**Morning**

1. SELinux概述（Security-Enhanced Linux）

-增强Linux系统安全的强制访问控制体系

-集成到Linux内核（2.6及以上）中运行

1. SELinux运行模式

-enforcing（强制）、permissive（宽松,日志记录）、disabled（彻底禁用）

-任何一种运行模式，变成Disabled都要经历重启系统（反之也是）

-切换运行模式

getenforce #查看当前运行模式

setenforce 1|0 #临时切换enforcing|permissive

#永久配置文件路径：/etc/selinux/config

1. 搭建基本的web服务

-安装httpd（Apache）软件包（服务端软件）

-重启httpd服务

systemctl restart httpd

systemctl enable httpd （提示ln -s创建快捷方式）

-验证本机访问测试 firefox 172.25.0.11

#显示红色测试页面表示测试成功，但没找到页面

-书写一个页面

网页文件默认存放路径：/var/www/html

默认网页文件的名字：index.html

例：cat /var/www/html/index.html

<marquee><font color=red><h1>食屎啦梁非凡!

#<滚动效果><红色字体><最大字体>

4、搭建FTP服务（文件数据传输）

端口：20、21（21用于连接、20用于传输数据）

-安装vsftpd软件包

-重启vsftpd服务

默认共享数据目录/var/ftp

默认的配置文件/etc/vsftpd/vsftpd.conf

关于匿名用户的配置语句为anon开头。如anon\_upload\_enable

**Afternoon**

1、防火墙（隔离作用）

-硬件防火墙（保护网络内部）

-软件防火墙（保护系统本身）

firewalld服务：默认安装，随机自启

管理工具：firewall-cmd（命令）、firewall-config（图形）

-预设安全区域（根据所在的网络场所区分，预设保护规则集）

trusted：允许任何访问

block：阻塞任何来访请求，明确拒绝

drop：丢弃任何来访的数据包，直接丢弃

其他区域：除明确允许的以外全部拒绝

public：仅允许访问本机的sshd，ping，dhcp等少数几个服务

-防火墙进入区域的规则：匹配及停止

1. 根据数据包的源IP地址
2. 根据数据包从哪块网卡收到
3. 进入默认区域

2、配置安全区域

虚拟机server端：

firewall-cmd --get-default-zone #查看默认区域

firewall-cmd --set-default-zone=block #修改默认区域为block

firewall-cmd --zone=public --list-all #查看public区域当前规则

firewall-cmd --zone=public --add-service=ftp #临时加ftp协议

firewall-cmd --permanent --zone=public --add-service=ftp

#永久添加ftp协议

firewall-cmd --reload #重新加载永久配置

firewall-cmd --zone=block --add-source=172.25.0.10

#添加源ip，单独拒绝172.25.0.10

虚拟机desktop端：

firefox 172.25.0.11 #测试http服务

firefox <ftp://172.25.0.11> #测试ftp服务

1. 端口转发

数据包：数据 源ip地址 目标ip地址 目标端口号

-端口号：编号，标识程序及应用、服务

-互联网常见协议：

http：超文本传输协议，默认端口号80

https：安全的超文本传输协议，443

FTP：文件传输协议，21

DNS：域名解析协议，53

SMTP：用户发邮件协议，25

pop3：用户收邮件协议，110

talnet：远程管理协议，23

TFTP：简单的文件传输协议，69

SNMP：网络管理协议，161

#协议的端口可以由root改变，也可以具备多个端口

-本地应用的端口重定向（端口1--->端口2）

firewall-cmd --permanent --zone=public --add-forward-port=port=5423:proto=tcp:toport=80

#设置端口转发

firewall-cmd --reload #重载配置,重置

1. 配置IPv6地址

-128个二进制组成，利用冒号分隔8部分，最终每一部分利用4个16进制数表示，网络位/主机位均为64位

-nmcli connection...ipv6.method ..ipv6.addresses ‘’ #配置v6地址

-ping6 2003:ac18::305

1. 配置聚合连接（链路聚合）

-创建虚拟网卡team0，参考man teamd.conf

-轮询式(roundrobin)、热备份(activebackup)

1）添加虚拟网卡team0

nmcli connection add type team con-name team0 ifname team0 autoconnect yes config '{"runner": {"name": "activebackup"}}'

#nmcli connection 添加 类型为 team(队伍) 配置文件名 team0 网卡名 team0 每次开机自动启动 工作模式为 热备份

#参考 man teamd.conf --->/example

nmcli connection delete team0 #删除team0，打错了必须要删

1. 添加成员

nmcli connection add type team-slave con-name team0-1 ifname eth1 master team0 #把网卡eth1添加到team0中

nmcli connection delete team0-1 #删除成员team0-1 (按配置文件名)

1. 为虚拟网卡team0配IP地址

nmcli connect ... Ipv4.address 192.168.1.1/24 ...

1. 激活设备（先激活主设备）

nmcli connection up team0

nmcli connection up team0-1

5）专用于查看链路聚合的命令

teamdctl team0 state

ifconfig eth1 down #把eth1禁用

1. 自定义命令

-永久别名的配置

~/.bashrc，影响当前用户，每次开启终端才会生效

/etc/bashrc，优先影响所有用户，每次开启终端才会生效