Linux 系统几种查找漏洞工具

Linux 操作系统是一个开放源代码的免费操作系统，它不仅安全、稳定、成本低，而且很少发现有病毒传播，因此，Linux 操作系统一直被认为是微软 Windows 系统的劲敌。近年来，随着 Linux 操作系统在我国的不断普及，随着越来越多的服务器、工作站和个人电脑开始使用 Linux 软件，当然，越来越多的安全发烧友也开始对这个操作系统发生了浓厚的兴趣。本文的目的是希望用户以最快的速度对 Linux 下的精品 Hack 软件功能及使用方法有一个比较细致全面的了解。今天我们先了解寻找肉鸡的 N 种兵器。

漏洞扫描器是一种自动检测远程或本地主机安全性弱点的程序。和 Windows 系统一样，当黑客得到目标主机的清单后，他就可以用一些 Linux 扫描器程序寻找这些主机的漏洞。这样，攻击者可以发现服务器的各种 TCP 端口的分配、提供的服务、Web 服务软件版本和这些服务及安全漏洞。而对系统管理员来说，如果能够及时发现并阻止这些行为，也可以大大减少入侵事件的发生率。按常规标准，可以将漏洞扫描器分为两种类型：主机漏洞扫描器（Host Scanner）和网络漏洞扫描器（Network Scanner）。主机漏洞扫描器是指在系统本地运行检测系统漏洞的程序；网络漏洞扫描器则是指基于 Internet 远程检测目标网络和主机系统漏洞的程序，下面，我们选取一些典型的软件及实例进行介绍。

1、基于主机的实用扫描软件

（1） sXid

sXid 是一个系统监控程序，软件下载后，使用“make install”命令即可安装。它可以扫描系统中 suid 和 sgid 文件和目录，因为这些目录很可能是后门程序，并可以设置通过电子邮件来报告结果。缺省安装的配置文件为/etc/sxid.conf，这个文件的注释很容易看懂，它定义了 sxid 的工作方式、日志文件的循环次数等；日志文件缺省为/var/log/sxid.log。出于安全方面的考虑，我们可以在配置参数后把 sxid.conf 设置为不可改变，使用 chattr 命令把 sxid.log 文件设置为只可添加。此外，我们还可以随时用 sxid -k 加上 -k 选项来进行检查，这种检查方式很灵活，既不记入日志，也不发出 email。

（2）LSAT

Linux Security Auditing Tool (LSAT) 是一款本地安全扫描程序，发现默认配置不安全时，它可以生成报告。LSAT 由 Triode 开发，主要针对基于 RPM 的 Linux 发布设计的。软件下载后，进行如下编译：

```
cndes$ tar xzvf last-VERSION.tgz
cndes$ cd lsat-VERSION
cndes$ ./configure
cndes$ make
```

然后以 root 身份运行：root# ./lsat。默认情况下，它会生成一份名字叫 lsat.out 的报告。也可以指定一些选项：

-o filename 指定生成报告的文件名

-v 详细输出模式

-s 不在屏幕上打印任何信息，只生成报告。

-r 执行 RPM 校验和检查，找出默认内容和权限被改动的文件

LSAT 可以检查的内容很多，主要有：检查无用的 RPM 安装；检查 inetd 和 Xinetd 和一些系统配置文件；检查 SUID 和 SGID 文件；检查 777 的文件；检查进程和服务；开放端口等。LSAT 的常用方法是用 cron 定期调用，然后用 diff 比较当前报告和以前报告的区别，就可以发现系统配置发生的变化。下面是一个测试中的报告片断：

```
*****************************************
This is a list of SUID files on the system:
/bin/ping
/bin/mount
/bin/umount
/bin/su
/sbin/pam_timestamp_check
/sbin/pwdb_chkpwd
/sbin/unix_chkpwd
```

```
****************************************
This is a list of SGID files/directories on the system:
/root/sendmail.bak
/root/mta.bak
/sbin/netreport
****************************************
List of normal files in /dev. MAKEDEV is ok, but there
should be no other files:
/dev/MAKEDEV
/dev/MAKEDEV.afa
****************************************
This is a list of world writable files
/etc/cron.daily/backup.sh
/etc/cron.daily/update_CDV.sh
/etc/megamonitor/monitor
/root/e
/root/pl/outfile
```

（3）GNU Tiger

这是扫描软件可以检测本机安全性，源自 TAMU 的 Tiger（一个老牌扫描软件）。Tiger 程序可以检查的项目有：系统配置错误；不安全的权限设置；所有用户可写的文件；SUID 和 SGID 文件；Crontab 条目；Sendmail 和 ftp 设置；脆弱的口令或者空口令；系统文件的改动。另外，它还能暴露各种弱点并产生详细报告。

（4）Nabou

Nabou 是一个可以用来监视系统变化的 Perl 程序，它提供文件完整性和用户账号等检查，并将所有数据保存在数据库里。此外，用户也可以在配置文件中嵌入 Perl 代码来定义自己的函数，执行自定义测试，操作其实十分方便。

（5）COPS

COPS 是可以报告系统的配置错误以及其他信息，对 linux 系统进行安全检查。其检测目标有：文件、目录和设备文件的权限检查；重要系统文件的内容、格式和权限；是否存在所有者为 root 的 SUID 文件；对重要系统二进制文件进行 CRC 校验和检查，看其是否被修改过；对匿名 FTP、Sendmai 等网络应用进行检查。需要指出的是，COPS 只是监测工具，并不做实际的修复。这个软件比较适合配合其他工具使用，其优点在于比较擅长找到潜在的漏洞。

（6）strobe

Strobe 是一个 TCP 端口扫描器，它可以记录指定的机器的所有开放端口，运行速度非常快。它最初用于扫描局域网中公开的电子邮件，从而得到邮件用户信息。Strobe 的另一个重要特点是它能快速识别指定机器上正在运行什么服务，不足之处是这类信息量比较有限。

（7）SATAN

SATAN 可以用来帮助系统管理员检测安全，也能被基于网络的攻击者用来搜索脆弱的系统。SATAN 是为系统和管理员设计的一个安全工具。然而，由于它的广泛性，易用性和扫描远程网络的能力，SATAN 也可能因为好奇而被用来定位有弱点的主机。SATAN 包括一个有关网络安全问题的检测表，经过网络查找特定的系统或者子网，并报告它的发现。它能搜索以下的弱点：

NFS??由无权限的程序或端口导出。
NIS-??口令文件访问。
Rexd??是否被防火墙阻止。
Sendmail??各种弱点。
ftp??ftp、wu-ftpd 或 tftp 配置问题。
远程 Shell 的访问??它是否被禁止或者隐藏。
X windows??主机是否提供无限制的访问。
Modem??经过 tcp 没有限制拨号访问。

（8）IdentTCPscan

IdentTCPscan 是一个比较专业的扫描器，可以在各种平台上运行。软件加入了识别指定 TCP 端口进程的所有者的功能，也就是说，它能测定该进程的 UID。这个程序具有很重要的功能就是通过发现进程的 UID，很快识别出错误配置。它的运行速度非常快，可以称得上是入侵者的宠物，是一个强大、锐利的工具。

2、基于网络的实用扫描工具

（1）Nmap

Nmap即Network Mapper，它是在免费软件基金会的GNU General Public License (GPL)下发布的。其基本功能有：探测一组主机是否在线；扫描主机端口，嗅探提供的网络服务；判断主机的操作系统。软件下载后，执行 configure、make和make install三个命令，将nmap二进制码安装到系统上，就可以执行nmap了。

Nmap的语法很简单，但功能十分强大。比如：Ping-scan命令就是“-sP”，在确定了目标主机和网络之后，即可进行扫描。如果以 root来运行Nmap，Nmap的功能会更加增强，因为超级用户可以创建便于Nmap利用的定制数据包。使用Nmap进行单机扫描或是整个网络的扫描很简单，只要将带有“/mask”的目标地址指定给Nmap即可。另外，Nmap允许使用各类指定的网络地址，比如 192.168.100.*，是对所选子网下的主机进行扫描。

Ping扫描。入侵者使用Nmap扫描整个网络寻找目标。通过使用“-sP”命令，缺省情况下，Nmap给每个扫描到的主机发送一个ICMP echo和一个TCP ACK，主机对任何一种的响应都会被Nmap得到。

Nmap支持不同类别的端口扫描，TCP连接扫描可以使用“-sT”命令。

隐蔽扫描(Stealth Scanning) 。在扫描时，如果攻击者不想使其信息被记录在目标系统日志上，TCP SYN扫描可帮你的忙。使用“-sS”命令，就可以发送一个SYN扫描探测主机或网络。

如果一个攻击者想进行UDP扫描，即可知哪些端口对UDP是开放的。Nmap将发送一个O字节的UDP包到每个端口。如果主机返回端口不可达，则表示端口是关闭的。

Ident扫描。攻击者都喜欢寻找一台对于某些进程存在漏洞的电脑，比如一个以root运行的WEB服务器。如果目标机运行了identd，攻击者就可以通过“-I”选项的TCP连接发现哪个用户拥有http守护进程。我们以扫描一个Linux WEB服务器为例，使用如下命令即可：

nmap -sT -p 80 -I -O www.yourserver.com

除了以上这些扫描，Nmap还提供了很多选项，这是很多Linux攻击者的必备法宝之一，通过这个软件，我们就可以对系统了如指掌，从而为下面的攻击打下良好的基础。

（2）p0f

p0f对于网络攻击非常有用，它利用SYN数据包实现操作系统被动检测技术，能够正确地识别目标系统类型。和其他扫描软件不同，它不向目标系统发送任何的数据，只是被动地接受来自目标系统的数据进行分析。因此，一个很大的优点是：几乎无法被检测到，而且p0f是专门系统识别工具，其指纹数据库非常详尽，更新也比较快，特别适合于安装在网关中。软件下载后，执行如下命令编译并安装p0f：

#tar zxvf p0f-1.8.2.tgz
#make&& make install

p0f的使用非常简单，使用如下命令可以在系统启动时，自动启动p0f进行系统识别：

#cp p0f.init /etc/init.d/p0f

#chkconfig p0f on

然后，每隔一段时间对p0f的日志进行分析即可。为了便于使用，p0f软件包提供了一个简单的分析脚本p0frep，通过它，攻击者可以很方便找到运行某类系统的远程主机地址。P0f还可以检测如下内容：防火墙的存在或伪装；到远程系统的距离以及它启动的时间；其他网络连接以及ISP。

（3）ISS

ISS Internet Scanner是全球网络安全市场的顶尖产品，通过对网络安全弱点全面和自主地检测与分析并检查它们的弱点，将风险分为高中低三个等级，并且可以生成大范围的有意义的报表。现在，这个软件的收费版本提供了更多的攻击方式，并逐渐朝着商业化的方向发展。

（4）Nessus

Nessus是一款功能强大的远程安全扫描器，它具有强大的报告输出能力，可以产生HTML、XML、LaTeX和ASCII文本等格式的安全报告，并能为每个安全问题提出建议。软件系统为client/sever模式，服务器端负责进行安全检查，客户端用来配置管理服务器端。在服务端还采用了 plug-in的体系，允许用户加入执行特定功能的插件，可以进行更快速和更复杂的安全检查。除了插件外，Nessus还为用户提供了描述攻击类型的脚本语言，来进行附加的安全测试。

软件下载后，解压并完成安装。安装完毕，确认在/etc/ld.so.conf文件加入安装已安装库文件的路径： /usr/local/lib。如果没有，只需在该文件中加入这个路径，然后执行ldconfig，这样Nessus在运行时就可以找到运行库了。 Nessus的配置文件为Nessusd.conf，位于/usr/local/etc/Nessus/目录下。一般情况下，不建议改动其中的内容。注意，使用时要创建一个nessusd 帐号，以便将来登陆扫描时使用。完成上面的准备工作后，以root用户的身份用下面的命令启动服务端：Nessusd ?d。

在客户端，用户可以指定运行Nessus服务的机器、使用的端口扫描器及测试的内容及测试的ip地址范围。Nessus本身是工作在多线程基础上的，所以用户还可以设置系统同时工作的线程数。这样用户在远端就可以设置Nessus的工作配置了。设置完毕，点击start就可以开始进行扫描。当扫描结束后，会生成报表，窗口的左边列出了所有被扫描的主机，只要用鼠标点击主机名称，在窗口右边就列出了经扫描发现的该主机的安全漏洞。再单击安全漏洞的小图标，会列出该问题的严重等级及问题的产生原因及解决方法。

（5）Nikto

Nikto 是一款能对 web 服务器多种安全项目进行测试的扫描软件，能在 200 多种服务器上扫描出 2000 多种有潜在危险的文件、CGI 及其他问题。它也使用 Whiske 库，但通常比 Whisker 更新的更为频繁。

（6）Whisker

Whisker 是一款非常好的 HTTP 服务器缺陷扫描软件，能扫描出大量的已知安全漏洞，特别是些危险的 CGI 漏洞，它使用 perl 编写程序库，我们可以通过它创建自己 HTTP 扫描器。

（7）Xprobe

XProbe 是一款主动操作系统指纹识别工具，它可以测定远程主机操作系统的类型。XProbe 依靠与一个签名数据库的模糊匹配以及合理的推测来确定远程操作系统的类型，利用 ICMP 协议进行操作系统指纹识别是它的独到之处。使用时，它假设某个端口没有被使用，它会向目标主机的较高端口发送 UDP 包，目标主机就会回应 ICMP 包，然后，XProbe 会发送其他的包来分辨目标主机系统，有了这个软件，判断对方的操作系统就很容易了。