实验六:系统防火墙管理

一、实验目的

- 1、理解 iptables 的工作原理;
- 2、掌握 iptables 防火墙的安装与配置;
- 3、掌握 iptables 防火墙的基本操作方法,能够熟练使用防火墙。

二、实验学时

2 学时

三、实验类型

综合性

四、实验需求

1、硬件

每人配备计算机1台,不低于双核CPU、8G内存、500GB硬盘。

2、软件

Windows操作系统,安装VirtualBox虚拟化软件,安装Putty管理终端软件,安装Nmap 工具软件。

3、网络

计算机使用固定 IP 地址接入局域网,并支持对互联网的访问,虚拟主机可通过 NAT 方式访问互联网。

4、工具

无。

五、实验任务

1、完成 iptables 防火墙的安装与配置;

2、完成 iptables 防火墙规则的管理,满足实验的场景要求。

六、实验内容及步骤

1、iptables 的安装与管理

- (1) 防火墙检测
- ①关闭 firewall 防火墙
- 关闭 CentOS 的 firewall 防火墙,并取消开机自动启动,其操作命令如下。

systemctl stop firewalld

管理科学与工程学科 / 阮晓龙 / 13938213680 / 共 6 页, 第1页

systemctl disable firewalld

②检查 iptables 是否安装

一般情况下, iptables 已经包含在 Linux 系统中,可以通过命令来检测系统是否已经安装 iptables,具体命令如下,检测结果如图 6-1 所示则表示系统已经安装 iptables 防火墙。

iptables --version



③检查是否安装 iptables-services

查看 iptables 服务是否安装,其命令如下所示。

systemctl status iptables

若出现如图 6-2 所示的结果则说明 iptables 服务未安装,若出现如图 6-3 所示的结果则 说明 iptables 服务已安装。

[root@localhost ~]# service iptables status Redirecting to /bin/systemctl status iptables.service Unit iptables.service could not be found. [root@localhost ~]# systemctl status iptables Unit iptables.service could not be found.

图 6-2 iptables service 未安装



图 6-3 iptables service 已安装

- (2) 安装 iptables 软件
- 安装 iptables 以及 iptables services 服务软件,其操作命令如下所示。
 - # yum install -y iptables
 - # yum install -y iptables-services
- (3) iptables 服务配置
- 进行 iptables 服务管理,其操作命令如下所示。

##开启 iptables 服务
systemctl start iptables
##设置开机自动启动
systemctl enable iptables
##关闭 iptables 服务
systemctl stop iptables
##重启 iptables 服务

管理科学与工程学科 / 阮晓龙 / 13938213680 / 共 6 页, 第2页

- # systemctl restart iptables
- ##取消开机自动启动
- # systemctl disable iptables

2、iptables 的基本配置

(1)规则的查看

使用一下命令进行防火墙规则查看,并将防火墙规则信息填写到表 6-1 中。

iptables -n -L

表 6-1 防火墙规则

(2)规则的添加

①端口配置

●开启需要的端口,如配置 TCP 协议的 22 端口允许进出系统,其配置命令如下。

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

●关闭不安全的端口,如配置不允许通过 TCP 协议的 445 端口进出系统,其配置命令 如下所示。

iptables -A INPUT -p tcp --dport 445 -j DROP

iptables -A OUTPUT -p tcp --sport 445 -j DROP

●配置服务端口,如配置允许通过 HTTP 访问系统的 80 端口,其配置命令如下。

iptables -A INPUT -p tcp --dport http -j DROP

②IP 地址配置

●拒绝某单一IP地址,如拒绝某一单独IP地址访问系统,且系统拒绝访问该IP地址, 其配置命令如下。

iptables -A INPUT -s xxx.xxx.xxx -j DROP
iptables -A OUTPUT -d xxx.xxx.xxx -j DROP

●拒绝某 IP 地址段,如拒绝某 IP 地址段中任一地址访问系统,且系统拒绝访问该 IP 地址段中任一 IP 地址,其配置命令如下。

iptables -A INPUT -s xxx.xxx.xxx.xxx/xx -j DROP

iptables -A OUTPUT -d xxx.xxx.xxx/xx -j DROP

③IP 地址与端口结合

●拒绝某 IP 地址访问某端口,如拒绝某一单独 IP 地址访问系统的 22 端口(TCP 协议),其配置命令如下。

iptables -A INPUT -s xxx.xxx.xxx -p tcp --dport 22 -j DROP

●允许某段 IP 地址访问系统的服务端口,如允许某段 IP 地址访问系统的 HTTP 服务端口,其配置命令如下。

管理科学与工程学科 / 阮晓龙 / 13938213680 / 共 6 页, 第3页

iptables -A INPUT -s xxx.xxx.xxx/xx -p tcp --dport http -j ACC EPT

④网络协议配置

配置拒绝 ICMP 协议通过,如配置拒绝网络中通过 PING 方式发现系统 IP 地址,其配置命令如下。

iptables -A INPUT -p icmp -j DROP

⑤网卡接口配置

iptables 防火墙可单独为某个网卡接口设定不同的策略规则,如不允许任何主机通过防火墙本机的 eth0 网卡访问系统的 80 端口,其配置命令如下。

iptables -A INPUT -i eth0 -p tcp --dport 80 -j DROP

⑥MAC 地址配置

●拒绝某 MAC 地址主机的所有通信请求访问,其配置命令如下。

iptables -A INPUT -m mac --mac-source XX:XX:XX:XX:XX:XX -j DR OP

●拒绝网络中某一固定 IP 地址且固定 MAC 地址的主机访问系统任意端口,其配置命 令如下。

iptables -A INPUT -s xxx.xxx.xxx/x -m mac --mac-source XX:X
X:XX:XX:XX -j DROP

●允许网络中某一固定 IP 地址且固定 MAC 地址的主机访问系统的 22 号端口,其配置 命令如下。

iptables -A INPUT -p tcp --dport 22 -s xxx.xxx.xxx/x -m mac --mac-source XX:XX:XX:XX:XX:XX -j ACCEPT

(3) 规则的测试

①软件获取

获取端口扫描工具 Zenmap 软件可通过本课程网站(http://linux.xg.hactcm.edu.cn)下载 获得,也可通过 Zenmap 官方网站(https://nmap.org/zenmap)下载获得,如图 6-4 所示。本 实验所使用的 Zenmap 软件为 nmap-7.60-setup.exe。

NMAP.ORG		building tour	Online Business.				
Nmap Security Scanner • Intro • Ref Guide		WHAT IS	YOUR OPERAT Letting	ING SYSTEN OTHERS DO	Nmap	W namp -A -14 Starting Mage (Interesting Por Che 1667 port) PORT STMTE 22/16 open	
Install GuideDownload	Construction	Intro	Reference Guide	Book	Install Guide	25/5cp opn 55/5cp open 70/5cp closed 80/5cp open 113/5cp closed	
ChangelogBook		Download	Changelog	Zenmap GUI	Docs	Running: Linux OS details: Lin Uptime 26,177 o Interesting por	
Docs Security Lists	/	Bug Reports	OS Detection	Propaganda	Related Projects		
Nmap		In the Movies		In the News			
Announce Nman Dev							
 Bugtraq 	Introduction						
 Full Disclosure Pen Test Basics More Security Tools Password audit Sniffers 	Zenmap is the official Nmap Security Scanner GUL. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be						

②软件安装

管理科学与工程学科 / 阮晓龙 / 13938213680 / 共 6 页, 第4页

点击下载的 EXE 执行安装文件,可根据安装过程提示进行默认选择安装。 ③软件使用

打开工具,展示如图 6-2 所示工具界面。在"配置"下拉框中选择"Regular scan"(使用规则扫描),在"命令"输入框输入"nmap-p1-1024-T4-A-v172.16.124.127"命令规则, 点击【扫描】按钮,工具将自动扫描 IP 地址为"172.16.124.127"的主机,其1-1024 端口的 状态情况。

④信息查看

在"Nmap 输出"选项卡中可查看扫描的过程,如图 6-2 所示,查看主机端口的状态信息,并将信息填写到表 6-2 中。通过该工具可测试防火墙规则配置是否正确且生效。

扫描(a) 工具(T)	配置(P)	帮助(土)	
目标: 172.16.124	.127	▼ 配置: ▼ 扫描 用	取消
命令: nmap -T4 -	-v -p 1-1	024 -A 172.16.124.127	
主机服务	务	Nmap输出 端口/主机 拓扑 主机明细 扫描	
操作系统 ◀ 主机		nmap -T4 -v -p 1-1024 -A 172.16.124.127	月細
♥ 1/2.10	•	<pre>Starting Hmsp 1.00 (https://mem.org) at 2018-03-02 11:35 701d:&+v&:?) Initiating Parg Scan at 11:35 Scanning 172.16.124.127 [1 port] Completed APP Fing Scan at 11:35 .1.155 .2.45 at 11:35 Scanning 172.16.124.127 [1000 ports] Discovered open port 22/tc port 172.16.124.127 Completed SVM Stealth Scan at 11:35 .108 elapsed [1000 total ports] Failed to resolve "MBH". Failed to resolve "MBH". Failed to resolve "MBH". Host is up (0.00185 latercy). Port Sinte SteWard 127.155.155.155.155.155.155 Mix date: BigS(52):EES:055 (Whare) Read date file<u>f fromt (NFProgram Fi</u>ler (v80) Wharp Hmap done i f<u>address</u>(host up) (scanced in 43.99 seconds Read star file<u>f fromt (NFProgram Fi</u>ler (v80) Wharp Hmap done: 1 for 1991 (\$7.588KB) Revd: 29 (1.820KB)</pre>	
过调生机		图 6-5 扫描结果	_

表 6-2 端口检测结果



3、iptables 的应用

请根据下面的要求,写出防火墙的配置,将配置命令写入到实验报告册中。 ①允许来自于 IPA 地址的报文,通过 UDP 方式,访问系统的 4486 端口。

②丢弃来至 IPB 地址的使用 TCP 方式,访问系统 20 和 21 端口的报文。

管理科学与工程学科 / 阮晓龙 / 13938213680 / 共 6 页, 第5页

③允许 IP 地址属于 xxx.xxx.xxx/x 段的主机、由指定 eth0 网口,通过 SSH 远程连接本机。

④允许 IP 地址为 C 的主机通过 422 端口进行 SSH 远程连接本机。

⑤将来自 IP D 地址的主机使用 TCP 协议,访问 21 端口的数据包信息记录到 messages 日志中。

⑥当超过 100 个用户同时访问系统的 80 端口时,限制每分钟最大连接数为 25 个,防止系统遭受 DOS 攻击。



七、实验扩展

1、防火墙

(1)防火墙一共有几种?分别是什么,主要作用是什么?管理科学与工程学科 / 阮晓龙 / 13938213680 / 共6页,第6页

(2) iptables 防火墙是工作在计算机网络的哪一层上的?

2、iptables 防火墙规则

(1) iptables 防火墙规则除了可以通过配置端口、IP 地址,还能通过配置哪些选项来 制定防火墙策略? 请举例说明。

(2) 如何将防火墙规则进行备份?