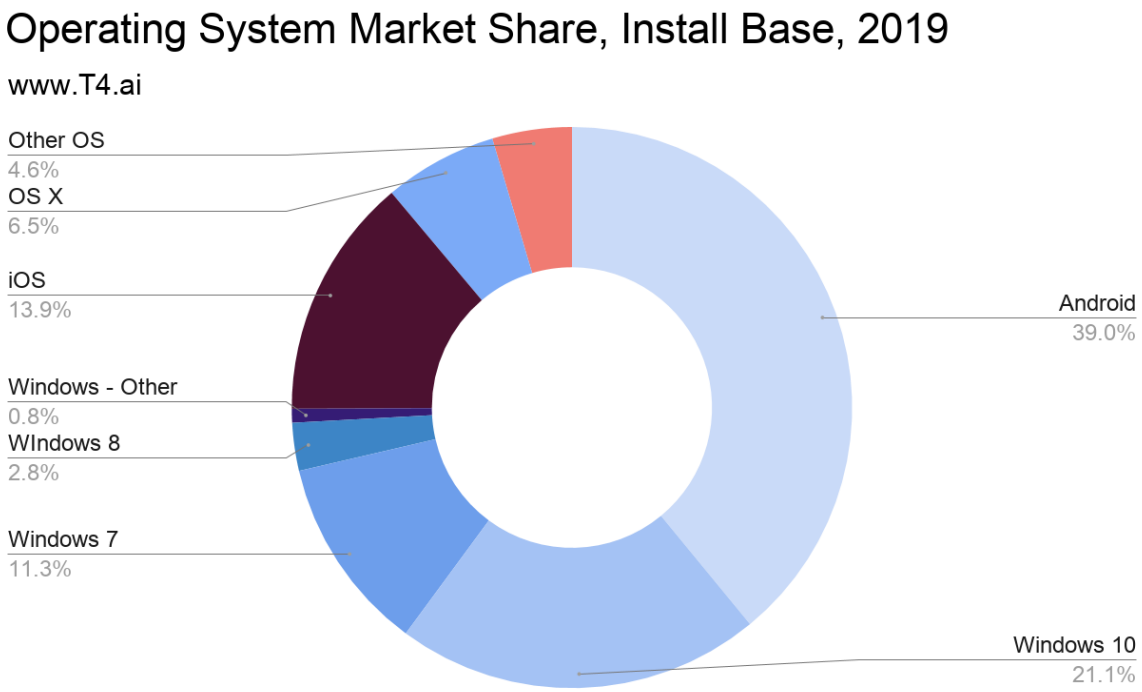
리눅스 실습

- CentOS 8 -

***** 목차 *****

1. 리눅스란 무엇인가?

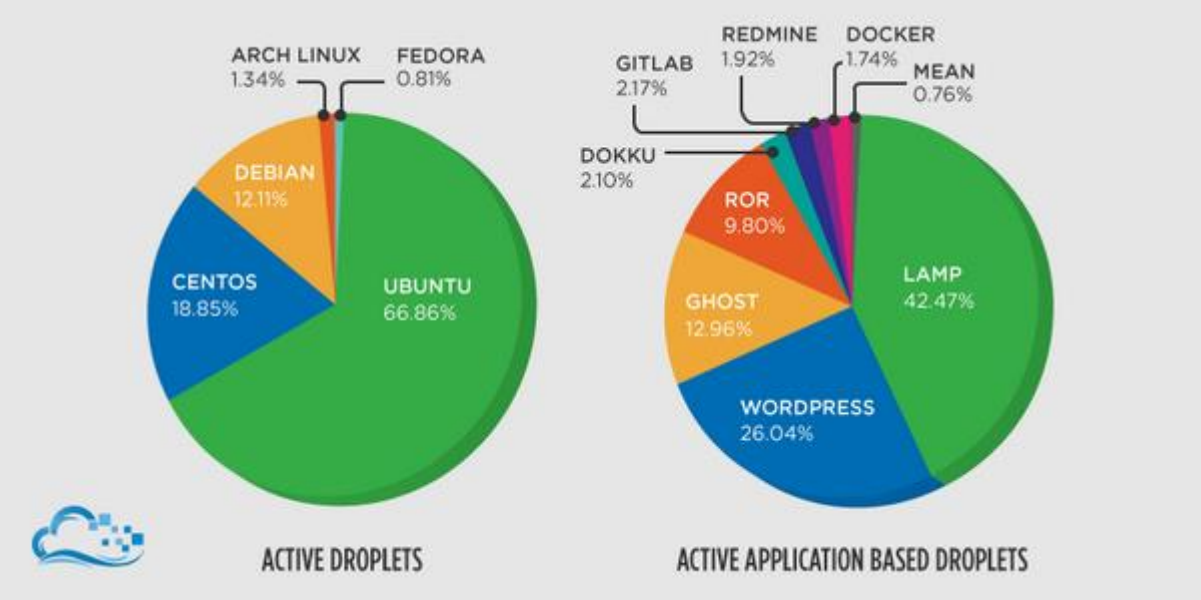


미래에는 점차 Windows의 비중이 줄어들고, 범 리눅스 계열의 운영체제들이 점점 비중이 높아지게 될 것이다.

- 4차산업혁명시대의 리눅스의 중요성

1) IoT : IoT 기기들의 운영체제는 대부분 Linux를 기반으로 한다.
2) Cloud : 클라우드에서 사용하는 운영체제의 대부분은 리눅스이다.
3) Big data : Big data 분석을 위해서는 Cloud에서 실행하는 것이 최근의 추세이다.
4) Machine Learning : 머신러닝도 최근 Cloud에서 실행하는 것이 최근의 추세이다.
5) AI : 인공지능도 최근 Cloud에서 실행하는 것이 최근의 추세이다.
6) Blockchain : Blockchain 채굴기의 대부분은 Linux기반이다.

- 어떤 리눅스를 배워야 할까?



- IoT, Cloud에서 최근의 추세는 Ubuntu이다.
- 국내에서는 Red Hat의 비중이 높아 CentOS를 사용하는 경우가 많지만, 전세계적으로는 Ubuntu를 가장 많이 사용하고 있다.

- 리눅스에 어떤 Application을 많이 사용하고 있을까?
- 단연 LAMP. Linux기반의 Apache, MySQL/MariaDB, PHP를 LAMP라 한다.
- 그 다음으로는 WordPress가 2위
- LAMP와 WordPress를 잘 사용할 수 있도록 연습해야 한다.

2. 리눅스 설치 준비

* VMware 다운로드 방법

https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

Windows용 지금 다운로드 클릭

(다시 시작 하지 마세요. 수업 마치고 해도 됩니다.)

* CentOS 다운로드 방법 (CentOS 8버전으로 다운로드 합니다.)

https://vo.la/YYRio

* VMware IP 변경

https://cafe.naver.com/cloudengineer/4

vmnetcfg_v15.zip 파일을 다운로드 합니다. 압축을 풀면 vmnetcfg.exe를 복사해서

C:₩Program Files (x86)₩VMware₩VMware Player 에 붙여넣기 (관리자 권한 승인)

vmnetcfg.exe를 관리자 권한으로 실행합니다.

VMnet8의 IP를 192.168.5.0 으로 변경 (세번째 옥텟만 5로 변경합니다)하고 ok클릭

* 리눅스 버전

- 리눅스가 버전마다 설치나 사용 방법이 다름
- 메이저 버전 : CentOS7, CentOS8, ... ------> 많이 다름
- 마이너 버전 : CentOS7.1, 7.2, 7.3, 7.4 -------> 일부 다름

* 리눅스 실습할 때 주의사항

- 막히는 부분이 생김 ----> 실망하거나 좌절하지 말것!!!
- 책대로 잘 안됨.... (버전이 달라지면 다르게 동작 ---> 다른 리눅스라고 생각하면 됨)
- 달라진 부분은 저자의 까페 또는 구글에서 검색해서 찾아봐야 함 ----> 공유하고 노하우로 작성해놓을 필요성
- 실습한 내용을 캡쳐 또는 기록의 필요성 ----> 안됐던 부분을 어떻게 해결했는지 리포트 작성 또는 블로그에 써놓음 (공유)

----> 시행착오를 최소화하도록 함. 노하우를 모아서 에러노트를 만듦

* 스마트폰, 클라우드, IoT, 딥러닝, AI등에서도 모두 리눅스를 사용 ---> 무료
  윈도우를 사용하면 데이터센터에 추가 비용이 발생 ex) 10만원*5만대 = 50억...

* 가상머신 : HW에 운영체제 설치하고 그 위에 가상환경을 지원하는 도구(VMware, Virtualbox, Hyper-V등)를 설치하고 그 위에 리눅스, 윈도우, 맥OS 등을 설치하여 사용하는 것
- 진짜 컴퓨터를 host OS로 부르기로 함
- 가상머신은 guest OS로 부르기로 함

* VMware
- Workstation Pro : 상용버전, 모든 기능이 다 있음. (30일 동안은 무료로 사용 가능)
- Player : 비상업적인 경우 무료로 사용 가능. 단, 기능제한이 있음 (스냅샷, IP변경 안됨 등)
  (상업적인 용도는 가상머신을 임대해서 수익창출...)

*** 본격적으로 설치해봅니다.**

Edit Virtual Machine Settings

1) 메모리를 2048로 변경(2G)

2) CD/DVD 클릭해서 Brower클릭해서 CentOS 다운로드 받은 위치에 가서 CentOS-~~~~-dvd1.iso 선택

Play Virtual Machine 클릭

remind me later 클릭

Install CentOS8 선택(화살표키로 이동해서 선택)하고 엔터

(만약에 마우스 바깥으로 안나오면 ctrl키와 alt키를 동시에 눌렀다 떼면 됨)

English ----- English (United States)

루트 패스워드 : telecom

노란색 세모 표시가 나오면 마우스로 클릭해서 무슨 문제가 있는지 해결하고 Done을 클릭

Begin Install 클릭

(VMware Tool 설치할꺼냐고 물어보면 Never Remind me 클릭)

Reboot System 클릭

* 설치가 끝나면 아래와 같이 실습해 봅니다.
  목표) 계정 생성 : blackpink / princess

terminal을 열고
$ date   // 현재 시간을 표시해 줌
$ sudo date   // 패스워드 입력하면 관리자 권한으로 사용 가능
$ ls   // 디렉토리에 있는 디렉토리나 파일의 이름을 보여줌 (List)
$ ls -l   // 상세 보기
$ pwd   // 현재 위치 보기
$ whoami   // 현재 로그인 한 계정의 이름을 알고 싶을 때
$ who   // 현재 접속자 리스트 : Multi-User OS이므로 여러 명이 동시접속 가능

터미널 창을 열고
$ sudo ifconfig   // 네트워크 상태를 볼 수 있는 명령
  (sudo : switch user do, 루트 권한을 사용하겠다)

참고) VMware에서 1~127까지는 수동으로 IP를 사용할 수 있는 구간, 128~253번까지는 DHCP(자동주소 할당 구역) 구간이 됨

* 기타 설정하기
1) 시간 설정하기
- 전원버튼 - 설정(드라이버와 스패너 모양) - Details - Date & Time - Time Zone을 클릭하고 KST로 변경 (검색창에 seoul 입력)
- 시간 설정 : Automatic Date & Time을 Off 하고, Date & Time 클릭해서 현재 시간으로 맞추어줌 (시간 부분만 변경하면 됨)

2) 화면이 잠기지 않도록 설정
- 설정 - Power - Blank Screen - Never 선택
- 설정 - Privacy - Screen Lock - Automatic Screen Lock ----> Off
  (단, 보안에 좋지 않으니, 실습 환경이 아니면 주의해야 함)

3) 가상 머신 끄는 방법
- Suspend : 사용하던 상태 그대로 저장했다가 다시 불러올 수 있음
- Power off : 정상 종료 (Software update : Remind me later 선택)

3. 리눅스 기본

* 리누스 토르발스 : 리눅스를 처음 만든 사람 (Linus + Minix = Linux)
- Kernel만 만듦 (나머지는 수많은 사람들의 노력으로 현재의 리눅스로 발전하였음)

* 리눅스 배포판 = 커널+컴파일러+셸+기타 응용프로그램
- Redhat 계열 : CentOS, Fedora 등 (우리나라에서는 Redhat을 많이 사용, CentOS가 Redhat과 가장 비슷)
---> Redhat 9까지만 무료, 이후 유료
- Debian 계열 : Ubuntu 등 (미국 등에서 IoT, Smart기기에서 Ubuntu를 많이 사용)

* GNU Project (GNU's Not Unix! ----> GNU : 그누)
- GNU는 온전히 자유 소프트웨어로 이루어져 있음 (자유 소프트웨어 : 무료 및 복제 가능)
- Unix는 상용 프로그램이므로, GNU는 상용이 아니다라는 의미 (누구나 쉽게 소프트웨어를 무료로 자유롭게 사용)

* GPL 라이센스 (General Public Licence)
- 수정과 공유에 있어서 기본적인 자유를 보장
- 진정한 자유란? : 사용, 수정, 재배포 및 이익을 전체가 얻을 수 있도록 배포할 자유

* 다음은 GPL의 주요 특징이다. (GPL은 한마디로 오픈 소스 프로그램 개발자 또는 판매자를 위한 라이센스이다.)
- GPL 라이센스 프로그램을 어떠한 목적으로든지 사용할 수 있다. 다만 법으로 제한하는 행위는 할 수 없다.
- GPL 라이센스 프로그램의 소스 코드를 용도에 따라 변경 할 수 있다. (개작 가능)
- GPL 라이센스 프로그램을 판매/배포시 소스 코드도 요청하면 제공하여야 한다. (원본 배포 의무)
- 변경된 컴퓨터 프로그램 역시 프로그램의 소스 코드를 요청시 제공해야 한다. (파생물 배포 의무)
- 변경된 컴퓨터 프로그램 역시 반드시 똑같은 GPL 라이선스를 취해야 한다. (파생물 라이선스 의무)

* 저작권(Copyright) 소개 -----> Right는 권한 또는 권리
http://www.copyright.or.kr/

* Copyleft : Copyright의 반대개념
카피레프트 또는 저좌권은 저작권에 반대되는 개념으로, 저작권에 기반을 둔 사용 제한이 아니라 저작권을 기반으로 한 정보의 공유를 위한 조치이다. 즉, 저작권 소유자가 자신의 창작물을 무료로 사용하도록 허용하는 것이다.

* 커널 확인 방법

$ uname -r //커널 버전 확인 방법

* 리눅스 배포판

- Red Hat : 유료이지만 설치, 문제해결 등을 지원 (RHEL : 레드햇 엔터프라이즈 리눅스)
- CentOS : 무료이지만, 문제 생기면 혼자 해결 -----> 구글 검색, Linux 커뮤니티(국내, 해외 등)
- Fedora 공식 웹사이트 : https://getfedora.org/

- X window : 마우스, 바탕화면, 폴더 등이 보이는 화면 (메모리를 많이 차지함 ----> 서버 버전에서는 사용하지 않음)
- GUI (Graphic User Interface) : 그래픽 사용자 환경
- CLI (Command Line Interface) : 터미널 창에 명령어를 입력하는 환경

* 터미널 프롬프트

// 관리자(root)권한

$ // 일반사용자 권한

$표시 상태에서 관리자 권한을 사용하려면

1) 명령어 앞에 sudo를 붙이고 사용

2) 관리자 모드로 전환하는 방법

```
sudo  -i      ( 또는 sudo -s를 사용하기도 함)
su -
su
```

* 전원 끄는 명령 ----> 관리자 권한

```
poweroff
shutdown -P now
halt -p
init  0
```

```
# shutdown --help
      --help            Show this help
   -H --halt            Halt the machine
   -P --poweroff        Power-off the machine
   -r --reboot          Reboot the machine
```

```
  -h                    Equivalent to --poweroff, overridden by --halt
  -k                    Don't halt/power-off/reboot, just send warnings
     --no-wall          Don't send wall message before halt/power-off/reboot
  -c                    Cancel a pending shutdown
```

* 종료 방법 사례

```
shutdown   -h   now          // 즉시 정상 종료하라는 의미  -----> 나 혼자만 사용하는 경우 가능
shutdown   -P   +10          // 10분후에 종료함 -------> 다른 사용자들에게 작업을 저장할 시간을 줌
```

* 시스템 재부팅

```
shutdown   -r   now                  //   -r : reboot
reboot                               // 가장 많이 사용
init   6                             // 시험에 많이 출제 됨
```

* Multi-User 환경 : 여러명이 하나의 컴퓨터를 공동으로 사용

- Linux에서 실행되는 Application들이 종료되면 안되므로 Linux를 전원 Off하면 안됨
  (Application의 사례 : 웹서비스, 출입문 관리 서비스, 인텔리전스 빌딩의 전원관리, 공기정화기능 등등)
- 자신의 작업이 끝나면 로그아웃하고 나가면 됨 (관리자는 여러명일 수 있음)

* Run Level

```
# cd /lib/systemd/system
# ls -l runlevel?.target
```

* 자동완성과 history

```
pwd
whoami
ls
who
history                      // 방금 사용했던 명령어를 확인 가능
history    --help            // 옵션 리스트 확인
history
history    -d   [번호]       // 해당번호를 지우는 방법
```

실습) whoami 했던 명령을 삭제해보기 (만일 whoami가 5번이면)

```
history    -d   5
history    -c                // 전체 히스토리 삭제
```

자동 완성은 키보드에 있는 위화살표키(과거 명령), 아래화살표키(최근 명령) 사용 가능

cd ~ // 자기의 홈디렉토리로 이동 (root권한이므로 /root 위치로 이동하게 됨)
pwd // 현재 위치 확인 가능

실습) 자동완성 작업
디렉토리 또는 파일의 앞부분만 입력하고 Tap키를 누르면 자동으로 완성이 됨
ls // 파일인지 디렉토리인지 알 수 없음
ls -l // 맨 앞부분이 d면 디렉토리, -이면 파일

cd /etc
cd sysco<tap>

cd / // 리눅스의 최상위 디렉토리로 이동
ls // 디렉토리 리스트 보여짐
ls -l // 상세보기
디렉토리는 d로 표시
링크는 l로 표시 (바로가기 링크)
파일은 -으로 표시

일반사용자의 홈 디렉토리는 /home 아래에 존재 ex) /home/blackpink
루트의 홈 디렉토리는 /root 임

4. 에디터 사용

- gedit : GUI(X Window)환경에서 사용 가능
- vi : GUI가 없는 경우에도 사용 (서버 관리자 등 vi를 많이 사용, 서버 세팅, 구성 변경 등)

실습4

// root권한 & Root 사용자 상태로 명령어 사용

GUI (바탕화면, 마우스 클릭) -------> Blackpink 계정으로 사용 -----> root의 홈디렉터리에 저장할 수 없음

cd /home/blackpink

ls -l

test1.txt

* vi와 vim의 차이

- 옛날 vi : 사용하기 어려움
- vim : 사용하기 쉬워짐

dnf install vim // 최신 vim으로 업그레이드 됨 ----> 명령어는 똑같이 vi 사용

vi test1.txt

화살표키로 왔다갔다 이동 가능

맨 아랫줄로 이동

i // 편집모드 상태로 전환됨 (--insert--)

(글씨 작성)

ESC 키를 누름 // 편집모드 종료됨

:wq // 저장하고 종료 (write and quit)

* 종료 옵션

:wq //저장하고 종료

:q! // 저장하지 않고 종료 (!는 확인하지 말고 그냥 실행하라는 의미)

ex) 실수로 무언가 변동이 생겼을 때

:wq! // 저장하고 종료 (!는 확인하지 말고 그냥 실행하라는 의미)

:w // 중간 저장 (변동이 많을 때는 중간 중간 저장할 필요가 있음)

:q // 저장이 안된 상태에서는 빨간색 경고메시지가 보임

* 매뉴얼 보는 명령 (manual의 약자는 man)

man vi

- 아래줄로 내려가는 방법 : pageup, pagedown, 마우스 스크롤, 스페이스 바 등
- 종료할 때는 q를 누름

실습)

vi new.txt // 기존에 있는 파일이 수정되거나 파일이 없으면 새로 생성됨
vi // 파일명을 지정하지 않으면 새로운 문서가 열림
:w 파일명 // 파일명으로 저장함
:wq 파일명 // 파일명으로 저장하고 종료함

* vi 편집 기능 : 오래된 vi를 사용할 수 밖에 없는 경우가 있으므로 알고 있어야 함

hjkl : 좌하상우
^ : 캐럿 = home
$: = end
gg : 맨 처음으로 이동
x : 한글자 삭제
X : 앞글자 삭제(=backspace)
dd : 한줄 삭제
. : 앞에 수행했던 명령 반복
:set nu // 왼쪽에 줄 번호 표시하기 (자주 사용하므로 반드시 기억)
(:set number라고 입력하는 것이 맞지만, 줄여서 :set nu라고 많이 사용함)

* 문자열 바꾸기

:%s/기존문자열/새문자열
ex) :%s/centos/linux centos를 linux로 변경하는 방법

cf. password.lst 파일은 자주 사용하는 패스워드를 모아놓은 파일 (Password Dictionary라고 함)
실습) password.lst 파일을 복사해서 /home/(사용자계정) 에 붙여넣기 하세요.
vi password.lst
#으로 시작하는 부분은 모두 주석 -----> 주석 삭제하기
gg //맨처음으로 이동
dd //한줄 삭제
. // 앞명령 반복
실습) 주석 부분을 삭제해서 123456이 맨 위로 오도록 수정해보세요.

:w

:set nu

(20번째 줄에 있는 123을 trump로 수정하세요.)

gg

/trump //trump가 포함된 단어를 찾아줌

/trump //trump 이후에는 trumpet을 찾아줌

22번줄이 비어있음(Null) -----> korea로 변경

:w //중간 저장

yy //한줄 복사

p //(소문자p) 현재 행 이후에 붙여넣기

P //(대문자P) 현재 행 이전에 붙여넣기

5. 파일 및 디렉토리 관리

1) 리스트 (ls : list)

ls -a

ls -l을 줄여서 ll (엘엘)로 입력 가능

2) 이동 (cd : change directory)

```
cd                          // 홈 디렉토리 이동
cd ~blackpink
cd ..                       //한 수준 위로 올라감

cd /usr/local                          // 가장 최상위를 기준으로 찾아 들어가는 방법
cd ../lib                              // local과 같은 수준의 옆에 있는 디렉토리로 이동
cd ..                                  // 부모 디렉토리로 올라감
```

3) 현재 위치

```
pwd                                 // 현재 위치를 확인 (Print Working Directory)
```

4) 삭제 (rm : remove)

```
rm                                  // remove    삭제 명령
cd ~blackpink
rm  new.txt                         // 파일은 별다른 옵션 없이 그냥 삭제됨
rm  -r  [디렉토리명]                 // 디렉토리 삭제              ( -f를 추가하면 물어보지 않고 삭제)
mkdir  new                          // new디렉토리 생성
rm  -r  new                         // new딕렉토리 삭제
rm  -rf  new                        // 안물 삭제
```

5) 복사

```
cp    test1.txt     text4.txt              //같은 디렉토리 이므로 파일명이 달라야 함
cp    test1.txt     /usr/local/src           // 다른 디렉토리로 복사할 때에는 위치만 지정하면 됨
mkdir    matrix
cp  -r  matrix  /usr/local/src                 //디렉토리 복사
```

6) 생성 또는 최종 수정시간 변경

```
cd
touch  abc.txt
```

7) 파일 이동

mv /root/abc.txt /home/blackpink

8) 디렉토리 만들기

mkdir [디렉토리명]

9) 디렉토리 삭제

rmdir [디렉토리명]

= rm -r [디렉토리명]

10) 문서 내용을 읽기

cat [파일명] //짧은 길이의 문서를 읽을 때

cat /etc/passwd //계정정보 출력

cat /etc/hosts // IP주소와 도메인 네임이 연결되어 있는 파일

cat /etc/group // 그룹리스트 조회

11) 로그 분석할 때 많이 사용

head [파일명] // 위에서부터 볼 때 (오래된 로그)

head -20 /var/log/secure // 위에서부터 20줄만 볼 때

tail [파일명] // 아래에서부터 볼 때 (최신 로그)

tail -20 /var/log/secure // 아래에서부터 20줄만 볼 때

tail -f /var/log/messages // finishless(끊지 말고) 계속 최신 로그를 실시간으로 보여달라는 의미

(Firefox를 켜면 메시지에 새로운 로그가 생성 됨)

종료하려면 ctrl + c 를 누르면 취소됨

12) more

more [파일명] //페이지 단위로 출력하라는 명령

(페이지를 넘길 때는 space bar를 누른다. 종료할 때는 q를 누른다.)

13) 긴 문서를 볼 때

less password.lst // pageup/pagedown으로 올리고 내리고 가능

종료할 때는 q를 입력

14) 화면을 깨끗하게 할 때

clear

ctrl + l // clear와 동일함

과제) worst-passwords-2019.jpg 파일의 내용을

vi로 작성하고, https://cafe.naver.com/cloudengineer/ '과제제출'에 업로드 하세요.

주석에 자신의 이름 이니셜 (홍길동이면, made by hgd)

파일명은 worstpassword_2019.txt (텍스트파일)로 작성, 작성 한 내용을 리눅스 화면도 캡쳐해서 같이 업로드

주석 작성 방법

Made by hgd

yy // 한줄 복사

p // 아랫줄에 붙여넣기

* vi 명령어들

yy : 한줄 복사

p (소문자p) : 아래에 붙여넣기

P (대문자P) : 위에 끼워넣기

dd : 한줄 삭제

. : 앞명령 반복

:set number : 왼쪽에 줄번호 표시

:w : 저장

:q : 종료

:wq : 저장하고 종료

:wq! : (묻지도 따지지도 말고) 저장하고 종료

:q! : (묻지도 따지지도 말고) 그냥 종료

hjkl : 좌하상우 (화살표키 대용으로 사용하는 것, 최근에는 화살표키로 다 됨)

* 리눅스 명령어 Quiz

quiz1) abc.txt를 cba.txt로 바꾸려고 합니다. 이때 사용하는 명령어는?

$ touch abc.txt

$ cp abc.txt cba.txt // abc.txt를 복사해서 cba.txt를 만듦 -----> abc.txt와

$ cba.txt 두개 모두 존재

$ rm cba.txt

$ mv abc.txt cba.txt // abc.txt의 이름을 cba.txt로 바꿈

$ mv cba.txt /usr/local/src

-------> Permission denied : 권한이 없어서 안됨 ----> 일반사용자이기 때문

$ sudo -i // root 권한으로 전환

(사용자 비밀번호 입력)

cd ~blackpink

ll

mv cba.txt /usr/local/src // 가능

* 문서 읽기

- 짧은 텍스트 파일은 cat 으로 읽기 cat /etc/passwd
- 긴 텍스트 파일은 less 로 읽기 less /etc/passwd
- 매뉴얼 보기 man [도구이름] man history

-----> less, man을 종료할 때는 q(quit의 약자) 입력

6. 사용자 관리와 파일 속성

cat /etc/passwd
사용자:암호:사용자ID:사용자그룹ID:전체이름:홈디렉터리:기본셸
root:x:0:0:root:/root:/bin/bash
blackpink:x:1000:1000:blackpink:/home/blackpink:/bin/bash

- 암호가 x로 되어 있는 이유는, 오래된 unix/linux의 경우 이부분에 패스워드가 실제로 기록되었음 ----> 누구나 모든 사람의 패스워드를 볼 수 있었다 ----> 개선된 unix/linux는 이 부분을 x로 표시하고 실제 패스워드는 해쉬값으로 만들어서 /etc/shadow라는 파일에 저장

참고로 IoT의 운영체제 들 중 리눅스기반이 많음
/etc/passwd에 패스워드를 그대로 저장하기도 함 ----> IoT 패스워드 그대로 노출!!!

- 루트는 사용자 ID, 그룹ID가 모두 0
- 일반사용자는 사용자ID, 그룹ID가 모두 1000번부터 시작
- Bash Shell ex) 2014년에 Bash Shell 취약점이 알려진 적이 있음 -----> Shell Shock (너무나 충격적이어서 쇼크라고 함)

cat /etc/group
그룹이름 : 비밀번호 : 그룹id : 그룹에속한 사용자
root:x:0:
blackpink:x:1000: // 그룹에 사용자를 추가하지 않아서 현재는 null로 되어 있음 (null은 없다는 의미)

useradd redvelvet // redvelvet 사용자 계정 생성 (딱 계정만 생성... 아무것도 설정이 안된 상태)
passwd redvelvet // 패스워드 설정하는 명령
red
red
BAD PASSWORD: The password is shorter than 8 characters // 패스워드가 너무 짧음(경고) ----> 최소한 8자 이상으로 설정해야 함

* 홈디렉터리가 없으면 FTP로그인이 안됨 ----> FTP를 사용해야 하는 계정이면 home directory를 만들어 주어야 함
(FTP : File Transfer Protocol의 약자, 파일을 업로드/다운로드 하는 서비스)

* Red Hat 계열(CentOS등)은 useradd로도 홈디렉터리가 만들어짐 (useradd와 adduser가 동일하게 사용)
  Debian 계열(Ubuntu 등)은 useradd는 홈디렉터리가 안만들어짐. adduser를 사용해야 만들어짐

* useradd 옵션들이 있음
  -u : userid를 지정
  -g : 그룹
  -d : 홈디렉터리 지정
  -s : 기본 셸 지정

* usermod
- 사용자 계정에 대한 수정이 필요할 때
- useradd와 옵션이 비슷

* userdel
$ userdel redvelvet //사용자 계정이 삭제됨

* chage
$ chage blackpink //전체적으로 변경, 그냥 엔터치면 넘어가짐
  -l : 확인만 할 때
  -m : 최소 의무 사용기간
    ex) 패스워드를 변경하라고 했더니, 변경하고 금방 다시 원래 패스워드로 변경하는 사람
    ex) -m 5 : 한번 바꾸면 무조건 5일은 사용해야 함
  -M : 최대 사용 기간 너무 오래사용하면 다른 사람이 같이 보고 있을 수도 있음
  -E : Expire 날짜 지정 가능
  -W : Warning 경고일 지정
    ex) -W 7 : 7일전 경고 (패스워드 유효기간이 7일 남았습니다....)

참고) 회사의 보안 정책 중 패스워드 정책 (정책이란 최고경영자의 승인 내용이므로 지켜야 함. 정책을 위반하면 징계가 따름.)
- 패스워드는 60일간 사용한다. (60일이 지나면 패스워드를 변경해야 함)
- 의무적으로 7일이상 사용해야 한다.
- 대/소/숫/특 섞어서 12자리 이상으로 한다.

실습) twice라는 계정을 만들고, 패스워드는 cheerup 으로 하세요.

최소 의무 사용기간은 5일, 최대 사용기간 90일, -W은 7일 전, root 그룹에 속하도록 설정하세요.

useradd twice
passwd twice
(패스워드 cheerup 두번 입력)
chage -m 5 twice
chage -M 90 twice
chage -W 7 twice
usermod -g root twice

* 혹시 passwd를 입력하다가 잘못 입력한 느낌이 나면
1) backspace를 여러번 누르고 다시 입력
2) 그냥 엔터치고 나와서 다시 passwd 설정하는 방법
* 그룹 관리
groups //그룹 목록 확인
groupadd girlgroup
usermod -g girlgroup twice
groups twice
(twice는 girlgroup에 속해있음을 확인)

groupmod //그룹에 대한 설정을 변경할 때
groupdel //그룹 삭제
gpasswd
-A : 관리자(Admin) 지정
-a : 사용자 추가(add)
-d : 사용자 제거(delete)

실습) bts라는 계정을 만들고 boygroup이라는 그룹을 만든 후에 bts를 boygroup에 추가하고 관리자로 지정하기
bts의 패스워드는 dynamite 로 지정

useradd bts
passwd bts
(패스워드 dynamite 두번 입력)
groupadd boygroup

```
usermod -g boygroup    bts
gpasswd -A bts boygroup
grep    boygroup    /etc/gshadow                    // boygroup의 관리자(Admin)를 확인하는 방법
```

7. 파일과 디렉터리의 소유권과 허가권

d : 디렉토리

- : 파일

l : link

ls -l의 결과

-rw-------. 1 blackpink blackpink 25596 Dec 15 15:40 password.lst

----> 소유자는 읽기와 쓰기 가능, 그룹이나 기타는 아무 권한이 없는 상태

rwxrwxrwx 소유자(User) 그룹(Group) 기타(Other)

r : read (4) : 읽기

w : write (2) : 쓰기

x : execute (1) : 실행

- : 권한이 없는 상태 (0)

* 권한을 숫자로 표시하는 방법

rw------- : r(4)+w(2) = 6, 0, 0 -----> 600

rwxr--r-- : rwx(7) r--(4) r--(4) ----> 744

예제) 권한이 600인 password.lst 파일을 777로 바꾸려면?

chmod 777 password.lst

결과 : 600(rw-------)에서 777(rwxrwxrwx)로 바뀜

chmod (change mode) 권한을 변경하는 명령

* 파일 허가권

* 권한을 상대모드로 추가하거나 삭제하는 방법(리눅스 마스터 시험에 나옴)

chmod u+x // user에 실행권한(x)을 추가(+)

chmod u-x // user에 실행권한(x)을 제거(-)

chmod o+r // other에게 읽기권한(r)을 추가(+)

실습) password.lst 파일(현재777)에서 그룹은 읽기만, 기타는 모든 권한을 제거하세요.

* 여기서 잠깐

UNIX/LINUX 에서는 확장자는 중요하지 않음 (Windows는 확장자가 중요함)

파일을 어떻게 인식하는가? 파일의 첫 부분에 파일의 고유한 시작 문자열이 있음(File Signature, Magic Number) ---> 판단

1) JPG파일

ÿØÿà : JPG/JPEG 파일의 파일 시그니처

file twice.jpg

2) PDF 파일

%PDF-[버전] : PDF파일의 파일 시그니처

file 03가상화실습.pdf 라고 입력하면 파일 시그니처를 읽어 들임 (%PDF-1.5)

* 확장자를 믿지 마세요. File Signature를 믿으세요.

이력서.pdf .exe ----> exe파일임 ---> 클릭하면 랜섬웨어...

* 파일 소유권

cp password.lst /home/twice

cd /home/twice

ll // password.lst 파일의 소유자가 root로 되어 있음 (root가 복사했으므로... root가 생성한 것과 같음) -----> 생성자가 소유자임

예제) 소유자만 변경

chown twice password.lst

결과

-rwxr-xr-x. 1 twice root 25596 Dec 16 12:24 password.lst

예제) 소유자와 그룹을 동시에 변경

chown twice.girlgroup password.lst // Owner는 twice, Group은 girlgroup에 속함

-rwxr-xr-x. 1 twice girlgroup 25596 Dec 16 12:24 password.lst

예제) 그룹만 변경

chgrp root password.lst

* 파일 실행 방법 ./[파일명]

ex) ./test //test파일안에 들어있는 명령어들이 모두 실행됨

/root 디렉토리의 권한 r-xr-x--- (550)으로 되어 있음 -----> 파일권한보다 디렉토리 권한이 우선 적용되기 때문

* 특수한 형태의 파일 권한 ------> 리눅스 마스터 시험 및 다른 시험에서도 리눅스 관련 문제인 경우 많이 출제됨

8진수 : 가장 큰 숫자가 7(0~7), 7다음의 숫자는 10 (두자리로 넘어감)

10진수 : 가장 큰 숫자가 9(0~9), 9다음의 숫자는 10 (두자리로 넘어감)

2진수 : 가장 큰 숫자가 1(0~1), 1다음의 숫자는 10 (두자리로 넘어감)

16진수 : 가장 큰 숫자가 F(0~F), F다음의 숫자는 10 (두자리로 넘어감)

* 8진수 세자리 : 000~777 ----> rwx (4+2+1 = 7) ----> 8진수라고 볼 수 있음

000~777 ----> 0**000**~0**777**

----> 빨간색 0부분(8진수 = 2의3승 = 3bit = _ _ _) 000, 001,010,011,100,101,110, 111

0 : r이 온다면 r=4이므로 4를 이진수로 만들면 100, -----> 4는 setuid

w가 온다면 w=2이므로 2를 이진수로 만들면 010, -----> 2는 setgid

x가 온다면 x=1이므로 1을 이진수로 만들면 001, -----> 1은 stickybit

-가 온다면 -=0이므로 0을 이진수로 만들면 000

1) setuid (셋유아이디) : set userid

- 파일 권한 4자리 중에 첫번째 자리 (빨간색 부분)에 4가 온다면 (4=read) ----> setuid라고 함

passwd bts // bts 패스워드 변경시 사용하는 명령

passwd라는 명령의 리눅스 위치는 /bin/passwd 에 있음

cd /bin

ls -l passwd

-rwsr-xr-x. 1 root root 33600 Apr 7 2020 passwd // passwd는 root의 소유, root권한이 아니면 사용할 수 없음

s는 setuid의 s임

rwsr-xr-x ---> 4755 // setuid : 일반사용자는 실행하는 순간에 root권한을 잠시 빌려서 사용하게 됨 (자신의 비밀번호만 바꿀수 있음)

rwxr-xr-x ----> 755

* setuid 설정 방법

chmod u+s // s는 setuid의 s임

2) setgid

-rwxrwsr-x. 1 root root 33600 Apr 7 2021

group권한에 x대신 s로 표현하면 setgid

3) stickybit : 디렉토리에 stickybit가 설정되어 있으면 파일이나 디렉터리를 생성 가능, 남의 파일의 삭제할 수는 없음 (공유디렉토리)

-rwxrwxrwt. 1 root root 33600 Apr 7 2020 [디렉토리명]

cd /

ls -l

drwxrwxrwt. 22 root root 4096 Dec 16 12:29 tmp //tmporary(임시폴더)의 의미 ---> 공유폴더임

ex) 음악 파일 업로드 하기 (남의 음악파일은 지울 수 없음, 업로드 가능)

ex) 공격자들이 악성코드를 업로드하는 용도로 사용하기도 함

* 정리

- setuid(4~) : user가 자신의 파일을 변경해야 할 때, 잠시 root권한을 사용하는 것

-rwsr-xr-x ex) 4xxx : 4755, 4640, 4754

- setgid(2~) : group이 자신의 파일을 변경해야 할 때, 잠시 root권한을 사용하는 것

-rwxrwsr-x ex) 2xxx : 2755, 2640, 2754

- sticky bit(1~) : 공유폴더임

drwxrwxrwt ex) 1xxx : 1777

설정 사례)

chmod 4777 test

chmod 2640 test1

참고)

"StickyBit"는 다른 사람의 파일을 변경하지 못하게 하는 기능이고, 디렉터리에만 효과가 있다.

https://mamu2830.blogspot.com/2019/10/setuid-setgid-sticky-bit.html

실습)

/tmp sticky bit(스티키 비트)가 적용되어 있는 공유폴더에 twice계정으로 파일을 생성하고, bts 계정으로 삭제시도 해보기

[blackpink@localhost ~]$ cd /tmp //blackpink 계정 사용중

[blackpink@localhost tmp]$ su twice // twice 계정으로 전환

Password: // 패스워드는 cheerup 입력

[twice@localhost tmp]$ // twice 계정 사용중
[twice@localhost tmp]$ touch yesoryes // yesoryes 파일 생성
[twice@localhost tmp]$ vi yesoryes // 내용 입력 후 저장하고 종료 (:wq)
[twice@localhost tmp]$ su bts // bts 계정으로 전환
Password: // 패스워드는 dynamite
[bts@localhost tmp]$ rm yesoryes // 남의 파일 삭제 시도
rm: remove write-protected regular file 'yesoryes'? y
rm: cannot remove 'yesoryes': Operation not permitted // 권한이 없어서 파일을 못 지움

[bts@localhost tmp]$ mkdir idol // bts 권한으로 idol 이라는 디렉토리 생성
[bts@localhost tmp]$ su twice // twice 계정으로 변경
[twice@localhost tmp]$ rm -rf idol // 삭제 시도
rm: cannot remove 'idol': Operation not permitted //다른 사람이 만든 디렉토리는 삭제 권한이 없음

[twice@localhost tmp]$ mv idol star // idol을 star로 이름을 변경 시도
mv: cannot move 'idol' to 'star': Operation not permitted

* 링크 (Link)
- 실제 파일은 다른데 있지만, 사용자에게 사용하기 편리하도록 연결해주는 기능
- twice, bts계정은 터미널에서 만든 계정이라서 root 권한으로 전환이 안됨 (sudo -i 사용 불가, sudo su 안됨)
- 설치하면서 만들었던 계정(blackpink)은 root 권한으로 전환 가능 (sudo -i 가능)

실습)
cd /root
mkdir linktest
vi basefile
(내용을 적당히 넣으세요. :wq)
cat basefile // 내용 확인
ln basefile hardlink
ln -s basefile softlink

cat basefile
cat hardlink

cat softlink

----------> 캡쳐 -----> 이미지로 저장 link.png로 저장

8. 어플리케이션 설치

* RPM

- RPM (Redhat Package Manager의 약자 ---> Redhat 계열에서만 사용)
- Redhat 계열에서 자동 설치 명령이 yum (old version)
  Redhat 계열에서 새로운 자동 설치 명령 : dnf (New Version)

* 동일한 파일이란? 해쉬값이 같아야 동일한 파일

md5sum basefile // 128bit 해쉬함수 (취약함)
md5sum hardlink
------> 두 파일의 해쉬값이 같음 -----> 같은 파일임
sha1sum basefile // 160bit 해쉬함수 (취약함)
sha1sum hardlink

sha256sum basefile // 256bit 해쉬함수 (안전함) ------> Bitcoin에서 사용중
sha256sum hardlink

* gzip

- 확장자가 gzip으로 되어 있으면 압축된 상태

* rpm

- 패키지를 설치하는 명령어
  rpm -Uvh [패키지 이름]
  -U : Upgrade (업그레이드 하거나 없으면 새로 설치)
  -v : verbose (상세하게)
  -h : 진행상황 표시(#으로)
  -i : 설치 install
- 패키지를 삭제하는 명령어
  rpm -e [패키지 이름]
  -e : erase

rpm -qa tar // tar 설치되어서 조회 가능
rpm -qa rpm // rpm도 설치되어 있음

* RPM의 단점

- 의존성 문제 발생 : 미리 설치되어 있어야 설치 가능, 버전마다 조금씩 달라지는 문제
- 강제로 패키지를 설치하는 방법 : --force

* dnf
- 설치 마법사 ----> 알아서 잘 설치해줌
- dnf : dandified yum (예전에는 yum을 사용) ----> 의존성 문제를 해결해줌
- dnf를 사용하면 CentOS의 중앙저장소에서 파일을 가지고 옴 ----> 이 경로는 /etc/yum.repos.d 에 저장되어 있음

* dnf 사용 방법
# dnf install [패키지 이름]
# dnf update [업데이트할 패키지]
# dnf check-update
# dnf update // 전체 패키지 업데이트 (지금 하지 마시길)
# dnf remove [패키지 이름] // 패키지 삭제
# dnf info [패키지 이름] //정보를 확인할 때

dnf info mysql-errmsg // 버전, 상태 등을 확인해보고
dnf install mysql-errmsg // 설치
dnf install -y mysql-errmsg // 중간중간에 Is this ok? 에서 계속 y를 선택함

* 다운로드 받은 파일이 정상적인 파일인지 아니면 수정된 파일인지를 알기 위해서 GPG라는 것을 사용
(GPG : GNU 프라이버시 가드)
GPG검사를 가급적 수행해야 함 ----> 변조된 파일인 경우, 악성코드가 포함되어 있을 수 있음

ping 168.126.63.1 응답이 없으면 네트워크 비활성화된 상태임

참고) zip 파일을 처음 만든 사람은? Phil Katz
-----> ZIP 파일, APK(안드로이드 실행파일), PPTx, XLSx, Docx등 의 파일 시그니쳐는 PK (50 4B : ASCII코드)

* 파일 권한 (복습)

rwxrwxrwx : user group other

- 755파일 : -rwxr-xr-x
- 640파일 : -rw-r-----

r = 4, w =2, x=1 -=0

- setuid : -rwsr--r—

// 관리자 권한으로 실행해야 하지만, 자신의 정보를 변경해야 할 경우 관리자권한을 빌려옴 4~~~~~

- setgid : -rwxrwsrwx

// 그룹에 대한 변경이 필요할 경우 관리자 권한을 빌려서 실행 2~~~~~~

- stickybit : drwxrwxrwt // 공유폴더 1~~~~~~

* DNF의 작동 방식과 설정 파일

cd /etc/yum.repos.d

less cert-forensics-tools.repo // 리파지토리(중앙저장소)의 설정 내용, 주소 확인

gpgcheck : 올바른 파일인지를 확인 (저작자의 서명을 확인)

* 파일 압축과 묶기

1) XZ

xz -d 파일명 // -d : decompress (압축 해제)

xz -l 파일명 // -l : list 압축된 파일의 리스트 확인

xz 파일이름 // 압축하고 원래파일은 삭제 (용량을 줄이기 위한)

xz -k 파일이름 // -k : keep 원래파일 놔두고 압축

2) bzip2

bzip2 파일이름 // 압축

bzip2 -d 압축파일.bz2 // 압축 해제

3) gzip

gzip 파일이름 // 압축

gzip -d 압축파일.gz // 압축 해제

4) gunzip

gunzip -d 압축파일.gz

5) zip 생성할파일.zip 압축할파일

6) unzip 압축파일.zip

실습) 압축해보기

cd ~blackpink

(password.lst를 압축)

1) xz로 압축해보세요.

xz -k password.lst

-----> password.lst.xz

2) bzip2로 압축해보세요.

bzip2 password.lst // 원본은 지워지고 압축률은 xz보다 떨어짐

bzip2 -d password.lst.bz2

bzip2 --help // 옵션에 대한 설명이 있음

bzip2 -k password.lst

3) zip 압축 (윈도우와 호환됨)

zip password.zip password.lst

* 압축 효율 : xz > bzip2 > zip

* 파일 묶기 : 여러개의 파일을 하나로 묶는 것

tar (Tape Archive) : 여러 파일을 묶는 역할만 수행, 압축은 위에서 배운 압축 프로그램을 별도로 사용해야 함

ex) 압축파일.tar.gz 압축파일.tar.xz

tar --help

-c : 새로운 묶음 (create)

-x : 묶음 해제 (extract)

-f : 묶음 파일 이름 지정

-v : 과정을 보여줌 (visual)

-z : gzip으로 압축한 경우 (tar + gzip)

-J : xz로 압축 (tar + xz)

-j : bzip2로 압축 (tar + bzip2)

사례) 압축해제 tar -zxvf 압축파일.tar.gz

tar -Jxvf 압축파일.tar.xz
tar -jxvf 압축파일.tar.bz2

* ipcamera.zip 파일을 다운로드 하세요.
# unzip ipcamera.zip 압축해제

* 파일 위치 검색
# find --help
# find / -name "shadow"
/는 최상위 디렉토리에서부터 그 아래 전체를 찾을 때
-name "찾을 파일"
find / -name "http*" // *를 붙이면 뒤에 다른 이름이 붙어있는 경우 모두 찾아줌
(http로 시작하는 모든 파일을 찾아줌)
find / -name "apache2*" // apache2로 시작하는 모든 파일을 찾아줌

find / -user "twice" // 소유자가 twice인 파일을 검색

find /etc -perm 644 // /etc에서 퍼미션(권한)이 644 인 파일 찾기
find /etc -perm 640

find /usr/bin -size +10k -size -100k // 10kbytes ~ 100kbytes 인 파일을 골라보기
find /usr/bin -size +60k -size -80k
find /usr/bin -size +100k -size -120k

find ~ -size 0k -exec ls -l {} ₩; // ~ : 홈디렉토리
find /tmp -size 0k -exec ls -l {} ₩;
find . -size 0k -exec ls -l {} ₩; // . : 현재 디렉토리

find /home -name "*.swp" -exec rm { } ₩;

which passwd
whereis passwd
updatedb // locate를 사용하기 전에 사용하므로 목록을 DB화해서 저장
locate passwd // updatedb 이후에 설치된 파일은 찾을 수 없음

9. 시스템 설정

* CRON과 AT

cron // 반복되는 작업 또는 특정 시점에 수행할 작업을 미리 등록해놓음 ex) 백업

분 시 일 월 요일 사용자 실행명령 -----> 리눅스 마스터 시험에 많이 나옴

00 05 1 * * root cp -r /home /backup

- * 표시는 항상 수행 (월 *표시는 매달 한다는 의미)
- 매월 말일에 하면 안되는 이유 : 매달 말일이 달라요. 1/31 2/28 4/30 12/31

요일 : 0 ~ 6 or SUN ~ SAT -----> 시험문제에는 요일을 숫자로 표시

0 : 일요일

1 : 월요일

2 : 화요일

3 : 수요일

4 : 목요일

5 : 금요일

6 : 토요일

7 : 일요일

셸 스크립트를 사용하는 방법 (셸 스크립트 : 명령어를 여러개를 수행하는 파일) 확장자는 .sh

```
#!/bin/sh                                   // shell script 선언
set    $(date)
fname="backup-$2$3tar.xz"
tar   cfJ   /backup/$fname   /home
```

백업할 내용은 crontab에 저장 : /etc/crontab

```
less   /etc/crontab
vi    /etc/crobtab                          // 작업 예약
```

```
cd   /etc/cron.monthy
touch   myBackup.sh
chmod    755   myBackup.sh
```

vi myBackup.sh //작업 내용 만들기
(각자 작성해봅시다)

mkdir /backup
systemctl restart crond //크론 재시작 ----> 등록한 내용이 적용됨

실습) (결과를 빨리보기 위해) 현재시간으로 변경해보기
vi /etc/crontab
i //편집모드 시작
01 14 17 * * root run-parts /etc/cron.monthly
:wq // 저장하고 종료

systemctl restart crond

예제) 매시간 5분마다 출석체크하는 작업 예약 등록
05 * * * 1-5 twice 출석체크
분 시 일 월 요일 사용자 작업

예제) 산타할아버지 로직 만들어보기
* 4 25 12 * 산타할아버지 선물주기
00 00 25 12 4 santa 선물
00 24 25 12 * santa delivery //산타할아버지 지각 (그 다음날 오심) 시간은 0~23까지
00 00 25 12 * santa 선물
0 0 24 12 * santa give a present // 산타할아버지 너무 일찍 오심 (전날)
* * 24 12 santa 선물 //매 분마다 주는 것 (산타할아버지 거덜남)
(60 * 24 = 1440 개)

* at
rdate -s time.bora.net // time.bora.net은 우리나라 시간 서비스를 해주는 서버와 동기화 (-s : syncronization)
dnf update

10. 네트워크 설정과 명령어

- TCP/IP는 누가 만들었을까요?
- 미국 국방성(Pentagon) 산하에 ARPA(고등연구소)에서 만듦 (로버트 칸, 빈트 서프)
- 원래 만든 목적 : 대형 무기 제작 프로젝트를 하기 위해서 연구소, 기업(군수업체), 대학교 등을 네트워크로 연결
- ARPA(고등연구소)는 DARPA로 이름이 변경됨
- 오늘날의 인터넷 (1960년대 중반부터 개발을 시작해서 1974년에 현재의 모습이 됨)

* 호스트이름과 도메인 이름

DESKTOP-30FTUBK : NetBios Name (윈도우끼리 서로를 인식하는 이름)

* 도메인 네임 : naver.com daum.net 11st.co.kr // 컴퓨터에 할당된 이름은 아님
- DNS서버에서 특정 서버와 매핑된 정보를 알려줌 (218.36.25.4 www.11st.co.kr)
  세자리를 사용하는 경우 : .com .net .org .tv 등
  국가코드를 사용하는 경우 : co.kr co.jp co.fr co.de 등
- DNS Root Server : 최상위 서버 (http://www.root-servers.org)
  총 13대 : A, B, C, D, E, F, G, H, I, J, K, L, M + Mirror Server들이 수천대 (Mirror Server는 Main Server와 동일하게 동작)
  만일, A~M까지의 메인서버를 모두 박살내면 DNS서비스가 중지됨
  ----> 위치가 대부분 기밀 ---> 어디있는지 알려져있지 않음 (미국9대, 일본1, 스웨덴1, 영국1, ????)
- 정방향 조회 : 도메인 이름을 입력하면 IP주소를 알려줌 A (도메인 이름 -->IPv4), AAAA (도메인 이름 -->IPv6) = A6
- 역방향 조회 : IP주소를 입력하면 도메인 이름을 알려줌 PTR (IPv4/IPv6 ---> 도메인 이름)
  this.hanbit.co.kr.(null) : hanbit.co.kr에 해당하는 this라는 서버를 지정
  kr 정보는 Root Server가 알려줌
  co.kr 정보는 kr서버가 알려줌
  hanbit.co.kr 정보는 co.kr 서버가 알려줌
  this.hanbit.co.kr 정보는 hanbit.co.kr 서버가 알려줌

* IP주소
- 공인IP : 전세계에 딱 1개만 있음(유료), 라우팅 가능 ----> 어디있는지 찾을 수 있음 ---> 인터넷 가능
- 사설IP : 누구나 공짜로 사용, 라우팅 금지됨(공식 표준문서에 지정) ----> 어디있는지 모름 ---> 인터넷 안됨
  (사설IP는 NAT를 사용해서 인터넷 연결하고 있음)
  사설IP의 종류 : 10.x.x.x, 172.16.x.x ~172.31.x.x, 192.168.x.x

* 사람 이름 : 임꺽정 -----> 성과 이름으로 구분, Brad Pitt -----> 이름과 성
IP 주소 : 네트워크 부분 + 호스트 부분
네트워크 부분 ----> 라우팅(목적지를 찾아주는 것)
cf. 집성촌 (같은 성씨를 가진 사람끼리 모여 사는 곳)
호스트 부분이 모두 0이면 네트워크 주소라고 함
192.168.5.128 -----> 192.168.5.0 (네트워크 주소)

* 전송 방식
- Unicast : 송신자가 수신자1에게 전송
- Multicast : 송신자가 그룹(Group)에 전송
- Broadcast : 송신자가 All(전체)에 전송

예시)
192.168.5.128 ----> 각자리는 8bit이고, 8bit가 4개이므로 32bit
(자리 구분은 . 으로 구분, 구분자는 . 임)

* IP주소에서 Broadcast는 호스트부분이 모두 1, 각자리는 8bit이므로 1111 1111 = 255 -----> 192.168.5.255

ex) 흥부네 집에 아이들이 10명이라면, 엄마(흥부 부인)가 밥을 드디어 해서 아이들을 부르려고 합니다.
"얘들아 밥먹어라~~" 얘들아 ----> Broadcast (한번에 여러 호스트를 호출하려고 할 때 사용함)
"차량 번호 2850님 차좀 빼주세요~~" ----> 식당에 있는 모든 사람에게 전송 (식당 = 같은 네트워크, 사람 = host)

* Gateway (게이트웨이) : 문 (외부로 나가는 경로)
ex) 문이 하나밖에 없으면? 화재 발생 (문쪽에서 화재가 나면... 탈출이 어려움...)
-----> 게이트웨이 이중화 : 하나는 SK Broadband를 연결하고, 다른 하나는 KT랑 연결 ----> 한쪽이 막혀도 다른 쪽으로 인터넷 가능해짐

* Netmask와 Class

- Netmask는 Subnet Mask라고도 함 ex) 255.255.255.0를 이진수로 바꾸면 1111 1111.1111 1111.1111 1111.0000 0000

- Subnet Mask에서 이진수로 1에 해당하는 IP주소는 네트워크, 0에 해당하는 IP주소는 호스트임

192.168.5.128

255.255.255.0

12.34.56.78

255.255.0.0

- 컴퓨터는 이진수가 편하고 (신호가 있다, 없다로 표시하는 것이 가장 명확함)

- 사람은 손가락이 10개라서 십진수를 사용하는 것

* 정리

ex) 168.126.63.1 (우리나라 KT에서 운영하는 DNS Mirror Server : 분당 KT 본사)

255.255.255.0

네트워크 주소?

→ Subnet Mask의 0에 대응하는 IP주소 부분(Host부분)이 모두 0 : 168.126.63.0

브로드캐스트 주소?

→ Subnet Mask의 0에 대응하는 IP주소 부분(Host부분)이 모두 1 : 168.126.63.255

→ 실제로 호스트에 할당 가능한 주소는 168.126.63.1 ~ 168.126.63.254 이다. (개수는 254개)

* 네트워크 확인 명령

ifconfig // 리눅스에서는 ifconfig, 윈도우에서는 ipconfig

ifconfig ens33 // ens33인터페이스의 정보만 보려고 할 때

ifup ens33 // ens33이 사용하지 않고 있는 상태일때, 사용하도록 설정

ifdown ens33 // ens33이 사용중일 때, 사용하지 않도록 설정

nmtui

(네트워크 설정을 변경한 후에는 반드시 아래 명령어를 입력해야 함

systemctl restart NetworkManager // 재실행을 해주어야 반영됨

systemctl stop NetworkManager

systemctl start NetworkManager

* nslookup // 도메인주소를 입력하면 IP주소를 알려주는 네트워크 명령어

ex) nslookup www.naver.com 하면 IP주소가 지역마다 다르게 나옴 ----> 지역에 따라서 서버를 부하 분산하는 방식(DNS Load Balancing)

* ping [IP주소] ex) ping 168.126.63.1 , ping 192.5.5.241

$ ping [도메인이름] ex) ping www.daum.net

* 압축 : xz, bzip2, gzip, zip 등 -d : 압축 해제 옵션(depress) , -k : 원본 파일 유지(keep)

* 묶기 : 여러파일을 하나로 묶는 것 tar

네이버, 다음 ----> 로그파일(텍스트) 하루에 몇 테라... ----> 백업테이프를 활용

1) 압축 풀기

$ tar -xvf [압축파일명]

$ tar -zxvf 압축파일.tar.gz

$ tar -jxvf 압축파일.tar.bz2

$ tar -Jxvf 압축파일.tar.xz

2) 압축 할때

$ tar -cvf 압축할파일명.tar /디렉토리 //디렉토리 통째로 압축할 때

$ tar -cvfz 압축할파일명.tar.gz /디렉토리

$ tar -cvfj 압축할파일명.tar.bz2 /디렉토리

$ tar -cvfJ 압축할파일명.tar.xz /디렉토리

* 파일 찾기

find / -name "http*" // 최상위디렉토리부터 전체 하위 디렉토리까지 ----> 전체에서 http로 시작하는 모든 파일 찾음

find . -name "*.php" // 현재 디렉토리에서 확장자가 php인 파일을 찾는 것

find ~ -perm 644 // 현재 사용자의 홈디렉토리에서 권한이 644인 파일을 찾는 것 (644 = rw-r--r--)

* 날짜로 찾기

- 파일의 시간 : 생성(Create)시간, 수정(Modify)시간, 접근(Access)시간 -------> MAC Time : 파일 포렌식할 때 사용

-atime : access time

-mtime : modified time

-ctime : creation time

날짜가 이후일 경우 +, 이전일 경우 - 뒤에 숫자를 입력
-mtime +60: 변경된지 60일 이후
-mtime -60: 변경된지 60일 이전
-ctime -30: 생성된지 30일 이내

* 참고 페이지
https://www.lesstif.com/lpt/linux-find-43844055.html

find -type f -ctime -7 // 7일 이내에 생성된 파일을 찾아라
find -type f -ctime +7 | xargs rm // 7일 이전에 생성된 파일을 지워라 (|는 두개의 명령을 사용, 앞 명령 결과를 조건으로 사용)

ls -l | wc –l
// 파일 리스트를 확인해서 개수를 세어라(wc) ----> 파일이 20개 있으면 '20'으로 출력됨

실습 예제)
find ~twice -type f -ctime -2 //twice 디렉토리에 생성된지 2일이내의 파일을 골라서 보기
~twice : 찾을 디렉토리 (경로)
-type f : 파일(file) 유형(type)을 찾음
-ctime -2 : 생성시간(create time) -2인 파일

find -type f -atime +10 // 접근시간(atime) 10일 이상된 파일 검색

사례) 해킹을 당한 후에 혹시 변경된 파일이 있는지를 찾아보기 위해서 MAC time으로 검색해봄

find -type f -mtime -15 // 수정된지 15일 이내의 파일을 검색

find 로 찾은 파일에 대해 처리가 필요할 경우 xargs 명령어를 pipe 로 연결해서 처리
find -type f -ctime +7 | xargs rm

* 기타 검색어
which 파일명
whereis 파일명
locate 파일명 (초보자용)

* 예약 명령

cron : 매번 반복되는 작업을 예약하는 명령어

ex) 2013년 3월 20일 10시에 예약 작업이 걸려 있음 ----> /etc/sda(부트로더) 삭제, DB삭제 등등....(MBC, 신한은행, 농협 등에서 대혼란 발생)

참고) 3.20해킹사건(2013년) : 북한 해커들이 cron명령으로 정해진 시간에 동작하도록 설정 (1년전부터 공격 준비)

분 시 일 월 요일 작업자 실행명령

(매번 하는 경우 * 표시)

01 00 25 12 * Santa 아이들에게 선물주기

at : 1회성 작업 예약

at now+1 minutes

at> echo "plus">>/home/blackpink/new.txt

ctrl+d // 명령 종료

-------> 1분후에 plus가 추가됨

[root@localhost blackpink]# at now+1 minutes

warning: commands will be executed using /bin/sh

at> echo "plus">>/home/blackpink/new.txt

at> <EOT> // ctrl+d를 누르면 <EOT>가 자동생성됨

cat new.txt

예제) 10시 45분에 /home/twice 에 whatislove 라는 파일을 생성하도록 예약해보기

at 10:45 2020-12-18

at> touch /home/twice/whatislove

ctrl+d

예제) 11시 정각에 /home/twice/santa.txt 파일을 만들고 그 안에 Merry Christmas라고 입력되도록 설정해보기

at 11:00 2020-12-18

warning: commands will be executed using /bin/sh

at> echo "Merry Christmas">>/home/twice/santa.txt // echo명령으로

santa.txt 파일이 자동생성되고 텍스트 입력됨
at> <EOT>
job 4 at Fri Dec 18 11:00:00 2020

* 네트워크 설정
1) nmtui를 이용해서 IP주소를 192.168.5.100 으로 변경하기
gateway : 192.168.5.2
dns server : 168.126.63.1
변경후에 변경 내용을 적용하려면
ifdown ens33
ifup ens33

또는
nmtui 에서
Active Connection에서 Deactivate & Activate

2) 설정 - 네트워크에서 IP주소 변경하기
(IP주소를 192.168.5.99로 변경해보세요)
ifdown ens33
ifup ens33
ifconfig ens33
------> 주소가 192.168.5.99로 변경되었음을 확인 가능

3) GUI가 없는 서버버전에서는 어떻게 할까?
cd /etc/sysconfig/network-scripts/
vi ifcfg-ens33
(ip주소가 99번으로 되어 있음 ----> 98번으로 변경)
i를 눌러서 편집모드로 들어감
IPADDR=192.168.5.98
ESC를 눌러서 편집모드 종료
:wq
ifconfig ens33 //아직은 99임
ifdown ens33
ifup ens33
ifconfig ens33 // 98로 변경되었음

* DNS 서버에 대한 설정

cat /etc/resolv.conf

* DNS 파일에 설정하는 방법 (우선순위가 DNS서버에게 물어보는 것보다 높음)

/etc/hosts

실습) www.daum.net 을 입력했는데, www.naver.com 으로 접속하도록 만들기

nslookup www.naver.com

(네이버의 IP주소 확인)

vi /etc/hosts

i

125.209.222.141<tab>www.daum.net

ESC

:wq

-------> Firefox를 켜고 주소창에 www.daum.net 을 입력

참고) Pharming 은 DNS Spoofing(속이기)의 의미이다. (올바른 도메인 이름을 넣어도 가짜사이트로 접속하게 됨)

Phishing : 잘못된 주소로 접속해서 가짜 사이트로 접속하는 것

Quiz) 올바른 씨티은행의 주소는?

www.citybank.com

www.citibank.com

echo "113.217.247.90 www.lotte.com">>/etc/hosts

11. 파이프, 필터, 리디렉션

ls -l /etc | more // etc디렉토리에 있는 파일이 많으므로 페이지 단위로 보는 방법 (스페이스바 만 사용 가능)

ls -l /etc | less // pageup과 pagedown을 사용해서 지나간 페이지도 다시 보기 가능

ls -l /etc | wc -l // etc디렉토리에 있는 파일의 개수를 세어 보기

필터 : grep, tail, wc, sort, awk, sed 등등

------> 로그의 양이 많아서 중요한 내용을 추출하기 위해서는 필터를 골고루 잘 사용해야 함

* 필터

- 텍스트 추출, 분석 등등
- 빅데이터 자연어(인간언어) 처리 등에 활용
- 로그 분석 활용

1) grep : 문자열이 일치하는 것을 찾아냄

sysctl -a | grep icmp // -a : 읽기, icmp가 포함된 sysctl의 내용을 추출

0 : 적용 하지 않음

1 : 적용 함

ex) net.ipv4.icmp_echo_ignore_all = 0

// ICMP로 Echo를 보내는 것(ping)을 무시(거부)하겠다? 0 (아니다) ---> 응답하겠음!!!

sysctl -w net.ipv4.icmp_echo_ignore_all=1

// ICMP Echo Request를 무시(ignore)하겠다? 1 (하겠다) ----> 응답없음

sysctl -w net.ipv4.icmp_echo_ignore_all=0

참고) sysctl : 시스템 설정 변경 (=systemctl)

sysctl -a | grep tcp

sysctl -a | grep udp

sysctl -a | grep arp

2) wc (word count)

wc -l // 라인수 계산해서 보여줌

wc -m // 알파벳 개수를 계산해서 보여줌

wc -w // 단어 개수를 계산해서 보여줌

3) sort (정렬)

```
# sort -n              // 오름차순으로 정렬(알파벳, 숫자가 작은 것부터)
# sort -rn             // 내림차순으로 정렬(숫자가 큰 것부터)
# sort -u              // uniq : 중복제거
```

4) awk (오크)

```
# echo 11 22 33 44 | awk '{print $4,$3,$2,$1}'

# cat /var/log/secure | awk '{print $5}' | sort | sort -u | sort -rn
# cat /var/log/secure | awk '{print $5}' | sort -u | sort -rn          // sort를 빼도 결과는 동일함
```

5) sed : 치환 등에 주로 많이 사용

```
# sed -i 's/(old)/(new)/g'                    // (old)가 (new)로 치환됨
```

* 리디렉션

```
# ls -l > list.txt                            // ls -l의 결과를 list.txt에 저장
# cat list.txt
# cat /var/log/secure | awk '{print $5}' | sort -u | sort -rn > /home/blackpink/log.txt
# cd /home/blackpink
# cat log.txt
# sort < log.txt                              // 알파벳 순서로 정렬

# ls -l > list.txt             // 덮어쓰기
# ls -l >> list.txt            // 이어쓰기
```

12. 프로세스, 데몬, 서비스

- HDD/SSD에 있던 파일이 메모리에서 실행중일 때 프로세스라고 함
- Foreground : 전면에서 실행중 -----> 사람눈에 보이게 실행
- Background : 후면에서 실행중 -----> 사람눈에 보이지 않게 실행
- 프로세스 번호 #ps -ef
  PID : Process ID
- 부모 프로세스 - 자식 프로세스
  ex) X-windows - Firefox

```
# ps   -ef                                  // 모든 프로세스 조회
# ps   -ef  |  grep    gdm

# kill   [PID]                             // 프로세스 정상 종료
# kill   -9   [PID]                        // 프로세스를 강제로 종료 (비권장) : 정상 종료가 잘 안될때 (무한
루프 또는 악성코드인 경우)
# kill   -l

# pstree
- 부모자식간 프로세스를 트리 모양으로 보여줌
[root@localhost blackpink]# pstree   6209
ibus-daemon─┬─ibus-dconf─────3*[{ibus-dconf}]
            ├─ibus-engine-sim─────2*[{ibus-engine-sim}]
            ├─ibus-extension-─────3*[{ibus-extension-}]
            └─2*[{ibus-daemon}]

# top  : 프로세스 현황을 2초마다 업데이트 해서 확인 가능
- %CPU : US(Usage, 사용량),    ID(idle, 유휴량)
   ( CPU는 새로운 계산이 필요할 때만 동작함 )
- 중지하려면 ctrl+c

# ps   -ef
# ps   -aux

* 명령어 뒤에 &(엠퍼샌드)를 붙이면 백그라운드에서 실행됨
   ex) 시간이 오래걸리는 작업 : 압축, 압축해제
```

vi를 주로 사용하고 gedit는 가급적 사용을 안하는 것으로 하겠습니다.

* 서비스
- 데몬(Daemon)이 메모리에 상주하면서 서비스를 해주는 역할
- 웹서비스, 메일서비스, 파일전송서비스 등을 해주기 위해서 메모리에 데몬이 항상 실행 중

* 서비스와 소켓
- Socket : 서비스를 실행하기 위해서 서비스를 뒷받침하는 역할
- Socket : IP주소(L3)와 Port번호(L4)의 조합 (서비스는 L7)
 http 서비스의 데몬은 httpd (d = daemon)
 ftp 서비스의 데몬은 ftpd
 ssh 서비스의 데몬은 sshd // sshd가 메모리에서 실행중인 프로세스로서 누가 ssh서비스를 원하면 응답을 해줌
 mysql 서비스의 데몬은 mysqld

* 서비스 설정
# systemctl start/stop/restart 서비스이름
# systemctl status 서비스이름
# systemctl enable/disable 서비스이름

cd /usr/lib/systemd/system
소켓만 보려면?
find . -name "*.socket"
less sshd.socket
service sshd start // ssh 서비스가 실행됨
netstat -na | less // 22번포트에서 ssh가 실행중임을 확인할 수 있음

실습) 윈도우 터미널을 열고 SSH서비스로 접속해보기
ssh 192.168.5.98 -l twice (-l : login)
 (CentOS의 공개키의 해쉬값(SHA256)을 보여주면서 맞냐고 물어봄... yes라고 입력)
 (twice의 패스워드를 물어봄 : cheerup 입력)
[twice@localhost ~]$ // twice 권한으로 명령 입력 가능

[twice@localhost ~]$ who //현재 시스템에 접속한 사용자를 보여달라

blackpink tty2 2020-12-18 09:37 (tty2) // tty : 터미널---> 콘솔(현장에 있음)
tty1, tty2, tty3, tty4, ... (여러명이 콘솔)
twice pts/1 2020-12-18 16:23 (192.168.5.1) // pts : 원격 접속 ---> IP주소가 보여짐

[twice@localhost ~]$ exit // 접속 종료됨

실습) 누가 접속했나 확인해보기

[root@localhost system]# lastlog
twice pts/1 192.168.5.1 Fri Dec 18 16:23:51 +0900 2020
(KST : Korea Standard Time = 기준시보다 +9시 , 기준시 : 그리니치 천문대, 런던, 영국)

ssh 192.168.5.98 -l bts //이미 앞에서 서버의 공개키는 저장했으므로 해쉬값이 맞는지는 물어보지 않음
cat /etc/passwd // passwd의 권한은 644이므로 일반사용자도 읽을 수 있음
pwd
exit

ps -ef | grep sshd // 프로세스 중에서 검색
netstat -nap | less // n : number, a : all, p : process ----> 프로세스ID(PID)와 프로세스 이름까지 보임

* 필터

1) grep : 내가 원하는 문자열을 골라 낼 때

ps -ef | grep http // 프로세스 리스트(ps -ef) 중에서 http가 포함된 문자열을 골라라

sysctl -a | grep icmp

// 시스템 설정(sysctl, systemctl) 내용을 읽어들여서(-a) icmp가 포함된 설정을 골라라

2) tail : 마지막 부분을 읽어들일 때 (위에서 아래로 기록하기 때문에, 최신 정보는 아래에 기록됨)

head : 첫 부분을 읽어들일 때 (위에서 아래로 기록하므로, 위에 있는 것은 오래된 정보임, 만일 sort -rn하면 가장 많은 것을 골라냄)

3) wc : 개수를 세는 것

wc -l : 라인 수

wc -w : 단어 개수

wc -m : 알파벳 개수

ex) 주관식 답안지를 쓸 때 작성한 글자 개수를 위에 표시하는 경우가 있음

4) sort : 정렬

sort -n : 개수를 오름차순으로 정렬

sort -rn : 개수를 내림차순으로 정렬

sort -u : 중복 제거 (unique) // uniq -c : 중복을 제거하는 옵션 (왼쪽에 중복된 개수를 표시함)

5) awk : 골라내기 등

echo 11 22 33 44 | awk '{print $3, $2, $4, $1}'

6) sed : 치환

sed -i 's/(old)/(new)/g'

* process 확인 방법

ps

ps -ef

ps aux

top //실시간(2초간격)으로 프로세스, 컴퓨터 상태 등을 확인

* 서비스 활성화

service sshd start // ssh 데몬을 시작함 (데몬 : 서비스를 해주기 위해서 항상 메모리에서 실행중이어야 함)

실습) CentOS8을 켜고 아래와 같이 실습해봅니다.

$ sudo -i

(비밀번호 입력)

ps -ef | grep ssh

netstat -na | less

tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN

//SSH가 실행중 ----> 22번 포트를 사용하기 때문

(22번 포트가 사용중이라는 것은 SSH가 실행중임을 알 수 있음)

netstat -nap | less

tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 1102/sshd // SSH의 PID는 1102, sshd가 실행중임을 알 수 있음

(리눅스에서는 p가 process)

참고) 윈도우에서는 netstat -nab (b : process)

* SSH 서비스 접속 방법 (Client : Windows의 cmd창을 열고 접속)

ssh 192.168.5.98 -l twice (-l : login)

pwd

cat /etc/passwd // 644 : -rw-r--r--

cat /etc/hosts // 644 : -rw-r--r--

cat /etc/group // 644 : -rw-r--r--

cat /etc/shadow //권한이 640이므로 읽기 권한이 없음 (640 : -rw-r-----)

exit //접속 종료

* 서버에서 접속 여부 확인

lastlog // 접속한 날짜와 시간이 표시됨

tail -20 /var/log/secure // 아래에서 20줄만 보겠음 (twice 접속 기록이 보임)

tail -20 /var/log/secure > /home/twice/log.txt

cd /home/twice

cat log.txt

```
# cat log.txt | awk '{print $3, $5}'
# cat log.txt | awk '{print $3, $5}' > log_command.txt
```

13. 부팅

- GRUB 부트로더 (GRUB : 그루브)
- 부팅할 때 보이는 첫 화면

* ISO 이미지로 부팅 ---> Live Booting (설치하지 않고 운영체제를 메모리에 로드)
  ex) 노트북에 Windows10이 설치되어 있음. ----> CentOS를 CD/DVD/USB에 넣고 부팅 ---> CentOS를 사용 ---> 사용후 재부팅 ---> 원래대로 Windows10으로 사용

실습) vi를 이용해서 /etc/default/grub 파일을 변경해 보기

```
# vi   /etc/default/grub
    i
    GRUB_TIMEOUT=20
    ESC
    :wq
```

* 변경 내용을 적용하기

```
# grub2-mkconfig    -o   /boot/grub2/grub.cfg
# reboot
```

(20초 카운트 하고 부팅)

실습) 비밀번호 설정하기 : 아무나 grub편집을 못하게 하기 위해서 필요 (부팅은 다 가능)

```
# vi   /etc/grub.d/00_header
```

(맨 아랫줄로 이동해서 아래와 같이 내용을 추가합니다.)

```
cat << EOF
set superusers="thisislinux"
password thisislinux 1234
EO
:wq
```

* 변경 내용을 적용하고 재부팅

```
# grub2-mkconfig    -o   /boot/grub2/grub.cfg
# reboot
```

* 간단한 커널 컴파일

- 커널 소스코드를 받아서 커널을 컴파일하면 최신 버전의 커널을 사용할 수 있음

(커널은 운영체제의 가장 핵심 부분)

- 모듈 : 당장 필요한 것이 아닌 경우, 커널에 넣지 않고 별도로 보관했다가 필요할 때 호출해서 사용
  ----> 커널이 불필요하게 커지는 것을 방지

- Apple/IBM/HP : HW+OS+App ----> OS를 만들 때, HW가 제한적임 (다양한 HW를 지원할 필요가 없음)
- MS-Windows/Linux : 사용자가 어떤 HW에 OS를 설치할지 알 수 없음 ----> 다양한 HW 동작 기능(커널, 드라이버 등)을 제공해야 함

14. 서버 설치

* 텔넷 서버 설치

```
# dnf   install   telnet-server                    // 설치
# systemctl   start   telnet.socket                // 서비스 시작
# firewall-config                                  // 방화벽 서비스 접근 허용  (GUI 모드에서만 가능)
# systemctl   enable   telnet.socket               // 리부팅 후에도 서버를 실행하도록 설정
```

(CLI환경에서)

```
# dnf   install   telnet-server                          // 설치
# systemctl   start   telnet.socket                      // 서비스 시작
# firewall-cmd    --permanent   --add-service=telnet     // 방화벽 해제  (CLI모드에서)
# systemctl   enable   telnet.socket                     // 리부팅 후에도 서버를 실행하도록 설정
```

* OpenSSH 서버

- 암호화를 지원 : 서버의 공개키를 받아서 저장하고, ID/PW를 서버의 공개키로 암호화하여 서버로 전송
  ----> 서버는 자신의 개인키를 이용해서 암호화된 ID/PW를 복호화 -----> ID/PW가 평문으로 보임

실습)

```
# rpm   -qa   openssh-server                  //서비스가 설치되어 있는지 확인
# systemctl   start   sshd                    // 서비스 실행       ( service   sshd   start )
```

리눅스 방화벽은 이미 설정이 되어 있음 (firewall-config해서 확인)

```
# netstat   -nap   |   less                   // 열려있는 포트들 확인 ----> 실행중인 서비스 확인
```

* Client(windows10)에서 CentOS-Server로 접속해보기

```
# ssh   192.168.111.100   -l   teluser
```

* XRDP 서버
- 원격에서 X-Window를 사용하기 위한 서비스

실습3) XRDP 서버 설치

```
dnf   -y   install epel-release                    // EPEL 저장소 추가
dnf -y install xrdp                                  // XRDP 설치
systemctl   start   xrdp
netstat   -nap   |   less                             // 3389번 포트에서 실행중
firewall-config
```

접속해제 : centos 로그아웃 클릭

* 웹서버 설치와 운영
* APM (Apache PHP MySQL)
- 웹서버를 구동하려면 Apache, PHP, MySQL을 모두 사용해야 하기 때문에 묶어서 설치하는 경우가 많음
  ex) XAMPP, Bitnami, LAMP(Linux Apache MySQL PHP) 등등 ------> 웹사이트 패키지

* CentOS_server 다운로드 (server가 지워졌거나 잘 안되시는 분들)
ha.do/vss

root / password 로그인 합니다. (centos/centos로 로그인해서 sudo -i를 사용)
----> root 패스워드 복구하기

* Cloud 업무의 80%는 리눅스 (Red Hat, Ubuntu등)
  Network ---> Cisco장비 (Switch, Router, PIX 등)
  DB ----> Oracle, MySQL 등

* 웹서버 구축 연습 방법
1단계 : GUI가 있는 server에서 설정(root권한으로) ----> 가급적 terminal만 사용
2단계 : GUI가 없는 server(B)에서 설정(root권한으로)
3단계 : GUI가 없는 server(B)에서 일반 사용자 계정으로 설정(root권한 사용하지 않고, 필요시 sudo 명령 사용) --> cloud
  (dnf로 자동설치 ----> 직접 다운로드해서 설치 등등 연습해볼 것)

* Cloud 서버의 약 80%이상은 웹서버 : LAMP를 지니처럼 잘 사용해야 함

실습) dnf를 사용해서 APM 설치하기

step0) httpd (Apache), php, MariaDB 설치 여부 확인

rpm -qa httpd php mariadb-server

----> 설치 여부만 확인

ps -ef | grep httpd

ps (process를 확인하는 명령)

-ef (옵션으로 많이 사용)

grep (단어가 포함된 경우를 보여 달라)

netstat -nap | less

netstat (network + status : 네트워크의 상태를 보여달라)

-nap (number, all, process)

less (페이지 단위로 보여달라)

* 웹서버 설치 실습

step1) dnf로 APM 설치하기

dnf -y install httpd php php-mysqlnd mariadb-server

(Debian 계열에서는 httpd라고 하지 않고, apache2라고 함)

아마존 등 클라우드 업체들도 다 미리 확인해보고 되는 버전으로만 서비스함 ---> 지원되는 버전이 따로 있음

step2) 설치 확인 및 시작하기

systemctl status httpd //설치 상태 확인

systemctl start httpd //httpd 시작

* 웹서버의 루트 디렉토리 (Root Directory)

/var/www/html //파일을 넣으면 웹브라우저로 보여짐

step3)

gedit 보다는 vi를 많이 사용 권장

cd /var/www/html

vi index.html

i //편집모드 시작

<html>

<body>

<h1> This is my website. Welcome!!
 어서오세요. 반갑습니다. </h1> //한영 전환 : shift+space

</body>

</html>

ESC

:wq

* 방화벽 해제

접속이 안되는 이유는 Linux 방화벽이 외부로부터의 연결을 막기 때문

firewall-config

영구적 - http,https를 체크하고 - 옵션 - 방화벽 다시 불러오기

----> 웹사이트가 잘 보임

* phpinfo.php 파일 생성

```
# vi   phpinfo.php
i
<?php                                          // php시작 선언
phpinfo();                                     // php 실행 코드
?>                                             // php종료
ESC
:wq
```

참고) 워드프레스를 사용해서 웹사이트 구축하기

- 웹사이트 패키지 : php코드, 이미지, 게시판코드 등등을 제공해줌 ----> 편리하고 많이 사용 (플러그인 많음-->보안 문제)
- 무료이지만, 플러그인이 일부 유료

https://ko.wordpress.org/ (한국어 페이지)

참고) DB권한을 root로 사용하면 DB가 해킹될 우려가 있음 (SQL injection 공격 우려)

```
# systemctl   restart   mariadb
# systemctl   enable   mariadb
# systemctl   status   mariadb                  // 상태 확인해보기 (확인 후 q를 누르면 종료됨)
# mysql   -u root –p                            // maria DB 시작
```

참고) MariaDB? MySQL이 오라클로 넘어가면서 기존에 있던 개발자들이 나와서 따로 MariaDB를 만들어서 GPL로 배포중

- MySQL과 MariaDB는 호환되도록 하고 있음 (명령어도 동일함)

```
create database wpDB;
// DB생성
grant all privileges on wpDB.* to wpUser@localhost identified by '1234';
                        // 사용자와 비밀번호 생성
```

cd /var/www/html
wget https://ko.wordpress.org/latest-ko_KR.tar.gz
tar zxvf latest<tab>

* 디렉토리 권한 변경
# chmod 707 wordpress
파일 소유자를 apache로 변경
chown -R apache.apache wordpress
cd wordpress
cp wp-config-sample.php wp-config.php //sample만 제거, cp대신에 mv를 사용해도 됨
vi wp-config.php
:set nu // 라인번호 왼쪽에 보임
~~_here부분을 순서대로 wpDB, wpUser, 1234로 변경
:wq

* 웹서버 설정파일을 수정
# vi /etc/httpd/conf/httpd.conf
:set nu
(WebServer의 Root Directory 변경)
:wq
dnf install php-json // CentOS8에서 Wordpress 에러 교정 방법
systemctl restart httpd // 아파치 재시작(변경내용을 적용하기 위함)
step2) 워드프레스 설정
http://192.168.111.100/wp-admin/ // 관리자 페이지 (글쓰기)
http://192.168.111.100/ // 일반 사용자에게 보여지는 페이지

15. 클라우드 서비스

* OneDrive(유료) : MS의 계정이 있으면 로그인을 하면 데이터를 MS의 클라우드에 저장
  ---> 아무 컴퓨터에서나 로그인 하면 자신의 데이터를 불러다 사용할 수 있음, 저장하면 다시 회사에서 사용 가능
  ----> HDD를 사용하다가 최근에는 SSD를 사용 ---> SSD용량을 큰것을 사용할 필요가 없음 --> MS의 클라우드에 저장

실습3) OwnCloud 설정
server.7z 파일의 이름을 server_cloud.7z으로 바꾸고 압축을 풀고 여기에 실습하겠습니다.
VMware에서 server_cloud 폴더에 들어가서 server.vmx 파일을 선택하고 불러오기 ---> 앞의 이름을 server_cloud로 변경
부팅시작 ---> 목록에 없습니까? ----> root / password 로그인

step1) APM과 OwnCloud 관련 패키지 설치
dnf -y install httpd mariadb-server php php-mysqlnd php-gd php-mbstring php-pecl-zip php-xml php-json php-intl

step2) DB설정
systemctl restart mariadb
systemctl enable mariadb

* DB생성 및 사용자 권한 부여
create database webDB;
grant all on webDB.* to webUser@localhost identified by '1234';
exit

* 방화벽에서 http,https 외부 접근 허용
# firewall-cmd --permanent --add-service=http
# firewall-cmd --permanent --add-service=https
# firewall-cmd --reload

step3) OwnCloud를 다운로드 받고 설치
cd /var/www/html
wget https://download.owncloud.org/community/owncloud-10.3.1.zip
unzip -q owncloud-10.3.1.zip

mkdir owncloud/data
chown -R apache.apache owncloud
chmod -R 755 owncloud
systemctl restart httpd

step4) 웹브라우저로 접속해서 설정
------> 사용자 생성 (batman / 123456)

step5) OwnCloud의 Client 설정 ----> 각자 해보세요.
https://owncloud.com/desktop-app/ 에서 windows용 msi 파일을 다운로드 하면 됨

wget https://download.owncloud.org/community/owncloud-10.3.1.zip

* FileCloud 서비스 회사
- 리눅스 서버를 아마존에서 실행
- OwnCloud를 설치해서 사람들에게 서비스

* port번호의 의미? ----> 서비스 식별자 역할
1) System Port (1~1023) : 서버들이 사용 (Global Service) -----> 포트마다 정해진 서비스가 있음 (Well-Known Port)
2) Registered Port, Application Port(1024~49151) : 사설 App들이 사용하는 번호 ----> 등록하고 사용
3) Dynamic Port (49152~65535) : 클라이언트들이 사용 ----> 자유롭게 사용 가능

- Listen : 서버쪽에서 포트를 열고 대기한다는 의미
  Client가 SYN를 보내면 ACK/SYN로 응답, Client가 ACK를 보내면 ---> 3Way Handshaking(TCP의 연결 설정과정)

* Web Hosting
- 웹서버를 여러개를 사용
 포트를 2000번 ~ 2200번까지 고객에게 할당
 100.20.30.40:2000 <------ www.green.com
 100.20.30.40:2001
 100.20.30.40:2002
 100.20.30.40:2003
  .....

100.20.30.40:2200

* Cloud (IaaS)

www.green.com ----> 100.20.30.40:80 (VM:가상머신)

www.red.com ----> 100.20.30.41:80 (VM)

16. FTP 서버와 Samba 서버 설치와 운영

* FTP (File Transfer Protocol) : 파일을 업로드 & 다운로드 하기위한 서비스

server.7z 파일을 이름을 server_FTP.7z 으로 바꾸고 압축을 풀고, VMware 이름을 Server_FTP로 변경

부팅하고 I copied it 클릭

* FTP 서버의 종류 : vsFTP, proFTP, pureFTP 등등

step1) vsftpd 서버를 설치

```
# dnf -y install vsftpd

# systemctl restart   vsftpd
# systemctl enable   vsftpd
```

참고) Anonymous FTP 허용은 보안에 위협이 될 수 있음

```
# systemctl stop firewalld
# vi /etc/vsftpd/vsftpd.conf
   anonymous_enable=YES                          //허용으로 변경
   :wq
# systemctl   restart   vsftpd
```

* FTP 클라이언트 다운로드

https://filezilla-project.org/

Step7) 텍스트모드에서 FTP접속 해보기

- Server(B)를 켜고, ncFTP설치

   get   : 파일을 하나만 다운 받을 때
   mget   : 파일을 여러개 다운 받을 때
   put   : 파일을 하나만 업로드 할 때
   mput   : 파일을 여러개 업로들 할 때
   bye   : 종료할 때

   ~~~d : d는 daemon(서비스를 해주기 위해서 항상 기다리고 있는 프로세스)
   ~~~

* WebServer 패키지 설치

- httpd (Apache2) : http를 서비스하는 Daemon(d) ---> httpd

  (Daemon : 서비스를 실행하기 위해서 메모리에 동작하고 있는 프로세스 ----> 줄여서 d라고 하고 각서비스 뒤에 붙임)

  ex) FTPd , httpd, Telnetd 등등

- MySQL : 무료로 사용 ----> Oracle에서 인수

  MariaDB : MySQL의 핵심 개발자들이 나와서 따로 만든 Database인데, MySQL과 거의 동일

- PHP : 가장 많이 사용하는 웹 스크립트 프로그래밍

  (ASP, JSP 등등)

참고) 따로따로 설치하면 의존성 문제 발생할 우려

-----> dnf(자동설치)를 사용해서 Repository(~~~.repo)에서 의존성 문제가 없는 버전 묶음 형태로 다운로드 함

* Repository의 위치

cd /etc/yum.repos.d

여기에 ~~~.repo를 넣어놓으면 여기에 있는 링크에서 Software를 다운로드 하게 됨 (의존성 문제가 해결된 버전들)

* Samba

- 로그인을 한 다음 로그인한 계정에 권한을 부여 사용하는 방식 ----> 문제 발생시 책임 소재 파악 가능

* Windows에서 파일 및 폴더를 공유하는 서비스 ----> SMB (Server Message Block) 시작 : 파일 및 폴더 공유 켜기

  Linux에서 SMB 서비스를 하기 위해서는 SaMBa Client를 설치

* Samba는 SMB를 리눅스에서 사용하기 위한 서비스

* 리눅스(Client)에서 Windows(Server)의 폴더와 프린터 사용

1단계) 계정 만들기

cmd를 관리자모드로 실행하고 계정을 생성

WinClient (Windows 10)에서 설정합니다.

cmd> net user root 1234 /add

(폴더 공유 권한에 root 추가)

share 폴더에 속성 - 공유 - root 추가 - 읽기/쓰기 - 공유 클릭

* Server(CentOS)에서는 root계정으로 진행

cd /root

mkdir share

mount -t cifs //192.168.111.131/share /root/share

cp /boot/vm* /root/share

  -----> 윈도우의 폴더에 동기화 됨

Server에서 /root/share 에서 vi 명령어로 파일을 만들어보기

----> WinClient에서 파일을 열어서 내용 확인

참고) Windows(Client)에서 리눅스(Server)의 폴더와 프린터 사용

  ex) 부서에서 운영하는 파일 서버를 사용하는 경우 ---> 업무상 공유해야 할 파일들을 보관

* 서버쪽 Samba설정

step1) Server에 samba 설치

dnf -y install samba

step2) samba그룹을 만들고 centos계정을 samba그룹에 추가

mkdir /share

groupadd sambaGroup

chgrp sambaGroup /share

chmod 770 /share

usermod -G sambaGroup centos

smbpasswd -a centos

(비밀번호는 1234로 지정)

* samba 설정 파일을 수정

systemctl restart smb nmb //서비스 재실행

systemctl enable smb nmb

firewall-cmd --permanent --add-service=samba

firewall-cmd --permanent --add-service=samba-client

17. 마운트

- Unix, Linux에서는 외부 장치를 인식하게 하는 방법을 마운트라고 함
- HDD를 추가로 장착, USB, CD/DVD 등을 연결하는 경우 인식하기 위해 마운트

mount // 마운트 실행
umount // 마운트 해제

cd /dev // 각종 장치(device)들의 정보가 있음
ls -al // 줄여서 ll 입력

* VMware에서 ISO파일을 CD/DVD로 인식을 시키고, connect를 해주면 CD/DVD처럼 인식됨

cd /run/media
(파일 구경...)

umount /dev/cdrom // 마운트 해제 시도 ----> Target is busy. (사용중이라 해제 안됨)
다른 디렉토리로 이동한 상태에서 마운트를 해제 해야 함

cd /root // CD/DVD에서 다른 디렉토리로 이동
umount /dev/cdrom // 마운트 해제

step4) USB인식 (Client)
-----> Client는 자동로그인 : centos / centos (root계정 비활성화)

* USB
- Linux에서는 FAT32만 인식됨, NTFS는 인식 안됨 (MAC OS에서도 마찬가지)

* MS-Windows에서 FAT(16) ---> FAT32(2G이상 파일 저장 못함) ---> NTFS(2G이상 파일 저장 가능)

FAT32를 사용하는 경우
cd /run/media/centos/USB이름

부록) Kali의 Medusa로 Dictionary Attack 해보기

Kali.org

http://ha.do/vsB

Kali Linux ~~~ .7z 파일을 압축풀고 압축 푼 디렉토리를

내 문서 > Virtual Machines 아래로 이동

VMware를 실행하고 Kali Linux를 열고 부팅하세요.

(kali / kali)

참고) 프롬프트 모양이 이상한 이유

미드중에 Mr.Robot이라는 드라마에서 주인공 해커가 사용하는 컴퓨터와 동일하게 프롬프트를 만듦

-----> 해제하려면 sh 입력후 엔터

sudo -i

(비밀번호는 kali)

* 딕셔너리 파일로 medusa 사용하기

cd /usr/share/john

vi password.lst // 딕셔너리 파일

(#으로 시작하는 내용은 주석이므로 불필요한 부분 ----> 한줄 삭제 : dd)

(123456이 맨 위로 오면 :wq)

Victim : Server_FTP (지우신 분들은 아무 Server를 켜서 dnf -y install vsftpd 입력)

systemctl stop firewalld // 방화벽 중지

systemctl restart vsftpd

(계정생성)

adduser blackpink

passwd blackpink

princess

princess

(사전 검사에 실패했다 ------> 그래도 만들어짐)

(Kali에서 Server쪽으로 FTP 서비스가 동작하는 지 확인) ---> 방화벽이 있는 경우 접속 안됨

ftp

ftp 192.168.111.100

name : blackpink
pass : princess
bye

* 메두사를 활용해서 FTP 서버에 Dictionary Attack 시도
# cd /usr/share/john
# medusa -h 192.168.111.100 -u blackpink -P password.lst -M ftp
(-h : host , -u : user, -P : Password dictionary, -M : module)

* Kali는 인도의 전쟁 여신, 시바의 부인 ----> 이미지 검색 금지 (정신건강에 안좋음...)
힌두교라는 종교는 없음 ----> 다신교

* Offensive Security라는 회사는 exploit-db.com 사이트를 운영 ---> 취약점 제보
- 취약점에 대한 인지가 부족하기 때문에 실습을 해볼 수 있게 Kali Linux를 배포하고 있음
- Kali Linux는 Debian Linux에 해킹툴과 보안 도구를 약 200개 정도, 추가 500개 정도 설치 가능
- 취약점 분석 실습을 할 수 있도록 미리 설치해서 배포 (의존성 문제를 해결해놓고 배포)

* 다른 사람이 운영하는 서버에 공격을 하시면 안됨 (정보통신 망법 위반)

* 공격 당한 로그 확인하기
tail -20 /var/log/secure

18. 방화벽 컴퓨터

- 전세계 방화벽의 약 90% 이상은 리눅스 기반의 방화벽임 ---> GPL이기 때문 (원가 절감, Kernel 안정적 등등)

* 보안을 위한 네트워크 설계
- 방화벽은 내부망(사무실 네트워크, 서버Farm등)과 외부망(인터넷)의 사이(경계)에 배치
- 외부망에서 내부망으로 들어오는 트래픽을 통제(허용/거부)하고, 내부망에서 외부망으로 나가는 트래픽 통제(허용/거부)
- 외부망에서 내부망으로 접근을 막기 위해서 사설IP를 사용함

* 사설IP의 주소 범위
- 10.x.x.x : 10으로 시작하는 모든 주소
- 172.16.x.x~172.31.x.x
- 192.168.x.x : 192.168로 시작하는 모든 주소

* 사설IP의 특징
- 무료(공짜), 누구나 사용 가능
- 인터넷이 안됨(라우팅이 금지되어 있기 때문 --> 표준문서인 RFC문서에 지정)
- 인터넷이 가능하도록 하기 위해서는 NAT를 사용 (NAT : 사설IP와 공인IP 주소를 변환)

* Dual Homed (집이 두개)
- 하나는 내부망(사설IP)에 연결하고 다른 하나는 외부망(공인IP)에 연결

* 방화벽에서 NAT기능을 활용해서 내부망을 보호하는 역할을 수행

* 방화벽 정책
- 회사에서 접속하면 안되는 사이트 : 증권, 가상화폐거래소, 도박사이트, 음란사이트 등등 ----> 차단
- 웹서버의 경우는 외부에서 누구나 접속 가능하도록 해야 함
- 지사, 재택근무자들이 접속할 IP를 허용

실습) 리눅스 방화벽 구축
실습1) 방화벽 컴퓨터를 구현해보자.
Server_FW.7z
Server(B)_Web.7z
Client 그대로 사용

------> 압축만 풀고 아직 VMware 실행하지 말고 준비합니다.

step0) 사전 준비 단계
(Server_FW, Server(B)_Web)
dnf -y install iptables-services

(Client)
su -c 'vi /etc/sysconfig/selinux'
------> 모든 가상머신 off

C:₩Program Files (x86)₩VMware₩VMware Player
vmnetcfg.exe 파일을 오른쪽 마우스 클릭해서 관리자 권한으로 실행 ---> VMnet0(Bridged), VMnet8(NAT) 확인 (변경없음)

Server(B)_Web를 Edit Virtual Machine Settings를 클릭하고 Network를 NAT ------> Bridged로 선택하고 부팅
ifconfig
nmtui edit ens32
(주소 변경)
ok
nmcli connection down ens32
nmcli connection up ens32

step3)
Client를 Edit Virtual Machine Settings를 클릭하고 Network를 NAT ----> Bridged로 변경하고 부팅
$su
#nmtui edit ens33
(주소 변경)
#nmcli connection down ens33
#nmcli connection up ens33

step5) 서버에 랜카드 추가
step6) Server_FW에서 IP주소 변경

step7) 설정 변경

vi /etc/sysctl.conf
net.ipv4.ip_forward = 1
:wq

echo 1 > /proc/sys/net/ipv4/ip_forward
cat /proc/sys/net/ipv4/ip_forward

iptables작성.pdf 파일을 까페에서 다운로드 하세요.
Rule set : 방화벽의 규칙(정책을 반영하는 것)

* 방화벽의 역사 : TCP Wrapper ----> IPchain ----> IPtables ----> UFW (우분투 방화벽)

* NEW는 새로운 연결, ESTABLESHED는 기존 연결
(내부망에서 나가는 규칙 정의)
iptables -A INPUT --in-interface ens34 -s 10.1.1.0/24 -m state --state NEW,ESTABLISHED -j ACCEPT

(내부망으로 들어가는 규칙 정의)
iptables -A OUTPUT --out-interface ens32 -d 10.1.1.0/24 -m state --state NEW,ESTABLISHED -j ACCEPT

(내부망에서 외부망으로 나가는 트래픽은 모두 허용되는 상태)
iptables -A FORWARD --in-interface ens34 -s 10.1.1.0/24 -d 0.0.0.0/0 -m state --state NEW,ESTABLISHED -j ACCEPT

(내부망으로 들어가는 트래픽은 기존 트래픽만 허용되는 상태)
iptables -A FORWARD --in-interface ens32 -d 10.1.1.0/24 -m state --state ESTABLISHED -j ACCEPT

* 잘못 입력한 경우 (화살표 위의 키를 이용해서 해당 줄에서 -A 대신 -D로 변경하고 엔터)
iptables -D FORWARD --in-interface ens32 -d 10.1.1.0/24 -m state --state ESTABLISHED -j ACCEPT

* 마스커레이드(가면) 허가 ----> 사설IP(본얼굴)에 공인IP(가면)을 사용하도록 허용 (NAT설정)

iptables -t nat -A POSTROUTING --out-interface ens32 -j MASQUERADE

* 저장
# iptables-save > /etc/sysconfig/iptables

* 방화벽에 NAT를 영구적으로 적용
# firewall-config

* 재시작
# reboot

* 경로 추적
# traceroute -d www.yahoo.com
# traceroute -d www.facebook.com
(-d : dns 조회 하지 않고)

step9) WinClient의 Filezilla를 이용해서 FTP서버 설정
(내부망에 있는 Client,Server(B)들이 외부에 있는 WinClient의 FTP서버에 접속하는 실습)

step10) Client에서 방화벽을 거쳐서 FTP서버(WinClient)에 접속되는지 확인
dnf -y install ftp // FTP클라이언트 설치
ftp 192.168.111.131
name : centos
password : centos
ftp>

step11)
netstat -na 하고 보면 방화벽의 IP가 보임 ----> NAT설정을 했기 때문에 10.x.x.x대신에 192.168.111.100의 주소가 보여짐

step12) Server(B)_web 를 웹서버로 만들고, 외부에서 내부망으로 Reverse NAT으로 접속하도록 설정하기
(Reverse NAT : 공인IP구간에 있는 사용자가 사설IP구간에 있는 웹서버로 접근하는 것)

cd /var/www/html 안들어가지면

dnf -y install httpd 를 안해서 그렇습니다.

step13) 포트 리디렉션 = 포트 포워딩(Port Forwarding) = Reverse NAT(네트워크)

iptables -t nat -A PREROUTING -p tcp --in-interface ens32 --dport 80 -j DNAT --to-destination 10.1.1.20

iptables -t nat -L //잘 입력되었는지 확인하기

참고) iptables를 작성할 때, 메모장에 작성을 한 후에 검토를 하고 복붙해야 안전

삭제 방법) -A를 -D로 바꾸고 입력하면 됨
iptables -t nat -D PREROUTING -p tcp --in-interface ens32 --dport 80 -j DNAT --to-destination 10.1.1.20
iptables -t nat -L //잘 지워졌는지 확인

ens32 -----> 운영체제에서 가상의 랜카드를 구별하기 위한 번호 (숫자는 하나씩 증가됨, 32, 33, 34, ...) ----> VMware에서 인식하는 번호

* 로그 정리 (방화벽 Server_FW) 실습

- 서버 관리, Cloud에서 분쟁 발생하면 ----> 로그를 봐야함

  Down Time(중단시간) ----> 보상 -----> SLA(Service Level Agreement,서비스 수준 계약)에서 DownTime에 대한 보상 명시

ex) Amazon의 EC2의 SLA 내용에 따르면

  매월 99.99%가용성 보장 ---> 0.0001

  한달=30일=30*24*60*60 ----> 259.2초(4분32초) 동안 DownTime이 발생해도 보상이 없다.

* 가장 많이 사용한 명령이 무엇일까?

```
# tail -30 /var/log/secure
# cat /var/log/secure | awk '{print $5}' | sort | uniq -c
        ( 5번째 컬럼이 명령어 이므로 명령어 부분만 골라냄)
# cat /var/log/secure | awk '{print $5}' | awk -F"[" '{print $1}' | sort | uniq -c
        ( 명령어 뒤에 [PS번호]가 있으므로, [이후를 제거하기 위해서 -F"~~~~"하면 ~~~~이후는 사라짐)
# cat /var/log/secure | awk '{print $5}' | awk -F"[" '{print $1}' | awk -F"]" '{print $1}' | sort | uniq -c
          ( ]도 있으므로 ]도 제거)

# cat /var/log/secure | awk '{print $5}' | awk -F"[" '{print $1}' | awk -F"]" '{print $1}' | sort | uniq -c | sort -rn
        ( 중복을 제거하고 중복 개수에 따라서 내림차순 정렬 -rn : 내림차순 정렬, -n : 오름차순 정렬)

# cat /var/log/secure | awk '{print $5}' | awk -F"[" '{print $1}' | awk -F"]" '{print $1}' | sort | uniq -c | sort -rn > /root/secure.txt
          ( 추출한 결과를 파일로 저장 > 뒤에 파일명)
# cat secure.txt
```

* 쉘 스크립트

- 스크립트(Script) : 텍스트 형태를 그대로 한줄씩 실행하는 방법, 컴파일 과정없음
- 사람의 언어를 이해하고 처리하는 방식, 장비의 특성을 거의 타지 않음 ---> 초보자들도 쉽게 할 수 있음

ex) Script Kiddie : 스크립트를 활용해서 공격을 하는 초보 해커 ex) 요린이(요리+어린이), 주린이(주식+어린이)

* Shell이란?

- 조개껍데기(튼튼)는 연약한 조개속살을 보호하는 역할
- Shell은 리눅스의 내부의 Kernel을 보호하는 역할 -----> 사용자들이 실수 또는 잘못된 명령을 사용해서 운영체제를 잘못되게 하는 것을 방지

* Shell의 종류 : Bash shell, Korn Shell, C Shell, Bourn shell 등등 다양한 종류의 쉘이 있음

- Bash shell이 많이 사용됨 : MAC OS, Linux 등에서 사용
- 2014년에 Bash Shell의 취약점이 발견됨 -----> Shell Shock (http header에 UserAgent 부분을 조작해서 shell명령을 수행하는 기법)