通过Linux系统伪装方法加固系统安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E9_80_9A_E8_BF_87Linu_c103_145381.htm 网络上的计算机很容易被黑客利用工具或其它手段进行扫描，以寻找系统中的漏洞，然后再针对漏洞进行攻击。 通过伪装Linux系统，给黑客设置系统假象，可以加大黑客对系统的分析难度，引诱他们步入歧途，从而进一步提高计算机系统的安全性。下面以Red Hat Linux为例，针对几种黑客常用的途径介绍一些常用的Linux系统伪装的方法。 针对HTTP服务 通过分析Web服务器的类型，大致可以推测出操作系统的类型，比如，Windows使用IIS来提供HTTP服务，而Linux中最常见的是Apache。 默认的Apache配置里没有任何信息保护机制，并且允许目录浏览。通过目录浏览，通常可以获得类似“ Apache/1.3.27 Server at apache.linuxforum.net Port 80 ”或“ Apache/2.0.49 (Unix) PHP/4.3.8 ”的信息。 通过修改配置文件中的ServerTokens参数，可以将Apache的相关信息隐藏起来。但是，Red Hat Linux运行的Apache是编译好的程序，提示信息被编译在程序里，要隐藏这些信息需要修改Apache的源代码，然后，重新编译安装程序，以实现替换里面的提示内容。 以Apache 2.0.50为例，编辑ap_release.h文件，修改“ #define AP_SERVER_BASEPRODUCT \"Apache\" ”为“ #define AP_SERVER_BASEPRODUCT \"Microsoft-IIS/5.0\" ”。编辑os/unix/os.h文件，修改“ #define PLATFORM \"Unix\" ”为“ #define PLATFORM \"Win32\" ”。修改完毕后，重新编译、安装Apache。 Apache安装完成后，修改httpd.conf配置文件

，将“ ServerTokens Full ”改为“ ServerTokens Prod ”；将“ ServerSignature On ”改为“ ServerSignature Off ”，然后存盘退出。重新启动Apache后，用工具进行扫描，发现提示信息中已经显示操作系统为Windows。 针对FTP服务 通过FTP服务，也可以推测操作系统的类型，比如，Windows下的FTP服务多是Serv-U，而Linux下常用vsftpd、proftpd和pureftpd等软件。以proftpd为例，修改配置文件proftpd.conf，添加如下内容：ServerIdent on \"Serv-U FTP Server v5.0 for WinSock ready...\" 存盘退出后，重新启动proftpd服务，登录到修改了提示信息的FTP服务器进行测试： C:\\>ftp 192.168.0.1 Connected to 192.168.0.1. 220 Serv-U FTP Server v5.0 for WinSock ready... User (192.168.0.1:(none)): 331 Password required for (none). Password: 530 Login incorrect. Login failed. ftp > quit 221 Goodbye. 这样从表面上看，服务器就是一个运行着Serv-U的Windows了。 针对TTL返回值 可以用ping命令去探测一个主机，根据TTL基数可以推测操作系统的类型。对于一个没有经过任何网关和路由的网络，直接ping对方系统得到的 TTL值，被叫做“ TTL基数 ”。网络中，数据包每经过一个路由器，TTL就会减1，当TTL为0时，这个数据包就会被丢弃。 通常情况下，Windows的TTL的基数是128，而早期的Red Hat Linux和Solaris的TTL基数是255，FreeBSD和新版本的Red Hat Linux的TTL基数是64。比如，ping一个Red Hat系统，显示如下： Pinging 192.168.0.1 with 32 bytes of data: Reply from 192.168.0.1: bytes=32 time Reply from 192.168.0.1: bytes=32 time Reply from 192.168.0.1: bytes=32 time Reply from 192.168.0.1: bytes=32 time Ping statistics for 192.168.0.1: Packets: Sent = 4, Received = 4, Lost =

0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms 用以下命令修改Red Hat Linux的TTL基数为128(本来为64)： # echo 128 > /proc/sys/net/ipv4/ip_default_ttl 若想使设置永久生效，可以修改/etc/sysctl.conf配置文件，添加如下一行： net.ipv4.ip_default_ttl = 128 保存退出后，再ping 192.168.0.1 ，TTL基数就变为128了。 针对3389端口和22端口 有时通过扫描3389端口和22端口，也可以推测操作系统的类型。Windows下一般利用TCP协议的3389端口进行远程控制，而Linux可能会用TCP协议的22端口，提供带有加密传输的SSH服务。 为了安全，可以利用iptables来限制22端口的SSH登录，让非授权的IP扫描不到TCP 22端口的存在： #iptables -I INPUT -s ! xx.xx.xx.xx -p tcp --dport 22 -j DROP 利用iptables，将本机的TCP 3389端口转移到其它开有3389端口的计算机上，给Linux系统伪装出一个提供服务的TCP 3389端口。命令如下： #echo 1 > /proc/sys/net/ipv4/ip_forward #iptables -t nat -I PREROUTING -p tcp --dport 3389 -j DNAT --to xx.xx.xx.xx #iptables -t nat -I POSTROUTING -p tcp --dport 3389 -j MASQUERADE 第一条命令表示允许数据包转发；第二条命令表示转发TCP 3389到xx.xx.xx.xx；第三条命令表示使转发数据包实现“ 双向通路 ”，给数据包设置一个正确的返回通道。若想使转发永久生效，可以把以上命令添加到/etc/rc.local文件中。 这样，当黑客扫描服务器所开端口的时候，就找不到22号端口，而是看到一个伪装的3389端口，从而不能正确判断出操作系统的类型。 针对netcraft netcraft是一个很厉害的扫描引擎，它通过简单的TCP 80，就可以知道所测服务器的

操作系统、Web服务程序和服务器开机时间(Uptime)等信息。上面介绍的几种方法对netcraft来说，均不奏效。针对netcraft，可利用iptables进行系统伪装，使netcraft错误判断操作系统：#iptables -t nat -I PREROUTING -s 195.92.95.0/24 -p tcp --dport 80 -j DNAT --to xx.xx.xx.xx #iptables -t nat -I POSTROUTING -s 195.92.95.0/24 -p tcp --dport 80 -j MASQUERADE 由于通过抓包发现，netcraft的服务器不止一台，所以需要对它所在网段进行转发欺骗处理。 小结 以上方法只能从某种角度上防止和阻挠黑客对系统漏洞的分析，在一定程度上可减少计算机被攻击的可能性，但仍然是“ 防君子，不防小人 ”，仅是给大家提供一个活学活用的新思路。