网络入侵一般步骤及思路 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E7_BD_91_E7_BB_9C_E5_85_A5_E4_c101_461724.htm 第一步：进入系统 1. 扫描目标主机。 2. 检查开放的端口，获得服务软件及版本。 3. 检查服务软件是否存在漏洞，如果是，利用该漏洞远程进入系统；否则进入下一步。 4. 检查服务软件的附属程序(*1)是否存在漏洞，如果是，利用该漏洞远程进入系统；否则进入下一步。 5. 检查服务软件是否存在脆弱帐号或密码，如果是，利用该帐号或密码系统；否则进入下一步。 6. 利用服务软件是否可以获取有效帐号或密码，如果是，利用该帐号或密码进入系统；否则进入下一步。 7. 服务软件是否泄露系统敏感信息，如果是，检查能否利用；否则进入下一步。 8. 扫描相同子网主机，重复以上步骤，直到进入目标主机或放弃。 第二步：提升权限 1. 检查目标主机上的SUID和GUID程序是否存在漏洞，如果是，利用该漏洞提升权限，否则进入下一步。 2. 检查本地服务是否存在漏洞，如果是，利用该漏洞提升权限，否则进入下一步。 3. 检查本地服务是否存在脆弱帐号或密码，如果是，利用该帐号或密码提升权限；否则进入下一步。 4. 检查重要文件的权限是否设置错误，如果是，利用该漏洞提升权限，否则进入下一步。 5. 检查配置目录(*2)中是否存在敏感信息可以利用。 6. 检查用户目录中是否存在敏感信息可以利用。 7. 检查临时文件目录(*3)是否存在漏洞可以利用。 8. 检查其它目录(*4)是否存在可以利用的敏感信息。 9. 重复以上步骤，直到获得root权限或放弃。 第三步：放置后门 最好自己写后门程序，用别人的程序总是相

对容易被发现。 第四步：清理日志 最好手工修改日志，不要全部删除，也不好使用别人写的工具。 附加说明： *1 例如WWW服务的附属程序就包括CGI程序等 *2 这里指存在配置文件的目录，如/etc等 *3 如/tmp等，这里的漏洞主要指条件竞争 *4 如WWW目录，数据文件目录等
/**********/好了，大家都知道了入侵者入侵一般步骤及思路 那么我们开始做入侵检测了。 第一步、我们都知道一个入侵者想要入侵一台服务器首先要扫描这台服务器，搜集服务器的信息，以便进一步入侵该系统。系统信息被搜集的越多，此系统就越容易被入侵者入侵。 所以我们做入侵检测时，也有必要用扫描器扫描一下系统，搜集一下系统的一些信息，来看看有没有特别流行的漏洞(呵呵这个年头都时兴流行哦：) 第二步、扫描完服务器以后，查看扫描的信息－－－－>分析扫描信息。如果有重大漏洞－－－－>修补(亡羊补牢，时未晚)，如果没有转下一步。 第三步、没有漏洞，使用杀毒工具扫描系统文件，看看有没有留下什么后门程序，如：nc.exe、srv.exe.....如果没有转下一步。 第四步、入侵者一般入侵一台机器后留下后门，充分利用这台机器来做一些他想做的事情，如：利用肉鸡扫描内网，进一步扩大战果，利用肉鸡作跳板入侵别的网段的机器，嫁祸于这台机器的管理员，跑流影破邮箱..... 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