黑客老鸟讲入侵攻击：简简单单讲扫描 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/287/2021_2022__E9_BB_91_E5_AE_A2_E8_80_81_E9_c101_287835.htm 通常扫描包括端口扫描和漏洞扫描1、端口扫描通常分为TCP 和UDP扫描、标识扫描、FTP 反弹扫描、源端口扫描；TCP 和UDP扫描TCP连接扫描：是完整的TCP全开放扫描（ 囊括了SYN、SYN/ack、ack），缺点是很容易被对方的防火墙、入侵检测设备截杀，得不到真实的端口开放情况。简单的说TCP连接扫描通常是在渗透到内网后，进行内网主机端口开放情况的扫描。这与直接在外网扫描时得到的结果差别很大。TCP SYN扫描：俗称为半开放扫描，因为它们都是只建立到目标主机的TCP半开放连接（单个SYN包）；如果探测到目标系统上的端口是开放的，则返回SYN/ack包；如果端口关闭，目标主机返回rst/ack包TCP FIN扫描：向目标主机端口发出单个的FIN包，如果端口关闭，目标系统将返回rst包。TCP Xmas树扫描：向目标主机端口发送具有fin、urg和push TCP标志的包，若目标系统所有端口关闭，则返回rst包。TCP 空扫描：关掉所有的标志，如果目标系统所有端口关闭，则返回rst包TCP ACK 扫描：这个扫描可以用于确定防火墙的规则集，或者使单个包穿过简单的包过滤防火墙。经过一些测试，在构造一些畸形包的时候，国内大多的防火墙都未进行过滤分析，都是直接放行。策略完善的防火墙将拒绝那些与防火墙状态表中的会话不相符合的ack响应包；而简单的包过滤防火墙将允许ack连接请求。TCP rpc扫描 ：主要用于识别远程过程调用（rpc）端口及相关程序和版本号。UDP扫描：主要扫描一些目标

主机的UDP端口扫描情况。看一个示例：220 mail.xxxx.com esmtp sendmail 8.8.3. mon,12 aug 06:05:53 -0500通过这个扫描信息，我们可以完整的推断出这是台邮件服务器，是一台sendmail8.8.3的邮件服务器，并且支持扩展smtp（esmtp）命令，我们可以通过telnet会话来向服务器发送特定的命令完成交换，从而确定 smtp/esmtp所支持的命令。利用TCP 和UDP扫描，可以获得目标系统运行的软件和版本信息。FTP反弹扫描主要是利用了FTP协议中对代理FTP这一特性，对FTP服务器进行欺骗扫描。FTP服务器作为反弹代理，黑客能够进行掩饰源扫描地址的端口扫描（通俗的理解就是让FTP服务器做“ 代理 ”将一组字符发到特定服务器的ip地址和端口）。需要注意的是，如果要执行FTP反弹扫描，中间FTP服务器必须提供一个可读写的目录。源端口扫描主要是通过扫描dns、smtp、http这些默认端口，来判断其打开情况。可使用的工具，个人推荐 supercan，目前最高版本是4.0的，并且集成了whois查询等实用功能。nmap 目前也出了win下的，但是得在本机安装的有active perl，具体的我也没有在windows环境下使用过，都是在linux下使用的。还有x-scan，国产的精品。这些都可以在网络上免费下载到。2、漏洞扫描漏洞扫描主要是利用漏洞扫描工具对一组目标ip进行扫描，通过扫描能得到大量相关的ip、服务、操作系统和应用程序的漏洞信息。漏洞扫描可分为系统漏洞扫描和web漏洞扫描主要扫描一些操作系统或应用程序配置漏洞，如：◆操作系统或应用程序代码漏洞◆旧的或作废的软件版本◆特络绎木马或后门程序◆致命的特权相关的漏洞◆拒绝服务漏洞◆web和cgi漏洞漏洞库信息对于漏洞扫描有很多帮助，它的来源主要是iss的x-force

漏洞库，安全焦点的bugtraq数据库、http：//cve.mitre.org上维护的cve列表。漏洞扫描推荐工具：启明的天镜漏洞扫描系列和web漏洞扫描的Acunetix.Web.Vulnerability.Scanner4 100Test下载频道开通，各类考试题目直接下载。详细请访问www.100test.com