使用Linux系统Iptables防火墙 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/245/2021_2022__E4_BD_BF_E7_94_A8Linu_c103_245706.htm Linux 的内置firewall机制，是通过kernel中的netfilter模块实现的(www.netfilter.ort)。Linux kernel使用netfilter对进出的数据包进行过滤，netfilter由三个规则表组成，每个表又有许多内建的链组成。通过使用iptables命令可以对这些表链进行操作，如添加、删除和列出规则等。 一、Netfilter规则表filter nat mangle filter,用于路由网络数据包。是默认的，也就是说如果没有指定-t参数，当创建一条新规则时，它会默认存放到该表内。 INPUT 网络数据包流向服务器 OUTPUT 网络数据包从服务器流出 FORWARD 网络数据包经服务器路由 nat,用于NAT表.NAT(Net Address Translation )是一种IP地址转换方法。 PREROUTING 网络数据包到达服务器时可以被修改 OUTPUT 网络数据包由服务器流出 POSTROUTING 网络数据包在即将从服务器发出时可以被修改 mangle,用于修改网络数据包的表，如TOS(Type Of Service),TTL(Time To Live),等 INPUT 网络数据包流向服务器 OUTPUT 网络数据包流出服务器 FORWARD 网络数据包经由服务器转发 PREROUTING 网络数据包到达服务器时可以被修改 POSTROUTING 网络数据包在即将从服务器发出时可以被修改 1.配置Iptables 当数据包进入服务器时，Linux Kernel会查找对应的链，直到找到一条规则与数据包匹配。如果该规则的target是ACCEPT，就会跳过剩下的规则，数据包会被继续发送。如果该规则的target是DROP，该数据包会被拦截掉，kernel不会再参考其他规则。 Note：如果从始至终都没有一

条规则与数据包匹配，而且表末尾又没有0drop all的规则，那末该数据包会被accept。Cisco则相反，在表末尾会因含deny all的规则。 1.) Iptables的命令选项 iptables [-t tables] command option parameter target -A 在链尾添加一条规则 -C 将规则添加到用户定义链之前对其进行检查 -D 从链中删除一条规则 -E 重命名用户定义的链，不改变链本身 -F 清空链，删除链上的所有规则 -I 在链中插入一条规则 -L 列出某个链上的规则，如iptables L INPUT 列出INPUT链的规则 -N 创建一个新链 -P 定义某个链的默认策略 -R 替换链上的某条规则 -X 删除某个用户相关的链 -Z 将所有表的所有链的字节和数据包计数器清零 2.) Iptables的命令参数 -p protocol 应用于数据包的协议类型，可以是TCP UDP ICMP或ALL。！也可使用。 当使用-p tcp时，还可使用其他可以选项，以便允许进一步定义规则。选项包括： sport 允许指定匹配数据包源端口.port1:port ,表示port1和port2之间的所有端口 dport 目的端口，和sport雷同。 当使用-p !udp时，也有特殊的选项供使包括： sport,dport,与-p tcp 相同，只不过用以用于UDP包。 使用-p icmp参数时，只有一个选项可用。 icmp-type，允许在过滤规则中指定icmp类型。 -s source 指定数据包的源地址。该参数后跟一个IP地址，一个带有sub-net mask的网络地址，或一个主机名。(不建议使用主机名) -d,- - destination 数据包的目的地址，同-s. -j,jump 用于指定一个target,告诉规则将该匹配的数据包发送到该 target。Target可以是ACCEPT,DROP,QUEUE,RETURN.如果没有-j,那么不会对数据包进行任何操作，只是将计数器加1。 -i - - in-interface ,对于INPUT FORWARD PREROUTING链，该参数指定数据包到

达服务器时所使用的端口。 -o - - out-interface,对于OUTPUT FORWARD POSTROUTING链，该参数指定数据包离开服务器时使用的端口。 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