网络扫描原理分析与研究

——端口扫描与漏洞扫描原理与分析

考号：　　姓名：

【内容提要】

网络扫描技术是一类重要的网络安全技术。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。

端口扫描技术和漏洞扫描技术是网络安全扫描技术中的两种核心技术，并且广泛应用于当前较成熟的网络扫描器中。

【关键词】 网络安全扫描技术　端口扫描技术　漏洞扫描技术

随着 Internet 的不断发展，信息技术已成为促进经济发展、社会进步的巨大推动力：当今社会高度的计算机化信息资源对任何人无论在任何时候、任何地方都变得极有价值。不管是存储在工作站中、服务器里还是流通于 Internet 上的信息都已转变成为一个关系事业成败关键的策略点，这就使保证信息的安全变得格外重要。

网络扫描技术是一类重要的网络安全技术。网络扫描技术与防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员可以根据扫描的结果更正网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。如果说防火墙和网络监控系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，可以有效避免黑客攻击行为，做到防患于未然。

网络安全扫描技术是一种基于 Internet 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 Web 服务器的各种 TCP/IP 端口的分配、开放的服务、Web 服务软件版本和这些服务及软件呈现在 Internet 上的安全漏洞。网络安全扫描技术也是采用积极的、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。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。

端口扫描技术和漏洞扫描技术是网络安全扫描技术中的两种核心技术，并且广泛运用于当前较成熟的网络扫描器中。

一、端口扫描技术

一个端口就是一个潜在的通信通道，也就是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息。通过端口扫描，可以得到许多有用的信息，从而发现系统的安全漏洞。它使系统用户了解系统目前向外界提供了哪些服务，从而为系统用户管理网络提供了一种手段。

1.1 端口扫描技术的原理

端口扫描向目标主机的 TCP/IP 服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭，就可以得知端口提供的服务或信息。端口扫描也可以通过捕获本地主机或服务器的流入流出 IP 数据包来监视本地主机的运行情况，它仅能对接收到的数据进行分析，帮助我们发现目标主机的某些内在的弱点，而不会提供进入一个系统的详细步骤。

1.2 各类端口扫描技术

TCP connect() 扫描

这是最基本的 TCP 扫描。操作系统提供的 connect()系统调用，用来与每一个感兴趣的目标计算机的端口进行连接。如果端口处于侦听状态，那么 connect()就能成功。否则，这个端口是不能用的，即没有提供服务。这个技术的一个最大的优点是，你不需要任何权限。系统中的任何用户都有权利使用这个调用。另一个好处就是速度。如果对每个目标端口以线性的方式，使用单独的 connect()调用，那么将会花费相当长的时间，你可以通过同时打开多个套接字，从而加速扫描。使用非阻塞 I/O 允许你设置一个低的时间用尽周期，同时观察多个套接字。但这种方法的缺点是很容易被发觉，并且被过滤掉。目标计算机的 logs 文件会显示一连串的连接和连接是出错的服务消息，并且能很快的使它关闭。

TCP SYN 扫描

这种技术通常认为是“半开放”扫描，这是因为扫描程序不必要打开一个完全的 TCP 连接。扫描程序发送的是一个 SYN 数据包，好象准备打开一个实际的连接并等待反应一样（参考 TCP 的三次握手建立一个 TCP 连接的过程）。一个 SYN|ACK 的返回信息表示端口处于侦听状态。一个 RST 返回，表示端口没有处于侦听态。如果收到一个 SYN|ACK，则扫描程序必须再发送一个 RST 信号，来关闭这个连接过程。这种扫描技术的优点在于一般不会在目标计算机上留下记录。但这种方法的一个缺点是，必须要有 root 权限才能建立自己的 SYN 数据包。

TCP FIN 扫描

有的时候有可能 SYN 扫描都不够秘密。一些防火墙和包过滤器会对一些指定的端口进行监视，有的程序能检测到这些扫描。相反，FIN 数据包可能会没有任何麻烦的通过。这种扫描方法的思想是关闭的端口会用适当的 RST 来回复

FIN 数据包。另一方面，打开的端口会忽略对 FIN 数据包的回复。这种方法和系统的实现有一定的关系。有的系统不管端口是否打开，都回复 RST，这样，这种扫描方法就不适用了。并且这种方法在区分 Unix 和 NT 时，是十分有用的。

IP 段扫描

这种不能算是新方法，只是其它技术的变化。它并不是直接发送 TCP 探测数据包，是将数据包分成两个较小的 IP 段。这样就将一个 TCP 头分成好几个数据包，从而过滤器就很难探测到。但必须小心。一些程序在处理这些小数据包时会有些麻烦。

TCP 反向 ident 扫描

ident 协议允许(rfc1413)看到通过 TCP 连接的任何进程的拥有者的用户名，即使这个连接不是由这个进程开始的。因此你能，举个例子，连接到 http 端口，然后用 identd 来发现服务器是否正在以 root 权限运行。这种方法只能在和目标端口建立了一个完整的 TCP 连接后才能看到。

FTP 返回攻击

FTP 协议的一个有趣的特点是它支持代理（proxy）FTP 连接。即入侵者可以从自己的计算机 a.com 和目标主机 target.com 的 FTP server-PI(协议解释器)连接，建立一个控制通信连接。然后，请求这个 server-PI 激活一个有效的 server-DTP(数据传输进程)来给 Internet 上任何地方发送文件。对于一个 User-DTP,这是个推测,尽管 RFC 明确地定义请求一个服务器发送文件到另一个服务器是可以的。但现在这个方法好象不行了。这个协议的缺点是“能用来发送不能跟踪的邮件和新闻，给许多服务器造成打击，用尽磁盘，企图越过防火墙”。

我们利用这个的目的是从一个代理的 FTP 服务器来扫描 TCP 端口。这样，你能在一个防火墙后面连接到一个 FTP 服务器，然后扫描端口（这些原来有可能被阻塞）。如果 FTP 服务器允许从一个目录读写数据，你就能发送任意的数据到发现的打开的端口。

二、漏洞扫描技术

通常是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测或是渗透攻击的行为。

漏洞扫描是对你的电脑进行全方位的扫描，检查你当前的系统是否有漏洞，如果有漏洞则需要马上进行修复，否则电脑很容易受到网络的伤害甚至被黑客借助于电脑的漏洞进行远程控制那么后果将不堪设想，所以漏洞扫描对于保护电脑和上网安全是必不可少的，而且需要每星期就进行一次扫描，一但发

现有漏洞就要马上修复，有的漏洞系统自身就可以修复，而有些则需要手动修复。

2.1 漏洞扫描技术的原理

漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞：在端口扫描后得知目标主机开启的端口以及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配，查看是否有满足匹配条件的漏洞存在；通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱势口令等。若模拟攻击成功，则表明目标主机系统存在安全漏洞。

2.2 漏洞扫描技术的分类和实现方法

基于网络系统漏洞库，漏洞扫描大体包括 CGI 漏洞扫描、POP3 漏洞扫描、FTP 漏洞扫描、SSH 漏洞扫描、HTTP 漏洞扫描等。这些漏洞扫描是基于漏洞库，将扫描结果与漏洞库相关数据匹配比较得到漏洞信息；漏洞扫描还包括没有相应漏洞库的各种扫描，比如 Unicode 遍历目录漏洞探测、FTP 弱势密码探测、OPENRelay 邮件转发漏洞探测等，这些扫描通过使用插件（功能模块技术）进行模拟攻击，测试出目标主机的漏洞信息。下面就这两种扫描的实现方法进行讨论：

（1）漏洞库的匹配方法

基于网络系统漏洞库的漏洞扫描的关键部分就是它所使用的漏洞库。通过采用基于规则的匹配技术，即根据安全专家对网络系统安全漏洞、黑客攻击案例的分析和系统管理员对网络系统安全配置的实际经验，可以形成一套标准的网络系统漏洞库，然后再在此基础之上构成相应的匹配规则，由扫描程序自动的进行漏洞扫描的工作。

这样，漏洞库信息的完整性和有效性决定了漏洞扫描系统的性能，漏洞库的修订和更新的性能也会影响漏洞扫描系统运行的时间。因此，漏洞库的编制不仅要对每个存在安全隐患的网络服务建立对应的漏洞库文件，而且应当能满足前面所提出的性能要求。

（2）插件（功能模块技术）技术

插件是由脚本语言编写的子程序，扫描程序可以通过调用它来执行漏洞扫描，检测出系统中存在的一个或多个漏洞。添加新的插件就可以使漏洞扫描软件增加新的功能，扫描出更多的漏洞。插件编写规范化后，甚至用户自己都可以用 perl、c 或自行设计的脚本语言编写的插件来扩充漏洞扫描软件的功能。这种技术使漏洞扫描软件的升级维护变得相对简单，而专用脚本语言的使用也简化了编写新插件的编程工作，使漏洞扫描软件具有强的扩展性。

2.3 漏洞扫描中的问题及完善建议

现有的安全隐患扫描系统基本上是采用上述的两种方法来完成对漏洞的扫描，但是这两种方法在不同程度上也各有不足之处。下面将说明这两种方法中存在的问题，并针对这些问题给出相应的完善建议：

（1）系统配置规则库问题

网络系统漏洞库是基于漏洞库的漏洞扫描的灵魂所在，而系统漏洞的确认是以系统配置规则库为基础的。但是，这样的系统配置规则库存在其局限性：

①如果规则库设计的不准确，预报的准确度就无从谈起；

②它是根据已知的安全漏洞进行安排和策划的，而对网络系统的很多危险的威胁却是来自未知的漏洞，这样，如果规则库要新不及时，预报准确度也会逐渐降低；

③受漏洞库覆盖范围的限制，部分系统漏洞也可能不会触发任何一个规则，从而不被检测到。

完善建议：系统配置规则库应能不断地被扩充和修正，这样也是对系统漏洞库的扩充和修正，这在目前仍需要专家的指导和参与才能够实现。

（2）漏洞库信息要求

漏洞库信息是基于网络系统漏洞库的漏洞扫描的主要判断依据。如果漏洞库信息不全面或得不到即时的更新，不但不能发挥漏洞扫描的作用，还会给系统管理员以错误的引导，从而对系统的安全隐患不能采取有效措施并及时的消除。

完善建议：漏洞库信息不但应具备完整性和有效性，也应具有简易性的特点，这样即使是用户自己也易于对漏洞库进行添加配置，从而实现对漏洞库的即时更新。比如漏洞库在设计时可以基于某种标准（如 CVE 标准）来建立，这样便于扫描者的理解和信息交互，使漏洞库具有比较强的扩充性，更有利于以后对漏洞库的更新升级。

网络安全扫描技术和主机安全扫描技术都是新兴的技术，与防火墙、入侵检测等技术相比，它们从另一个角度来解决网络安全上的问题。本文就网络安全扫描技术与其包含的端口扫描技术和漏洞扫描技术的一些具体内容进行了阐述和分析。随着网络的发展和内核的进一步修改，新的端口扫描技术及对入侵性的端口扫描的新防御技术还会诞生，而到目前为止还没有一种完全成熟、高效的端口扫描防御技术；同时，漏洞扫描面向的漏洞包罗万象，而且漏洞的数目也在继续的增加。就目前的漏洞扫描技术而言，自动化的漏洞扫描无法得以完全实现，而且新的难题也将不断涌现，因此网络安全扫描技术仍有待更进一步的研究和完善。

【参考文献】

（1）宋苑　著：　《网络扫描技术的原理》　2007.11 版
（2）《网络安全问题的探讨与研究》　2008.9　版
（3）李瑞民 著：《网络扫描技术揭秘》　机械工业出版社 2012-01 版