网络安全检测思路与技巧 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/265/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c67_265453.htm 对于主机的安全检测，我们通常直接采用nmap或者类似软件进行扫描，然后针对主机操作系统及其开放端口判断主机的安全程度，这当然是一种方法，但这种方法往往失之粗糙，我仔细考虑了一下，觉得按下面的流程进行判别是比较完整的。 1、通过DNS查询得到目标的网络拓扑基本情况，比如有几台主机，各自起的服务是什么等等。这是必要的步骤因为我们检测应该针对网络，而不是单一主机。 2、用nmap进行端口扫描，判断操作系统，结合自己的一些经验，必要的时候抓banner，判断出目标主机的操作系统类型。 3、用nessus进行普通漏洞的扫描,得到一个大致的报告。对报告进行分析。nessus的报告有些地方并不准确，而且有漏扫或误报的情况，比如严重的unicode漏洞机器明明有,它却会扫不到，对这种情况我们必须有人工的判断。 4、cgi漏洞也必须有专门的扫描器进行，可以结合whisker或者twwwscan或者xscan，自己判断需要增加哪些危险cgi的检测。 上面只是最简单的，任何一个初学电脑的人可能都能够较好完成的工作流程，但是如果在上面的各种扫描方式得到的信息无法分析出目标操作系统的情况甚至系统类型的时候，应该怎么办呢？这种事情现在经常遇到，因为大多数防火墙或者入侵检测系统现在都具备了动态地将tcp/ip协议栈如TTL、TOS、DF、滑动窗口大小等修改或者屏蔽，使扫描工具无法得出正确结果的功能。互联网上也有许多免费工具可以达到这一效果。 因此下面要谈到其它检查

方式 1、在有防火墙的情况下：建议可以使用如hping、firewalk之类的工具，更加灵活地探测目标主机的情况，根据数据包的返回做更进一步的判断。这需要操作者掌握TCP/IP基本知识，并能灵活运用判断。 2、对主页程序的检测，虽然我们只能在外面做些基本的输入验证检测。但按照现在常见的web错误，我们可以从下面几个方面着手分析：a、特殊字符的过滤: &amp..` ‘ \" *?~^()[]{}$\n\r 这些字符由于在不同的系统或运行环境中会具有特殊意义，如变量定义/赋值/取值、非显示字符、运行外部程序等，而被列为危险字符但在许多编程语言、开发软件工具、数据库甚至操作系统中遗漏其中某些特殊字符的情况时常出现，从而导致出现带有普遍性的安全问题。当有需要web用户输入的时候，根据不同的数据库系统、编程语言提交带不同参数变量的url，很可能造成服务器端资料泄露甚至可执行系统命令。 b、WEB服务器的错误编码或解码可能会导致服务器信息的泄露、可执行命令、源代码泄露等错误。比较典型的应该是unicode漏洞以及各种iis服务器、apache服务器的源代码泄露漏洞。 c、利用程序错误的边界判断而造成的缓冲区溢出进行攻击。最近的一个典型案例应该是eeye.com发现的.printer溢出漏洞。这是web server本身的问题；但网站应用程序的编写者也可能犯下同样的错误，就是对户输入不加验证。但这方面的错误比较不容易试出来。 通过这样一个过程，应该说在远程扫描，没有本地帐号或者权限的情况下，能够搜集到尽量多的信息了。当然，主机面临的并非是远程风险，还需要具体分析。