一个网络安全检测系统

王月桥　汪为农　（上海交通大学网络信息中心　200030）

摘要：本文主要介绍了有关网络和系统中存在的安全漏洞，然后提出了一个网络安全检测系统的结构模型并讨论了每一个组成部分的功能。最后，论文介绍了设计这个模型的意义。

关键词：安全隐患　安全补丁　竞争条件　源路由

一、网络安全现状

Internet 最初由大学和科研机构使用渐渐进入到社会的各个行业，接入 Internet 的机构越来越多。可以说 Internet 已与人们的日常生活紧密联系起来，而且有越来越多的机密信息利用 Internet 传送。

1. 企业安全意识淡薄

早期，企业单位在建网时，没有进行必要的安全评估，也没有制定必要的技术安全策略。从而导致网络各个环节中存在着很多安全隐患。此外，由于企业缺乏安全意识，所用的操作系统存在不安全因素，对外开放高风险的网络服务，却没有设置严密的安全防范措施，从而就为入侵者敞开了方便之门。

2. 黑客增多

随着网络技术的普遍使用，网络黑客也应运而生，如今黑客遍布世界。黑客的入侵手段越来越高明。在 Internet 上可以找到很多攻击网络和系统安全漏洞的小程序，黑客使用这些小程序来进行网络攻击，如 Crack、sniffer、SATATN、COPS、Tiger 等等。而且有许多专门的黑客站点，提供网络入侵的技术和工具，如 www.rootshell.com、www.10oht.com、www.2600.com 等。

3. 内部攻击

在网络黑客中，内部攻击者占很大比重。但内部攻击经常被网络管理人员忽视，因为内部攻击者通常了解系统很多有用信息，从而进攻更易得手，造成的危害往往也更大。

二、网络和系统的安全隐患

INTERNET 或以 INTERNET 为基础构建的网络正成为信息共享的重要手段，但由于 INTERNET 灵活构散的体系结构，安全性能很差，存在的安全漏洞也很多，安全漏洞主要产生于系统、服务和网络传输三个方面。

1. 服务进程的漏洞

·Telnet 的问题主要是存在无口令用户或用户口令过于简单等。

·mail 存在的问题主要有允许发信件到指定的文件中、允许发送的信件被执行。

·FTP 可能存在的安全漏洞有允许匿名用户执行系统命令、ftp 根目录为超级用户所有、有的 ftpd 存在竞争条件，入侵者利用这些漏洞可获得超级用户权限。

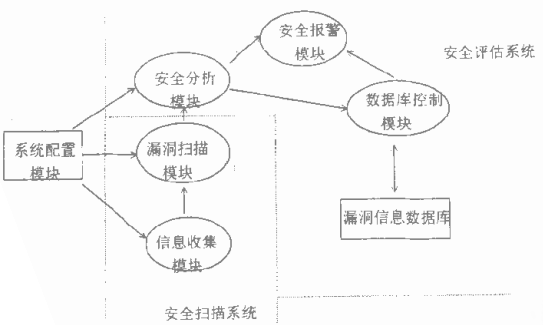
·HTTPd 出现的安全问题主要有栈溢出、不恰当的系统调用、对恶意的 Active X 及 Java Applet 的不能辨别。

2. 网络传输的漏洞 主要有 IP 地址期骗、IP 分片、源路由和 SYN flooding 攻击等。

3. 系统配置的漏洞 主要是文件系统、用户权限、系统程序、网络配置等方面的漏洞。

三、一个安全检测系统

本系统由两大部分组成，即安全评估系统和安全扫描系统。安全扫描系统首先收集被检测网络的有关信息，根据收集到的信息及事先制定的安全策略和系统配置文件，对监管网络进行扫描检测。安全评估系统对由安全扫描系统获得的结果进行分析，将安全漏洞按照系统、网络、服务及危害程度进行分类，然后通过数据库控制系统查询数据库，给出有关漏洞的详细信息，建议需要采用的安全补丁。如下所示系统结构图：



1. 系统配置模块

系统配置模块是整个系统的管理者，可使用 GUI（图形界面）或 HTML 文件加浏览器两种方式对系统进行管理。

系统配置模块主要用来对系统各个模块的运行规则进行配置。即(1)确定信息收集模块的作用范围。即收集某个子网的信息还是某一台主机的信息，若收集某个子网的信息，可设置该子网的 IP 地址范围如：202.120.24.1 - -202.120.24.254，这样就可以对子网 202.120.24.0 检测，收集必要的信息；若收集某台主机的信息，可仅设置该主机的 IP 地址如 202.120.24.34。(2)确定漏洞检查模块的检查对象，即是网络服务漏洞还是操作系统漏洞。对于网络服务漏洞，可以检测 mail 的 DEBUG 漏洞、ftpd 的 BOUNCE 漏洞或 httpd 的 CGI 漏洞等等；对于操作系统漏洞，可以是文件的权限、口令文件设置以及系统配置等方面的漏洞。

最后，根据各种配置信息生成系统配置文件。其他各个模块的初始化及正常运行，都要根据这个配置文件。

2. 信息收集模块的功能

(1)构建目标网络的拓扑结构。主要使用 sping 进行探测，确定网络大致的拓扑结构。sping 程序是网管中的一个十分有用的工具，它的基本原理是向目标网络发送大量的 ICMP 包，利用目标网络的响应信息，可以大致了解该网络中计算机的网络连接情况，根据这种连接情况能构建出网络的拓扑结构图。

(2)确定主机操作系统的类型和版本号。在网络中，往往是多种类型的计算机共存，不同类型的计算机可能运行不同类型的操作系统，而不同的操作系统可能产生的安全漏洞是各种各样。例如对于 UNIX 的各个版本，由于是不同厂商或不同的人编写的，有的版本可能存在某种漏洞，有的就避免了那种漏洞。WINDOWS 操作系统和 UNIX 操作系统相比较可能的安全漏洞又有所不同。所以确定操作系统的类型和版本号是完全必要的，使检测更具有针对性。

(3)确定主机开启的服务。主要利用与目标主机的各个端口建立 TCP 连接的方法，测试该端口是否处于服务状态。这种方法感兴趣的主要是 well _ known 端口，例如端口 21(ftp)、23(telnet)、25(Email)及 80(www)等，若该端口处于服务状态，以后可以检测该端口服务程序的安全漏洞。

3. 漏洞扫描模块的功能

扫描模块根据信息收集模块获得的信息和系统配置模块生成的配置文件，对目标进行扫描检测，收集网络和系统存在的安全漏洞的原始数据。

(1)网络扫描。即扫描网络服务和网络传输存在的各种安全漏洞。根据漏洞的特征，构造各种检测工具和数据包，如可构造具有恶意破坏性质的 Active X 控件来测试 HTTPD 的漏洞；构造具有假冒的 IP 地址的数据包，测试 IP SPOOFING 漏洞；构造具有分片和源路由的数据包，检测 IP 分片和 IP 源路由漏洞等等。

(2)防火墙扫描。当前防火墙的培植是十分复杂的，必须有专业人员来配置，但仍不免会出现漏配和错配，以致影响防火墙的防范能力，给黑客留下了后门。防火墙

可能被穿过或旁路掉，成为一个摆设。

首先必须检测防火墙的配置规则表，规则表有固定的格式，为配置和检测提供了方便；其次必须测试防火墙对各种攻击的防范能力，使用已有的各种工具来检测。

(3)操作系统扫描。可分为本地扫描和分布式扫描。本地扫描主要对象是检测系统所在主机的操作系统的安全漏洞，分布式扫描是检测远程主机的操作系统安全漏洞。

检测对象为口令文件是否对非超级用户可读、用户的根目录是否允许其他任何人均可写是否存在入侵者安放的 sniffer 程序、系统中是否有使用 SUID 的 shell 脚本程序等等。

4. 安全分析模块的功能和数据库控制模块

安全分析模块分析加工由漏洞扫描模块获得的原始信息，主要是对检测出的安全漏洞进行分类统计，即某种漏洞是属于操作系统还是属于网络服务程序的，是 mail 的还是 httpd 的，加工完成后将结果提交给报警模块和数据库控制模块。

数据库控制模块的任务是管理漏洞信息库并与报警模块进行交互。其一是检索漏洞信息，汇报给报警系统；其二是记录最新的安全漏洞信息，当有新的漏洞被发现时，将其必要的特征信息记录到数据库中。

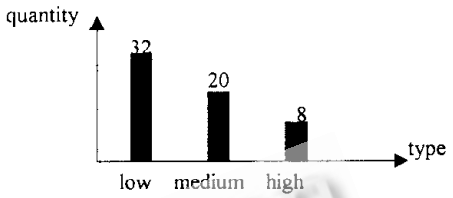
漏洞信息库的存储内容为漏洞的描述信息、漏洞的危害程度信息和补救措施信息。例如，漏洞 nfs－guess，描述信息 guessable NFS filehandles，危害程度 high，补救措施 patch.

5. 报警系统的功能

主要是根据由数据库检索模块和安全漏洞分析模块提供的信息，生成安全报告。安全报告可以采用饼状图、直方图和 HTML 文件三种形式。

·饼状图。主要用来表示各种程度的漏洞所占的百分比。如上所示：

·直方图。用来表示各种程度的安全漏洞数目的直观对比。如下所示：



·HTML 文件。汇报漏洞综合描述信息和网络及系统的安全水平，并建议应采用的补救措施。

四、系统实现的意义

1. 安全检测系统是对防火墙安全架构的必要补充

防火墙如同哨兵，守护着网络的出入口。但如果网络内部漏洞百出，入侵者一但突破或绕过防火墙，就可以肆意胡为。安全检测系统可发现网络的安全脆弱点，并提出相应的补救措施，从而加固网络的防御能力。另外，安全检测系统还可以对防火墙这个哨兵加以检测，看其是否称职。

2. 有助于进行有效的安全网络评估

企业建网络时，可利用安全检测系统对其网络进行检测，获得准确的有关网络安全审计及安全分析数据，以支持网络安全评估，进而制定合理的网络安全策略。

3. 确保配置一致性

保证所有系统和服务都是用与组织的安全策略一致的方式配置的，当出现新的差异和安全漏洞时，向系统管理员及时报警。

参考文献

[1] Cheswick William R. & Bellovin Steven M.《Firewalls and Internet Security－－Repelling the Willy Hacker》AT & Bell Lab.，1995

[2] Abrams M.，Podell H.《Computer and Network security》Los Alamitors，CA：IEEE Computer Society Press，1987

[3] Wietse Venema，《TCP Wrapper：Network Monitoring，ACCESS Control and Body Traps》USENIX Proceeding，UNIX security symposiunmIII；sept.1992

（来稿时间：1998 年 9 月）