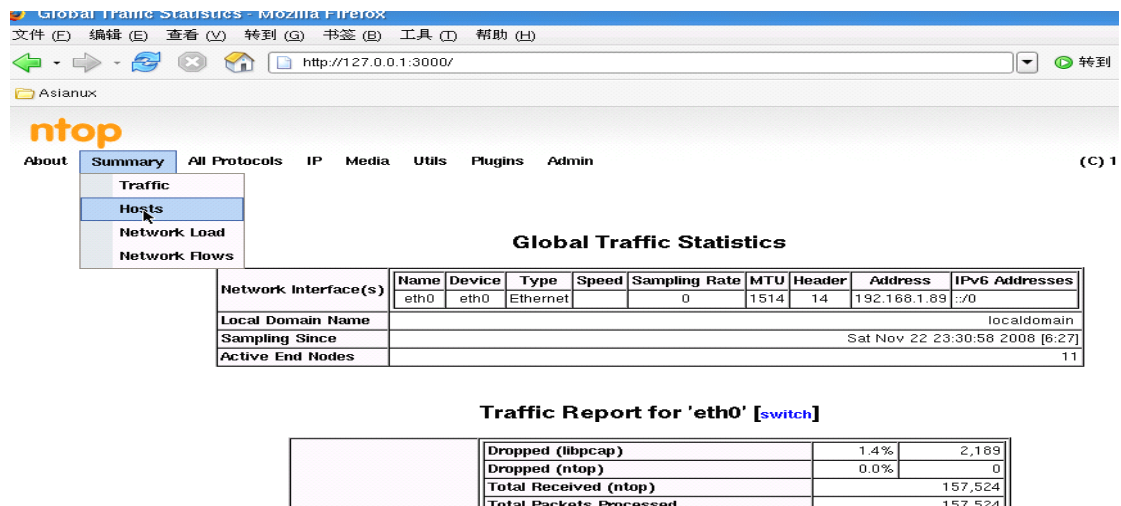


图4 ntop运行界面

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:

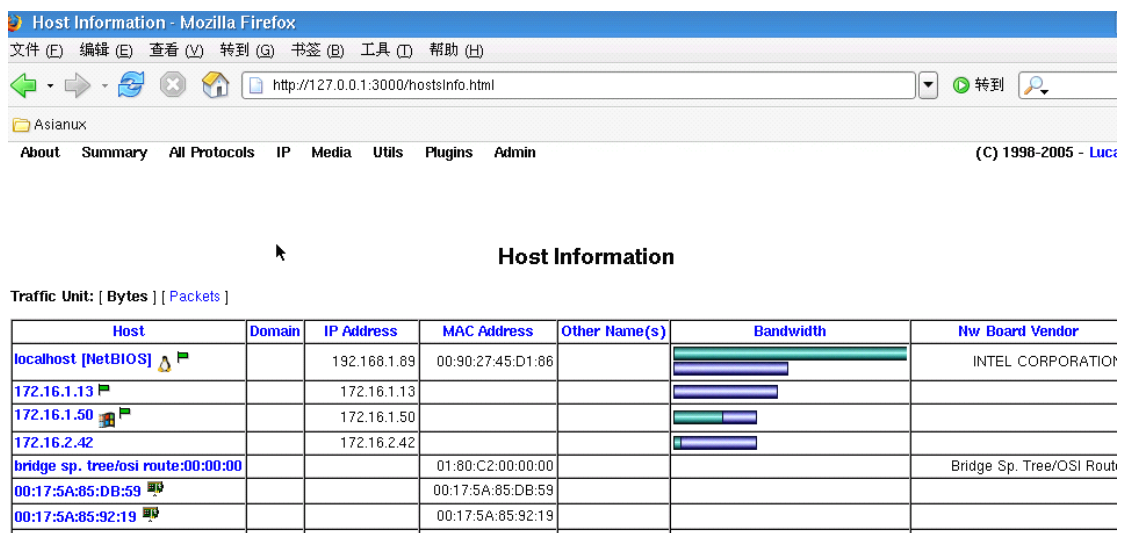


图6 选择summary下的hosts选项的分析结果

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。

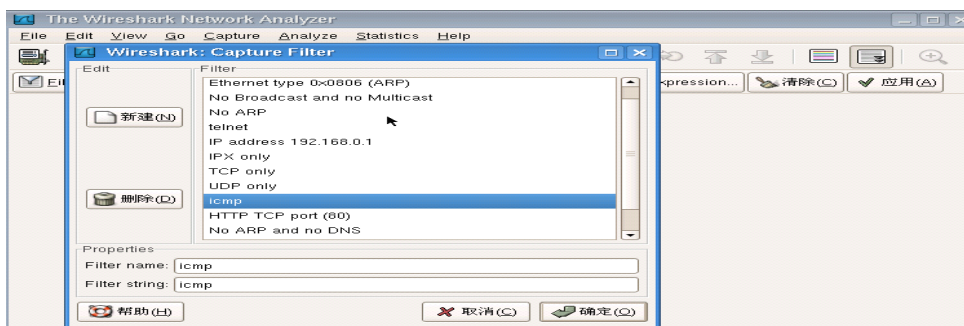


图7 ”CaptureFilter”对话框

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8 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

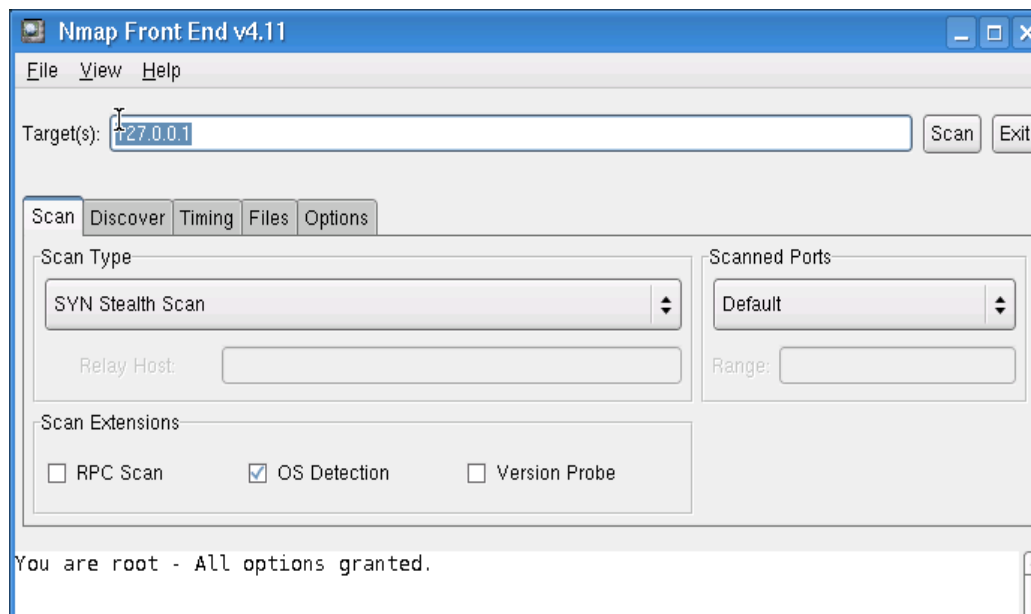


图9 输入要扫描的主机IP

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。