网络操作系统综合实践

网络安全技术实践

班　　级：_____

姓　　名：_____

学　　号：_____

指导老师：_____

完成日期：_____

目录

一、实践的基本目的

实践环节给学生提供了一个实践机会，让学生自己动手在在 linux 操作系统下安装配置服务器、防火墙，并实现利用防火墙来控制内网与外网的通信。

要求学生通过实践能熟练掌握 linux 操作系统的基本概念、基本命令及该系统的管理，了解 linux 操作系统的网络功能及利用 linux 操作系统进行网络服务器的配置，并通过客服端进行验证。

通过本实践环节的训练，学生应达到以下要求：

（1）理解 ftp 服务器和 samba 服务器的基本概念，并且能够在 linux 操作系统下

安装、配置 ftp 服务器和 samba 服务器，并通过客户端验证。

（2）理解dhcp服务器、dns服务器和ssh服务器的基本概念，掌握在linux操作系统下安装、配置dhcp服务器、dns服务器及ssh服务器，并学习这些服务器的应用。

（3）理解 web 服务器和邮件服务器的基本概念，能够在 linux 操作系统下安装、配置 web 服务器和邮件服务器，并且通过 web 方式使用邮件服务器。

（4）理解防火墙的概念，在 linux 操作系统下安装、配置防火墙，并通过防火墙在实现内网和外网的通信。

二、实践的主要任务

实践的主要任务是：构建基于 linux 服务器的小型企业网络，配置各种的网络服务，并提供相应的安全措施。

首先，设计 Linux 系统下网络互连拓扑图；接着，在该操作系统下实现 nfs 服务器、samba 服务器、ftp 服务器、samba 服务器、dhcp 服务器、web 服务器、邮件服务器、ssh 服务以及防火墙的配置，对于 Linux 下服务器使用动态分配 IP 地址，并通过防火墙实现 Linux 系统下的网络互连，将防火墙作为网关控制内网和外网的通信；最后，通过 web 方式使用邮件服务器。

下面详细介绍本次实践的的任务：

（1）通过实验熟练掌握 linux 的基本命令；

（2）掌握 linux 下 ftp 服务器的配置方法，架设 ftp 服务器，实现匿名访问及对登录用户配置相关权限；

（3）掌握 linux 和 Windows 的文件共享方法，掌握使用 samba 文件服务器实现资料的共享；

（4）掌握 Linux 下的域名服务器的配置方法，架设 DNS 服务器，在客服端的/etc/resolv.conf 文件进行配置，用来指定 DNS 服务器的 IP 地址，实现在客服端正向及反向解析域名；

（5）掌握 linux 下 web 服务器的配置方法，架设一台 web 服务器，服务器使用 Apache 软件，实现用户权限认证访问 web，基于 ip 地址的虚拟主机的配置，以及个人主页的访问；

（6）掌握 linux 下邮件服务器的配置方法，使用邮件服务器采用自带的 Sendmail 软件，只转发本地网络的信件，并且建立一个邮件列表，包含所有人的邮件地址；

（7）掌握 Linux 下服务器动态分配 IP 地址的方法，架设 dhcp 服务，客户机使用动态 IP 地址分配，并且为服务器分配一个固定的 IP。

（8）选做：掌握 SSH 服务器的配置，实现用户远程登陆系统，且具有用户在本地相同的功能；

（9）掌握 nfs 服务器的配置，在 Linux 系统之间实现资源的共享；

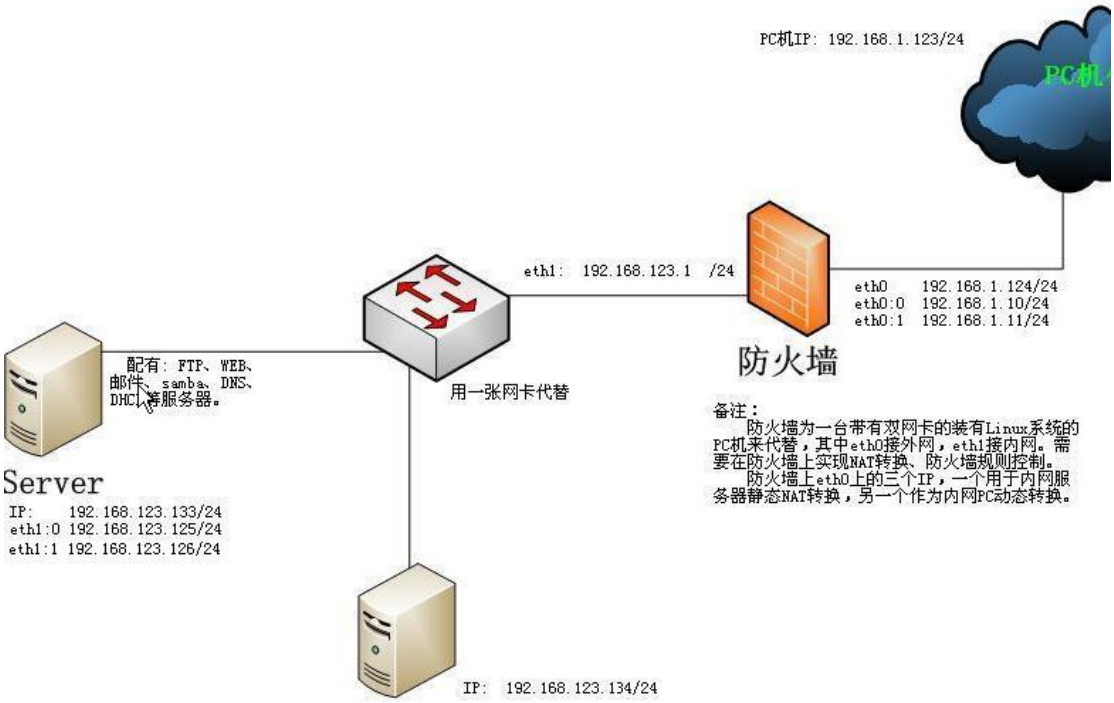
（10）在网关上安装防火墙，采用系统内置的 netfilter/iptables 软件，配置了一些基本的安全策略，实现内外网之间的通信：再添加具体的安全策略：允许内部局域网到互联网的全部数据通过防火墙，允许互联网上的计算机“ping”防火墙和访问 WWW 服务器。

三、需求分析

1.需求分析及环境搭建：

根据实践任务的要求，使用一台 Linux 作为内部网络的服务器，在此主机上配置所需的服务内容，在做 dhcp 服务时为其分配一个固定的 IP（192.168.123.125/24）与其网卡绑定；另外使用一台 Linux 主机作为内部网络（192.168.123.126/24）的代表机，采用动态 IP 获取的方式；另外，使用一台 Linux 主机作为连接内外网络的网关路由，在上面安装防火墙，配置基本的安全策略；最后，把我自己的主机当成外网的测试机（192.168.1.123/24）。

2.环境搭建方案拓扑：



如上拓扑图所示，内部网络的服务器和内测机是连接在同一虚拟机的虚拟网卡上的，作为一个内部的局域网；为作为防火墙的 Linux 主机添加两张网卡，作为内网口的网卡及内部网络以 host-only 的方式连接到虚拟网卡 vmnet3 上，作为外网口的网卡以桥接方式同真实主机连接。

四、服务配置及防火墙设置说明

1 ftp 服务器配置方法和步骤

（1）创建/var/vsftpd/upload 目录
（2）修改/var/vsftpd/upload 目录的权限
（3）编辑 vsftpd.conf，添加以下内容

```
write_enable=yes                    //可写
anonymous_enable=yes                //启用匿名用户
anon_root=/var/vsftpd               //匿名用户登录的指定目录
anon_umask=022                      //设置文件创建的掩码
anon_upload_enable=yes
```

//匿名用户可以向具备写权限的目录上传文件

anon_mkdir_write_enable=yes

//匿名用户可以在具备写权限的目录创建新目录

anon_other_write_enable=yes

//是否允许匿名用户可以使用除了建立文件夹和上传文件以外其他的 ftp 写操作命令

user_config_dir=/etc/vsftpd/user_config_dir

//用户单独配置文件所在目录

local_enable=yes //启用本地用户

local_umask=026 //设置文件创建的掩码

chroot_list_enable=no //不能切换到家目录之外，没有例外

chroot_local_user=yes //本地用户只能访问自己的家目录

chroot_list_file=/var/vsftpd/chroot_list

//chroot_list 的文件路径

userlist_enable=yes //启用 userlist 功能模块

userlist_deny=yes //拒绝 userlist 文件中用户登陆 ftp 服务

userlist_file=/var/vsftpd/user_list

//指定的 userlist 文件路径

(2)创建/var/vsftpd/chroot_list 文件，内容如下：

Fayero //这两个用户只能登录到自己的家目录

clinux

(3) /var/vsftpd/user_list，内容如下：

root //不能用 root 用户登入 ftp 服务器

(4)在/var/vsftpd/user_config_dir 目录下编辑 clinux 文件，内容如下：

write_enable=no //使 clinux 用户没有写的权限

2 samba 服务器配置说明

编辑配置文件：vim /etc/samba/smb.conf,

（1）在[global]部分设置 security = user //用户身份验证模式

（2）并添加以下内容 ：

```
[samba]
path = /tmp/samba                    //登录 samba 的目录
browsable = yes                      //允许浏览
read list = user01                   //user01 用户只有读的权限
write list = @share                  //share 组用户中有写的权限
```

3 dns 服务器配置说明

(1)配置主 dns，编辑配置文件；

vim /var/named/chroot/etc/named.conf

vim /var/named/chroot/var/named/localhost.zone

vim /var/named/chroot/var/named/localhost.arpa

vim /var/named/chroot/var/named/jsj.zone

vim /var/named/chroot/var/named/jsj.arpa

查看错误：tail /var/log/message

(2) 配置辅助 dns，只需配置主配置文件：

(3)修改/var/named 的所有者和群组：chown -R named:named /var/named

(4) 在 linux 客户端，通过修改/etc/resolv.conf 来设置主 dns 和辅 dns：

nameserver 192.168.2.x

nameserver 192.168.2.y

4 dhcp 服务器配置说明

(1) 编辑/etc/dhcpd.conf:

```
ddns-update-style ad-hoc ;                  //更新方式
#default-lease-time 28800;                  //默认租约期限
max-lease-time 43200;                       //最大租约期限
option subnet-mask 255.255.255.0;           //子网掩码
option broadcast-address 192.168.2.255;     //广播地址
option routers 192.168.2.10;                //默认网关
```

```
option domain-name-servers 59.77.139.1;     //DNS 服务器的 IP 地址
option domain-name "c2501.com";             //DNS 域名
subnet 192.168.2.0 netmask 255.255.255.0 {
      range 192.168.2.1 192.168.2.254;      //可分配的 IP 地址范围
    host hostname {                         //给服务器绑定特定 IP
    hardware ethernet 00:0C:29:2B:29:3D;
    fixed-address 192.168.2.10;
   }
 }
```

5 web 服务器配置说明

（一）Apache 服务器：用户权限认证

（测试是否安装 Apache 服务器　rpm –qa | grep httpd）

(1) 编辑/etc/httpd/conf/httpd.conf,添加如下内容:

```
Alias /httpd  “/var/www/httpd”                  //别名
<Directory  “/var/www/httpd”>
Options Indexes MultiViews                      //允许列目录
DirectoryIndex index.html index.html.en         //设置预设首页
AllowOverride AuthConfig                        //启用身份认证
</Directory>
```

(2) 在/var/www/httpd/目录下编辑.htgroup 文件，内容如下：

```
allowuser：jack  tom                            //用户分组授权文件
```

(3) 添加 jack 用户：htpasswd -c /var/www/httpd/.htpasswd jack

(4) 添加 tom 用户：htpasswd /var/www/httpd/.htpasswd tom

(5) 在//var/www/httpd 目录下编辑.htaccess 文件，内容如下：

```
AuthName  “This is a test”                      //设置使用认证的领域
AuthType Basic                                  //加密方式为 Basic
AuthUserFile /var/www/httpd /.htpasswd          //设置密码文件
AuthGroupFile //var/www/httpd /.htgroup         //设置用户组文件路径
require group allowuser                         //允许访问的群组
```

（二）基于 ip 地址的虚拟主机的配置

（1）编辑 Apache 主配置文件，主要内容如下：

<VirtualHost 192.168.2.11>

ServerName 192.168.2.11:80　　//虚拟主机名

ServerAdmin web1@163.com

DocumentRoot "/tmp/web1"　　/ /虚拟主机文档位置

DirectoryIndex index.html index.html.en　　//设置预设首页

ErrorLog logs/web1/error_log　　//设置错误记录文档

CustomLog logs/web1/access_log combined

</VirtualHost>

（2）添加两个虚拟 IP，并创建相应的目录。

（三）Apache 服务器：个人主页（~test）配置

（1）添加用户 test；

（2）编辑 Apache 主配置文件：

修改<IfModule mod_userdir.c> </ifModule>部分

UserDir disable，在前面加“#”注释掉此行，并修改为 UserDir enable test；

继续向下查找 UserDir public_html,将前面的“#”去掉，使生效。

保存退出　//设置用户是否可以在自己的目录下建立 public_html 目录来放置网页。

（3）使用 test 用户登录 ： 在宿主目录下创建 public_html 目录，并在此目录下放置主页 index.html, 在 home 目录下，赋予其他用户对 test 有可执行的权限： chmod o+x test

6　nfs 服务的配置说明

编辑配置文件: vim /etc/exports

/tmp/nfs　　192.168.2.10(rw,sync,no_root_squash)

192.168.2.0/24(rw,sync,root_squash)　　//用户可读写，同步，有映射

/tmp/fayero　*(rw,anonuid=501，anongid=501)

//登陆后映射为 uid=501，gid=501 的用户

7 邮件服务器的配置方法和步骤

（一）邮件系统域名解析配置，MTA 配置与安装，POP3 与 IMAP 配置的步骤基本上和指导书上一致，参见附件。

（二）这里主要说明一下 openwebmail 软件安装时的注意事项。

（1）安装 openwebmail 软件包，所需软件包有

openwebmail-data-2.53-3.i386.rpm

openwebmail-2.53-3.i386.rpm

由于这两个软件包有依赖关系，安装时必须同时安装，否则会陷入死循环

rpm -ivh openwebmail*.rpm

这两个软件包还有依赖性的软件包：

perl-suidperl-5.8.5-12.1.1.i386.rpm

perl-Text-Iconv-1.4-1.2.el4.rf.i386.rpm

需要在上面两个包安装前先安装。

（2）初始化 openwebmail

cd /var/www/cgi-bin/openwebmail/

./openwebmail-tool.pl --init

（3）配置

vim /var/www/cgi-bin/openwebmail/etc/openwebmail.conf

修改 domainnames auto 改成 domainnames c2501.com

default_language en 改成 default_language zh_CN.GB2312

default_iconset Cool3D.English 改 成 default_iconset Cool3D.chinese.Simplified

8 防火墙的配置方法和步骤

（1）防火墙的路由配置（eth0 为内网口，eth1 为外网口）

echo "1" > /proc/sys/net/ipv4/ip_forward **//开启 linux 的转发功能**

（2）加载模块

modprode ip_tables **//加载模块 ip_tables**

modprode ip_nat_ftp **//加载模块 ip_nat_ftp**

（3）配置防火墙的 nat 转发功能

iptables -t nat -A PREROUTING -d 192.168.1.254 -i eth1 -j DNAT --to-destination 192.168.2.10

//将外网目的地址为 192.168.1.254 的数据包转为目的地址 192.168.2.10（服务器）上

iptables -t nat -A POSTROUTING -s 192.168.2.10 -o eth1 -j SNAT --to-source 192.168.1.254

//将源地址为 192.168.2.10 的数据包转为源地址为 192.168.1.254 的数据包

iptables -t nat -A PREROUTING -d 192.168.1.253 -i eth1 -j DNAT --to-destination 192.168.2.1-192.168.2.254

//将目标地址和源地址对应

iptables -t nat -A POSTROUTING -s 192.168.2.0/255.255.255.0 -o eth1 -j SNAT --to-source 192.168.1.253 //将源地址和目标地址对应

（4）允许内部局域网到互联网的全部数据通过防火墙，允许互联网上的计算机“ping”防火墙和访问 WWW 服务器。

iptables -P FORWARD DROP //FORWARD 转发策略为ＤＲＯＰ

iptables -A FORWARD -i eth1 -o eth1 -p tcp --dport 80 -j ACCEPT

/ / 转发从外网向内网发送的ｈ ｔ ｔ ｐ请求，允许外网访问内网的ｗ ｅ ｂ

Iptables -A FORWAED -i eth0 -o eth1 -j ACCEPT

//允许转发内网向外网发送的任何数据

iptables -A FORWARD -i eth1 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

/ / 转发从外网到内网的处于 ESTABLISHED,RELEAED 状态的信息

iptables -P INPUT DROP

iptables -A INPUT -p icmp -j ACCEPT //只允许 ping 防火墙

六、总结