网络安全检测的理论和实践（四）

卿斯汉　(中科院信息安全技术工程研究中心　100080)

4.5 网络安全检测工具

以下，我们简要介绍网络安全检测系统的若干检测工具的实现方法。

(1) 匿名FTP检测。该检测方法先使用UNIX自带的ftp命令向目标机进行匿名ftp访问。若能登录，则继续查看是否可以将本地文件传输到该远程目标机，传输成功后再删除该文件。根据各种可能的返回值确定目标机的安全漏洞。匿名FTP检测的流程图如图4所示。

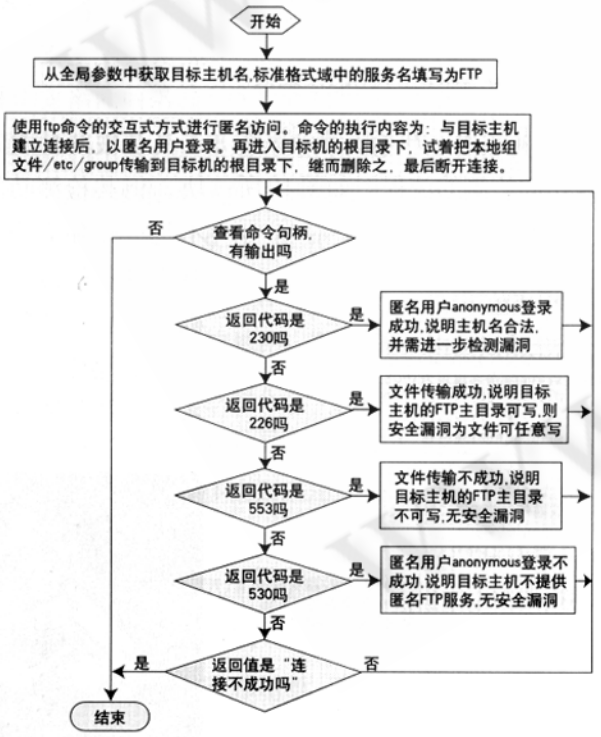

图 4　匿名FTP检测流程图

(2) 网络文件系统NFS检测。该检测方法查看宿主机的网络文件系统，先尝试是否能通过portmapper传输文件，再尝试是否允许未授权的用户传输或是否允许任意传输，根据检测结果分析系统安全漏洞。该指令须在根目录下运行。网络文件系统NFS检测的流程图如图5所示。

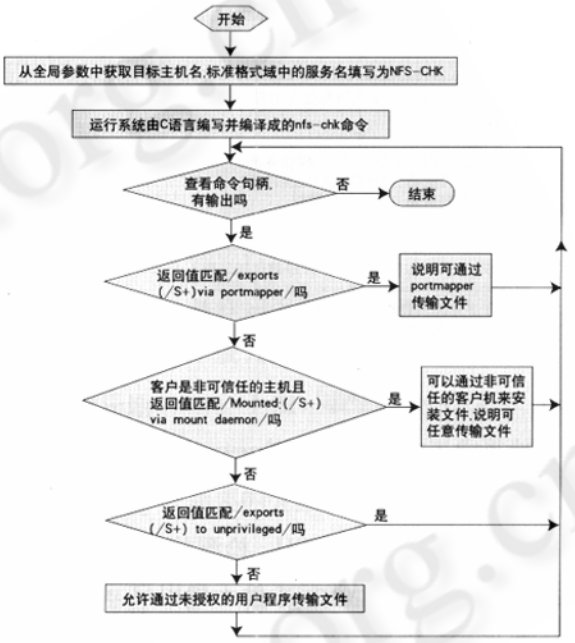

图 5　网络文件系统NFS检测流程图

(3) 网络信息服务NIS检测。本检测主要查看目标主机的NIS服务器是否设置了NIS映射访问控制，从而发现安全漏洞。程序通过运行C语言编译成的yp-chk命令，从不可信任的宿主机上查看目标机NIS映射访问控制。若访问成功则说明系统有安全漏洞，否则无安全漏洞测出。网络信息服务NIS检测的流程图如图6所示。

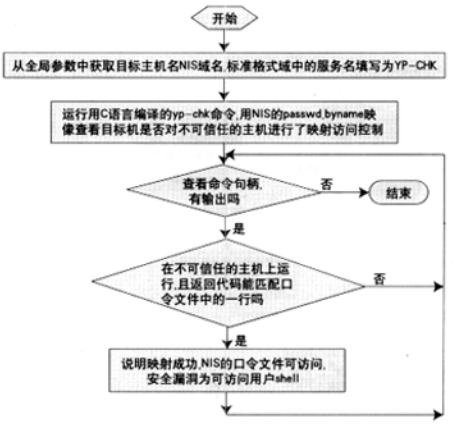

图 6　网络信息服务NIS检测流程图

(4) 域名服务DNS检测。本检测的思路较为简单，即利用UNIX的nslookup命令完成检测工作，然后再对其所获得的信息进行存储或输出。若系统无nslookup命令，则该检测无效。本检测只获取系统的CPU、操作系统、邮件传送器、邮件接收地址和名字服务器的信息。域名服务DNS检测的流程图如图7所示。

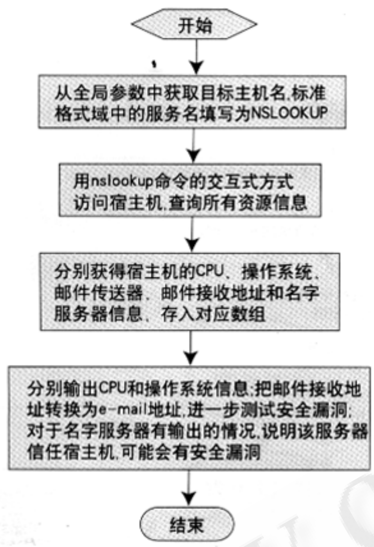

图 7　域名服务DNS检测流程图

(5) 远程shell检测RSH。检测前，系统先运行whoami命令查看是否处于根用户下。若是，再调用C语言编写并编译成的rcmd命令，看宿主机是否可执行远程shell命令。将输出的有效结果写入本地临时文件中，通过查看该文件的内容判断命令执行成功与否，从而检测目标主机的安全漏洞。最后删除该临时文件。远程shell检测RSH的流程图如图8所示。

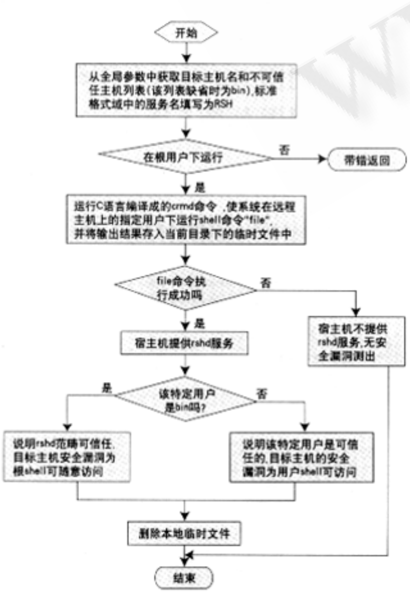

图 8　远程shell检测RSH流程图

(6) 普通文件传输协议TFTP检测。检测时运行tftp命令，访问远程目标主机。若能建立临时连接，则尝试能否将该机上的组文件/etc/group拷贝到本地的临时文件中。若传输成功则说明目标机有安全漏洞。最后删除该临时文件。普通文件传输协议TFTP检测的流程图如图9所示。

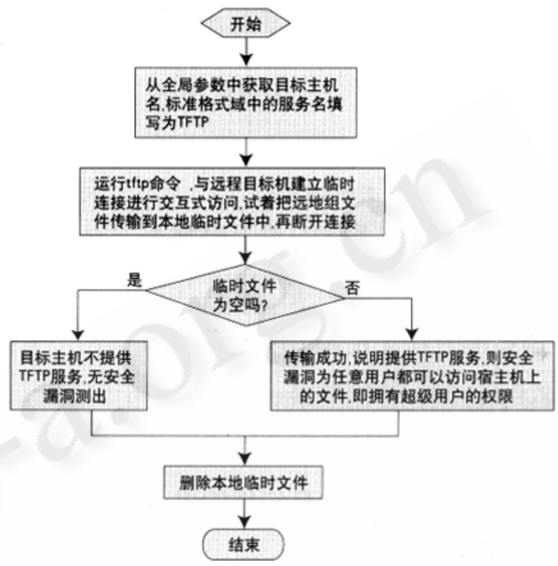

图 9　普通文件传输协议TFTP检测流程图

(7) X访问检测。检测时运行xhost命令，查看目标主机的X显示器，判定它是否设置了访问控制。X访问检测的流程图如图10所示。

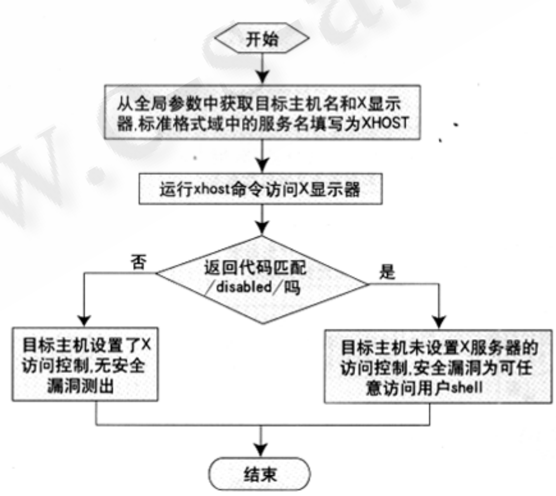

图 10　X访问检测流程图

至此，我们简要地介绍了网络安全检测系统部分检测工具的实现方法。由于篇幅有限，我们只能讲述一个大概，在设计真正的产品时，还需要进行大量的工作。

我们再提醒读者注意下面几点。

在实现中，TCP端口和UDP端口检测主要收集目标主机上正在使用的TCP和UDP端口的相关信息。FINGER和RUSERS检测分别收集近程和远程登录用户的登录信息，如用户的全名、主目录名、上一次登录时间和登录站点或者最后一次检查邮件的时间。REX检测则进行远程执行测试，查看目标主机是否提供rexd服务。若存在，则给出当前日期的输出结果并提出警告。RPC检测通过查看远程目标主机所有注册的RPC程序，收集该目标主机所提供的各种服务列表。此外，虽然从实现上来看，以上各种网络安全检测工具是彼此独立的模块，但其检测功能并不是彼此独立的。只有将各种检测工具有机地结合，才能全面和有效地检测出目标系统的安全漏洞。■