**深 圳 大 学 实 验 报 告**

**课程名称：­ 计算机安全导论**

**实验项目名称­： 防火墙实验**

**学院： 计算机与软件学院**

**专业： 软件工程（腾班）**

**指导教师： 陈飞**

**报告人： 黄亮铭 学号： 2022155028 班级： 腾班**

**实验时间： 2024年11月23日 – 2024年12月6日**

**实验报告提交时间： 2024年12月6日**

**教务部制**

|  |
| --- |
| **实验目的与要求**：   1. 搭建iptables实验环境。 2. 了解iptables的相关名词和术语。 3. 了解iptables的表和链知识。 4. 掌握iptables基本命令的使用。 5. 熟练使用iptables命令进行链表操作。 6. 了解如何配置iptables规则。 |
| **实验环境**：   1. Windows7 2. Windows server 2003 3. CentOS 6.5 4. VMware |
| **实验原理**：   1. VMware Workstation软件包含一个用于英特尔x86兼容计算机的虚拟机套装，其允许多个x86虚拟机同时被创建和运行。每个虚拟机实例可以运行其自己的客户机操作系统。VMware工作站允许一台真实的计算机同时运行数个操作系统。 2. iptables是与Linux内核集成的IP信息包过滤系统。如果Linux系统连接到因特网或LAN、服务器或连接LAN和因特网的代理服务器，则该系统有利于在Linux系统上更好地控制IP信息包过滤和防火墙配置。 3. 防火墙在做信息包过滤决定时，有一套遵循和组成的规则，这些规则存储在专用的信息包过滤表中，而这些表集成在Linux内核中。在信息包过滤表中，规则被分组放在我们所谓的链（chain）中。而netfilter/iptables IP信息包过滤系统是一款功能强大的工具，可用于添加、编辑和移除规则。 4. Netfilter/iptables是表（tables）的容器，iptables包含4个表，分别是filter、nat、mangel和raw。 5. ptables的表(tables)是链（chains）的容器，iptables包含5个链，分别是INPUT、OUTPUT、FORWARD、PREROUTING和POSTROUTING。 6. iptables是用来设置、维护和检查Linux内核的IP包过滤规则的。可以定义不同的表，每个表都包含几个内部的链，也能包含用户自定义的链。每个链都是一个规则列表，对对应的包进行匹配：每条规则指定应当如何处理与之相匹配的包。这被称作target（目标），也可以跳向同一个表内的用户定义的链。 7. 通过iptables命令对防火墙iptables的表链进行相关操作（因环境策略不同，表链会有所不同），如查看、添加、删除、修改等。 8. FTP 是File Transfer Protocol（文件传输协议）的英文简称，而中文简称为“文传协议”。用于Internet上的控制文件的双向传输。同时，它也是一个应用程序（Application）。基于不同的操作系统有不同的FTP应用程序，而所有这些应用程序都遵守同一种协议以传输文件。在FTP的使用当中，用户经常遇到两个概念："下载"（Download）和"上传"（Upload）。"下载"文件就是从远程主机拷贝文件至自己的计算机上；"上传"文件就是将文件从自己的计算机中拷贝至远程主机上。用Internet语言来说，用户可通过客户机程序向（从）远程主机上传（下载）文件。 |
| **实验内容**：   1. 了解iptables规则。 2. 配置iptables访问ftp服务。 |
| **实验步骤与结果**：  （依照实验内容，逐条撰写实验过程与实验所得结果：包括网络架构，核心数据包，调试过程。请附上相关截图，及注意格式排版的美观。实验提交时，以上为评分依据，请不删除本行）  搭建iptables实验环境   1. 将操作机Windows7的IP地址设置为192.168.1.2，子网掩码设置为255.255.255.0，默认网关为192.168.1.200。如图1所示。     图1配置Windows7的IPv4地址   1. 将Windows server 2003的IP地址设为20.0.0.2，子网掩码设置为255.255.255.0，默认网关设置为20.0.0.200，如图2所示。     图2配置Windows server 2003的IP地址   1. 将服务器CentOS 6.5的IP地址设置为10.0.0.2，子网掩码设置为255.255.255.0，网关设置为10.0.0.200，如图3所示。     图3配置服务器CentOS 6.5的IP地址   1. 将将作为防火墙的CentOS 6.5上的3块网卡的IP地址分别设置为192.168.1.200，10.0.0.200和20.0.0.200，同时将它们的子网掩码设置为255.255.255.0。     图4配置防火墙CentOS 6.5的网卡   1. 在终端中输入命令开启网卡之间的IP转发功能。然后查看结果，发现ip\_forward的数值为1，说明网卡之间的IP转发功能开启成功。     图5开启转发功能结果   1. 在操作机Window7上测试本机和除作为防火墙的CentOS6.5之外的主机是否连接（使用ping命令）。结果如图6所示，说明本机和其他两台主机连接成功。     图6 ping命令结果   1. 在Windows server 2003上测试本机和除作为防火墙的CentOS6.5之外的主机是否连接（使用ping命令）。结果如图7所示，说明本机和其他两台主机连接成功。     图7 ping命令结果   1. 在服务器CentOS 6.5上测试本机和除作为防火墙的CentOS6.5之外的主机是否连接（使用ping命令）。结果如图8所示，说明本机和其他两台主机连接成功。     图8 ping命令结果  Iptables相关术语  该部分介绍了iptables防火墙的相关术语以及iptables本身相关的名词。   1. iptables是Unix/Linux自带的一款优秀且开放源码的完全基于包过滤的防火墙工具，它的功能十分强大，使用非常灵活，可以对流入和流出服务器的数据包进行很精细的控制。特别是它可以在一台非常低的硬件配置下跑得非常好。 2. iptables的最大优点是它可以配置有状态的防火墙。iptables主要工作在OSI的数据链路层、网络层和传输层。如果重新编译内核，也可以支持7层控制。 3. iptables防护墙由两个组件netfilter和iptables组成。netfilter组件也称为内核空间,是内核的一部分，由一些信息包过滤表组成，这些表包含内核用来控制信息包过滤处理的规则集。iptables组件是一种工具，也称为用户空间,它使插入、修改和除去信息包过滤表中的规则变得容易。 4. 容器：在iptables中，容器用来描述包含或者属于的关系。Netfilter是表的容器。表是链的容器，即所有的链都属于对应的表。链是规则的容器。规则是iptables一系列过滤信息的规范和具体方法。   iptables的表和链   1. iptables包含4个表，分别为raw表、filter表、nat表和mangle表。但是raw表很少被使用，因此默认情况下iptables根据功能和定义划分3个表，实际上managel表也比较少使用。     图9不同表的功能   1. Filter表和链INPUT、FORWARD、OUTPUT之间的关系如图10所示。Nat表和链OUTPUT、PREROUTING、POSTROUTING之间的关系如图11所示。Mangle表主要负责修改数据包特殊的路有标记。     图10 filter和其链的关系    图11 nat表和其链的关系   1. Filter功能即防火墙功能的流程如下图所示。     图12 Filter功能  iptables的基本命令   1. 我们可以在系统终端输入命令：*iptables -h*获取iptables的使用方法，或者使用*man iptables*查看更加详细的使用方法。  |  |  | | --- | --- | |  |  | | 图13a第一条命令 | 图13b第二条命令 |  1. iptables的通用命令格式为iptables[-t tables] COMMAND chain[-m matchname[per-match-options]] -j targetname[per-target-options]。   其参数解释如下：   * tables：指定iptables的表，可以是filter、nat、mangle或raw。如果不指定，默认为filter。 * COMMAND：iptables命令，如-A（追加规则）、-D（删除规则）、-I（插入规则）等。 * chain：指定链，可以是INPUT、OUTPUT、FORWARD、PREROUTING或POSTROUTING。 * -m matchname[per-match-options]：指定匹配条件，matchname是匹配模块的名称，per-match-options是该模块的具体选项。 * -j targetname[per-target-options]：指定目标，targetname是目标的名称，per-target-options是该目标的具体选项。  1. iptables命令的格式可以使用图表示如下。     图14 iptables命令格式  iptables的表链操作   1. 查看CentOS 6.5防火墙iptables的表名，如下图所示。     图15防火墙iptables的表名   1. 查看表filter、nat、mangle和raw中的链以及链中的规则，如下图所示。其中的链默认规则均为ACCEPT。  |  |  | | --- | --- | |  |  | | 图16a filter表 | 图16b nat表 | |  |  | | 图16c mangle表 | 图16d raw表 |  1. 如果需要查看某一条链上的规则，可以增加参数-L指定链名。     图17表filter上FORWARD链的规则   1. 在终端输入命令查看防火墙配置文件。     图18防火墙配置文件   1. 我们可以使用命令*iptalbes -N [chain\_name]*创建新链，默认为filter表，但是我们可以使用-t参数指定表。     图19添加链后的filter表   1. 我们可以使用*-X table\_name*删除某一条自定义链或者使用*-X*删除所有自定义的链。     图20删除链simpleware1   1. 我们可以使用-P参数修改某条链的默认规则。     图21修改INPUT链的默认规则   1. 对于非自定义链，我们可以使用*-F chain\_name*清除链上的规则或者*-F*清除filter表中所有链的规则。     图22清除INPUT链的所有规则   1. 我们还可以使用命令：*iptables -A [policy\_name] -s [ip\_addr] -j [default\_policy\_name]*添加规则。     图23 INPUT链添加规则  配置iptables禁止访问ftp服务   1. 打开Win7的cmd，输入[ftp 10.0.0.2](ftp://ftp 10.0.0.2)，然后输入用户名ftp，密码123456进行登录操作，结果如下图所示，说明登录成功。     图24外网访问ftp服务   1. 打开Windows server 2003的cmd，输入[ftp 10.0.0.2](ftp://ftp 10.0.0.2)，然后输入用户名ftp，密码123456进行登录操作，结果如下图所示，说明登录成功。     图25内网访问ftp服务   1. 在防火墙CentOS 6.5中输入命令进行清除防火墙规则的操作。     图26清除防火墙规则   1. 对filter表中的FORWARD链进行配置，禁止内外网访问ftp服务。     图27添加丢弃规则   1. 将添加的规则保存到iptables的配置文件中，然后重启防火墙，查看防火墙规则，结果如下图所示，说明上一步添加的规则被成功配置到防火墙中。     图28配置防火墙   1. 重新进行步骤1和步骤2的操作，结果如下图所示，说明内网和外网均不能访问ftp服务。  |  |  | | --- | --- | |  |  | | 图29a 外网访问ftp服务结果 | 图29b 内网访问ftp服务结果 |   配置iptables按网段访问ftp服务  该部分内容的步骤1 – 步骤3的操作均与上一个部分即**配置iptables禁止访问服务**相同，因此这里不再重复。该部分将直接从步骤4开始。   1. 配置防火墙，按网段访问ftp服务。在终端输入如下命令，在转发的数据包中，如果源地址为192.168.1.0/24，目标端口为21，则将该数据包丢弃，同时允许源地址为20.0.0.2/24，目标端口为21的数据包通过。     图30添加接受和丢弃规则   1. 将添加的规则保存到iptables的配置文件中，然后重启防火墙，查看防火墙规则，结果如下图所示，说明上一步添加的规则被成功配置到防火墙中。     图31配置防火墙   1. 进行**配置iptables禁止访问ftp服务**中的步骤1和步骤2的操作，结果如下图所示，说明内网可以访问ftp服务，而外网不能访问ftp服务。  |  |  | | --- | --- | |  |  | | 图32a外网访问ftp服务结果 | 图32b内网访问ftp服务结果 |   思考题   1. **在搭建iptables的实验环境时，为什么要开启作为防火墙的CentOS 6.5上的IP转发功能**。   答：因为需要作为防火墙的CentOS6.5需要承担路由的功能，即一个网络接口接收到的数据包被转发到另一个网络接口。   1. **Netfilter、表、链和规则之间的关系是什么**？   答：它们之间的关系是包含关系，Netfilter是表的容器，表是链的容器，链是规则的容器。   1. **Iptables中默认的表是**？   答：当iptables不指定表时，iptables中默认的表是filter。   1. **指定源端口范围使用什么参数**？   答：使用—source port, --sport port[:port]   1. **如何一次性删除某个表中自定义的链**？   答：使用命令*iptables -t [tables\_name] -X*。   1. **iptables命令中，DROP和REJECT有什么区别**？   答：DROP会将数据包静默丢弃，不会给发送方发送任何消息，有利于隐藏服务器；REJECT会将数据包丢弃，然后发送icmp报文告知发送方数据请求被拒绝，容易暴露服务器。 |
| **实验结论**：  （撰写实验收获及思考）   1. 本次实验我完成了对iptables规则的学习，也完成了iptables规则的应用。 2. 通过本次实验，我掌握了如何配置防火墙规则允许某一网段访问服务和禁止某一网段访问服务，从而完成内网与外网的隔离。 3. 通过完成思考题，我对iptables的内容有了更加深入的了解。 4. 通过本次实验，我对iptables防火墙的配置和使用有了深入的理解和实践经验。 |
| 指导教师批阅意见：  成绩评定：  指导教师签字：  年 月 日 |
| 备注： |

注：1、报告内的项目或内容设置，可根据实际情况加以调整和补充。

2、教师批改学生实验报告时间应在学生提交实验报告时间后10日内。