리눅스 수업

Linux – file & directory

명령어

-> ls : 현재 파일의 목록을 보여줌

-> ls -l : 현재 디렉토리 파일과 디렉토리를 좀더 자세히 보여주는 명령어

-> pwd : 현재 위치 표시

-> touch [파일명] : 빈 파일 생성

서버 구축

1. Virtualbox에 리눅스 설치

2. 장치 – 게스트 확장 CD 이미지 삽입 선택후 설치

3. 장치 – 클립보드 공유 및 드래그 앤 드롭 양방향 설정

Vsftpd 설치

1. sudo apt-get update

2. sudo apt-get install vsftpd

3. /etc/vsftpd.conf 파일 설정

4. sudo gedit /etc/vsftpd.conf

아래 내용으로 변경

#inetd 모드 NO standalone 모드 YES

listen=YES

#inetd 모드 NO standalone 모드 YES ip6일때

listen\_ipv6=NO

#익명 접속 허용 여부 설정

anonymous\_enable=NO

#데이터 전송을 위해 Active Mode 사용 여부 설정

port\_enable=NO

#데이터 전송을 위해서 Passive mode를 사용할 것인지 설정

pasv\_enable=YES

#로컬 계정 사용자들의 접속을 허용할 것인가의 여부를 결정

local\_enable=YES

#ftp 전용명령어 중에 write 명령어를 허용할 것인가를 결정

write\_enable=YES

#서버의 FTP 데몬시간을 서버의 표준시간으로 고정할지 설정

use\_localtime=YES

#ftp 접속후에 파일 업로드와 다운로드에 대한 로그를 남길것인가(YES) 남가지 않을 것인가(NO)를 설정

xferlog\_enable=YES

#특정 사용자가 아닌 전체 사용자를 대상으로 chroot()기능을 적용하여

#자기 자신의 홈디렉토링 상위 디렉토리로 이동하지 못하도록 설정

chroot\_local\_user=YES

#FTP 디렉터리에 쓰기 가능하도록 chroot\_local\_user=YES 일때 YES 설정

allow\_writeable\_chroot=YES

#secure chroot()에 사용될 디렉토리를 지정

secure\_chroot\_dir=/var/run/vsftpd/empty

#vsftpd에서 PAM설정파일명으로 사용할 파일명을 지정 /etc/pam.d/vsftpd 파일이 사용

pam\_service\_name=vsftpd

ftpd\_banner=Welcome to My FTP Server!

#SSL을 통한 보안접속을 지원할 것인지에 대해 설정

ssl\_enable=no

rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key

listen\_port=21

pasv\_min\_port=60020

pasv\_max\_port=60030

#utf8\_filesystem=YES

#local\_umask=022

5. sudo systemctl restart vsftpd

- listen=NO로 restart하니 실행이 안되서 YES로 변경하고 나니 실행 잘됨

6. root 계정으로 변환

7. cd ~

8. mkdir firewall\_rules

9. cd firewall\_rules

10. iptables-save > 20210727.rules 현재 날짜를 쓰기

11. iptables-restore < 20210727.rules 방화벽 설정 복구 할 때 사용

12. iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT

13. iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 60020:60030 -j ACCEPT

14. iptables-save > 20210727.rules

15. 20210727.rules 파일 수정 굵은 글씨 부분 추가

# Generated by iptables-save v1.8.4 on Tue Jul 27 14:20:38 2021

\*filter

:INPUT ACCEPT [4:128]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [3:384]

**-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT**

**-A INPUT -p icmp -j ACCEPT**

**-A INPUT -i lo -j ACCEPT**

-A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp --dport 60020:60030 -j ACCEPT

**-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT**

**-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT**

**-A INPUT -j REJECT --reject-with icmp-host-prohibited**

**-A FORWARD -j REJECT --reject-with icmp-host-prohibited**

COMMIT

# Completed on Tue Jul 27 14:20:38 2021

16. 새 터미널에서 firewall\_rules로 이동해서 iptables-restore < 20210727.rules

17. iptables -nL 로 설정 확인

18. apt-get install iptables-persistent 설정 유지를 위해 설치

19. apt-get install iptables-persistent

- yes(엔터) yes(엔터)

/etc/iptables 라는 폴더가 생성되고

rules.v4, rules.v6 가 생성된다.

부팅시 실행되는 파일을 갱신하자. 아래의 작업은 방화벽 수정할 때마다 해주어야 한다.

20. iptables-save > /etc/iptables/rules.v4

Ipv6 차단하기

21. gedit /etc/sysctl.conf

맨 밑에

net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.default.disable\_ipv6 = 1

net.ipv6.conf.lo.disable\_ipv6 = 1

추가

22. sysctl -p 설정 파일 적용

23. 검사

cat /proc/sys/net/ipv6/conf/all/disable\_ipv6

1 이면 disable 적용 완료

24. reboot

25. sudo iptables -nL 확인시 설정 남아 있으면 완료

26. 공유기 포트포워딩 설정후 접속 확인