安全知识之网络扫描器概念与相关技术(上) PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E5_AE_89_E5_85_A8_E7_9F_A5_E8_c101_142627.htm 网络安全扫描器简介 迅速发展的Internet给人们的生活、工作带来了巨大的方便，但同时，也带来了一些不容忽视的问题，网络信息的安全保密问题就是其中之一。 网络的开放性以及黑客的攻击是造成网络不安全的主要原因。科学家在设计Internet之初就缺乏对安全性的总体构想和设计，我们所用的TCP/IP 协议是建立在可信的环境之下，首先考虑的是网络互连，它是缺乏对安全方面的考虑的。而且TCP/IP协议是完全公开的，远程访问使许多攻击者无须到现场就能够得手，连接的主机基于互相信任的原则等等这一些性质使网络更加不安全。 先进的技术是实现网络信息安全的有力武器，这些技术包括:密码技术、身份验证技术、访问控制技术、安全内核技术、网络反病毒技术、信息泄漏防治技术、防火墙技术、网络安全漏洞扫描技术、入侵检测技术等。而在系统发生安全事故之前对其进行预防性检查，及时发现问题并予以解决不失为一种很好的办法，于是网络安全漏洞扫描技术应运而生。 1. 扫描器基本工作原理 扫描器是一种自动检测远程或本地主机安全脆弱点的程序，通过使用扫描器可以不留痕迹的发现远程服务器的各种TCP端口的分配及提供的服务和它们的软件版本，这就能让我们间接的或直观的了解到远程主机所存在的安全问题。 扫描器采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。目标可以是工作站、服务器、交换机、数据库应用等各种对象。然后根据扫描结果向系统管理员提供

周密可靠的安全性分析报告，为提高网络安全整体水平产生重要依据。在网络安全体系的建设中，安全扫描工具花费低、效果好、见效快、与网络的运行相对对立、安装运行简单，可以大规模减少安全管理员的手工劳动，有利于保持全网安全政策的统一和稳定。 扫描器并不是一个直接的攻击网络漏洞的程序，它仅仅能帮助我们发现目标机的某些存在的弱点。一个好的扫描器能对它得到的数据进行分析，帮助我们查找目标主机的漏洞。但它不会提供进入一个系统的详细步骤。 扫描器应该有三项功能：发现一个主机和网络的能力；一旦发现一台主机，有发现什么服务正运行在这台主机上的能力；通过测试这些服务，发现这些漏洞的能力。 扫描器对Internet安全很重要，因为它能揭示一个网络的脆弱点。在任何一个现有的平台上都有几百个熟知的安全脆弱点。在大多数情况下，这些脆弱点都是唯一的，仅影响一个网络服务。人工测试单台主机的脆弱点是一项极其繁琐的工作，而扫描程序能轻易的解决这些问题。扫描程序开发者利用可得到的常用攻击方法并把它们集成到整个扫描中，这样使用者就可以通过分析输出的结果发现系统的漏洞。 2.端口扫描介绍 真正的扫描器是TCP端口扫描器，这种程序可以选通TCP/IP端口和服务（比如，Telnet或FTP），并记录目标的回答。通过这种方法，可以搜集到关于目标主机的有用信息（比如，一个匿旬用户是否可以登录等等）。而其他所谓的扫描器仅仅是UNIX网络应用程序，这些程序一般用于观察某一服务是否正在一台远程机器上正常工作，它们不是真正的扫描器，但也可以用于收集目标主机的信息（UNIX平台上通用的rusers和host命令就是这类程序的很好的例子）。 2.1 TCP

SYN 扫描 扫描程序发送的SYN数据包，好像准备打开一个新的连接并等待反映一样。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状态。如果收到一个SYN|ACK，扫描程序必须再发送一个RST 信号，来关闭这个连接过程。 优点：不会在目标计算机上留下纪录。 缺点：扫描程序必须要有root权限才能建立自己的SYN数据包。