server)
yum -y install httpd
systemctl restart httpd

systemctl is-active httpd : is-active : active(활성화)인지 확인
systemctl enable httpd : enable 로 변경

systemctl is-enabled httpd : is-enabled : enable(사용가능 상태)인지 확인

desktop)
curl http://10.0.2.20 -> 웹서버 -> 우클릭 -> View Page Source : 볼줄 알아야 한다.

///
desktop)
firewall
//

server)
getenforce
cd /var/www/html
ls
echo “hello world” > a.html
cat a.html : -> hello world 출력되어야 한다.

ls -lz
unconfined

ls -lz /etc/sysconfig/network-scripts/ifcfg-external-static
chcon -t net_conf_t a.html //속성 변경
ls -lz

server)
chcon -t default_t a.html //적절하지 않은 타입 지정
Desktop)

///
server)
 # firewall-cmd --add-service http
 # firewall-cmd --add-service http --permanent
 # chron -t default_t a.html

desktop)
 # curl 10.0.2.20/a.html
///

http response code
https://ko.wikipedia.org/wiki/HTTP_%EC%83%81%ED%83%9C_%EC%BD%94%EB%93%9C

- 1xx (정보): 요청을 받았으며 프로세스를 계속한다
- 2xx (성공): 요청을 성공적으로 받았으며 인식했고 수용하였다
- 3xx (리다이렉션): 요청 완료를 위해 추가 작업 조치가 필요하다
- 4xx (클라이언트 오류): 요청의 문법이 잘못되었거나 요청을 처리할 수 없다
- 5xx (서버 오류): 서버가 명백히 유효한 요청에 대해 충족을 실패했다

server)
chcon -t httpd_sys_content_t a.html
cp /etc/passwd ./b.html
 ls -lz
chron -t default_t

ps -ef | grep httpd
root PID = 5850 PPID = 1(systemd 프로세스)
그 아래 PPID가 동일

 systemctl status httpd
-> 가장 위의 것만 systemd
-> 그아래는 모두 Apache 프로세스가 실행하는 것
cat /etc/

ls -l /etc/passwd
cat (Process) Owner=root -> 소유자인 root는 rw 권한을 가진다.

ps -ef | grep httpd

id apache
uid=48
-> apache는 기타사용자(other)에 속한다.
server)
chmod o+r html

ubuntu -> apache2
ps -ef | grep apache2
w-data가 실행한다.
id w-data
uid=

chcon -t과 퍼미션을 보았다!
SELinux를 enable
p. 73 까지의 내용을 얘기하였다.
프로세스 실행할 때 다 생각할 수 있어야 한다?

firewall-config

ping 10.0.2.20

server)

//
server)
systemctl is-active httpd -> active 확인
systemctl enable httpd -> enable로 변경
systemctl is-enabled httpd -> enable 인지 확인

firewall-config -> firewall 명령어 확인용(귀찮으니까)

cat a.html -> hello world
ls -lZ -> unconfined_u:object_r:**default_t:**s0 **a.html**
-> desktop) curl http://10.0.2.20/a.html -> <h1> Forbidden</h1> 으로 접근 불가능
chcon -t httpd_sys_content_t a.html
ls -lZ -> unconfined_u:object_r:**httpd_sys_content_t**:s0 **a.html**
-> desktop) curl http://10.0.2.20/a.html -> hello world

//
p. 74)
chcon -t default_t a.html
ll -Z
restorecon a.html : content를 원래대로 되돌려라

chcon -t default_t a.html
ll -Z
restorecon -v a.html : content를 원래대로 되돌려라(자세히 보여줌)

chcon -t default_t -R html
ls -lZ
ls -lZ html/
restorecon -R -v a.html : content를 원래대로 되돌려라(자세히 보여줌)

semanage fcontext -l : 이 명령어에서 나온 결과가 기준이 된다 (p. 74)
type
regular
all files

semanage fcontext -l | “ grep /var/www/” | head -1
-> /var/www/(/.*) : 정규형식 메타문자로, 루트 디렉토리의 모든 파일?
////////////////////////////////
ls -> i-bin html
mkdir abc
ll -Z

cd /srv/
ls
mkdir test/html
mkdir -p test/html
ls -ldZ test/html
mkdir -p test/web

srv -> service에 사용할 디렉토리를 만든 것!
srv/(= /srv/ //www

//
cp /etc/httpd/comf/httpd.conf /etc/httpd/comf/httpd.conf.bak
vi /etc/httpd/comf/httpd.conf
-> DocumentRoot 수정
#DocumentRoot "/var/www/html”
DocumentRoot "/web_content”
//이게 다큐먼트 폴더
wq

diff /etc/httpd/comf/httpd.conf /etc/httpd/comf/httpd.conf.bak
: diff명령어로 백업파일과 바뀐것을 비교할 수 있다.
//

/web/app -> DocumentRoot
/web/app/a.html //데스크탑에서 접근해야 한다.

rm -rf /web_content/

cd

mkdir -p /web/app
touch ‘hello web app world: > /web/app/a.html
semanage fcontext -a -t httpd_sys_content_t ‘/web/app(/.*)?’
semanage fcontext

vi /etc/httpd/comf/httpd.conf
-> DocumentRoot
/web/app

//

cd /etc/httpd/conf.d/
ls
-> userdir.conf
cp userdir.conf userdir.conf.bak
vi userdir.conf
17번 라인 주석해제
24번 라인 주석처리
diff userdir.conf userdir.conf.bak
17c17 : userdir.conf 17th 라인 -> userdir.conf.bak 17th 라인
24c24 : userdir.conf 24th 라인 -> userdir.conf.bak 24th 라인

/home/user/public_html
cd ~user : user 계정의 홈디렉토리 이동
cd ~ : 자신 계정의 홈디렉토리 이동

/home/user/public_html/
http://x.x.x.x/~user
/home/abc/public_html/

httpd 프로세스(apache)가 접속할 수 있어야하는 데 현재는 불가능(권한 700이기 때문에! -> 권한 711로 바꿔줘야한다.)
execute가 있다는 것은 넘어갈 수 있다는 뜻으로
chmod 711 user

systemctl reload httpd

pwd -> /home/user
mkdir public_html
ll -Z public_html
ll -dZ public_html
semanage f

Desktop)
curl httpL//10.0.2.10/~user

p. 76)
SELunix 부울
getsebool -a | grep homedir
-> httpd enable homedir --> off : 홈디렉토리 접근 막음 -> 변경 방법
setsebool httpd_enable_homedirs { on | off } : 정책을 키고 끄기 가능
getsebool -a | grep homedir : 변경 확인
//정책을 키고 끄기 가능하나, 재부팅 시 원래대로 돌아감
-> setsebool -P httpd_enable_homedirs { on | off } : 영구적으로 정책 변경

semanage boolean -l | head

semanagee boolean -l | grep httpd_enable_homedirs
setsebool -P httpd_enable_homedirs off
semanagee boolean -l | grep httpd_enable_homedirs

setsebool -P httpd_enable_homedirs on : 영구적인 설정
setsebool httpd_enable_homedirs on : 현재 상태만 설정

semanage boolean -m -l httpd_enable_homedirs
semanage boolean -l | grep httpd_enable_homedirs
-> 어떤 명령어를 사용해도 가능하다.

desktop)
http://10.0.2.20/~user : 디렉토리 리스팅 : 디렉토리 목록을 본다. -> 웹의 기능 중 하나!
그

p. 77)
useradd user1 : 유저 만들기
su - user1 : user1로 전환하기
mkdir public_html
ll -Z
ls
chmod 711 user1
ll

desktop)
curl http://10.0.2.20/~user/a.html

server)
getsebool -a } grep httpd_enable
setsebool httpd_enable_homedirs on

Desktop)
curl http://10.0.2.20/~user/

임의의 유저를 만들어서 접근

명령어가 아닌 내가 무엇을 해야 하는 지를 봐야 한다.
-> 사용자 생성, 패스워드 고려, 컨텍스트 확인, 레이블 확인, boolean 정책 확인
-> 무엇을 해야 하는 지가 중요 -> 명령어는 모르면 찾아볼 수 있다.
-> 그러나, 무엇을 해야 되는 지를 모르면 할 수가 없다.

p. 69부터 시작

//////////////////
p. 70)
chcon : 파일의 컨텍스트를 일시적으로 변경
chcon -t : 컨텍스트 유형을 변경
ex) chcon -t httpd_sys_content_t a.html
ls -Z a.html : 변경된 컨텍스트 유형 확인

restorecon : 인자로 지정된 컨텍스트가 디렉토리에 지정된 컨텍스와 일치 하지 않을 경우 시스템에 등록된 보안 레이블 정책에 맞게 파일의 컨텍스트를 복구하는 명령. chcon명령과는 다르게 컨텍스트를 지정하지 않아 사용이 간단(장점)하나 수동 컨텍스트를 지정할 수 없다(단점)
restorecon명령을 영구적으로 설정하려면 semanage fcontext를 함께 사용한다.

p.

1. context 만 변경
   /var/www/html/a.html

   etc/passwd

   context 변경해서 default 변경하여 forbiden 만들어서

   http 선택 코드(4xx 번)

2. 디렉토리 루트 변경

var/www/html/ -> 원래 디렉토리 루트
그 루트를 root 디렉토리안에 /web/app 디렉토리 만들어서
디렉토리 루트를 옮긴다? -> vj

//

vi /etc/httpd/conf/httpd.conf
-> 42번째 라인 -> 서비스 포트 : listen 80
ss-tnlp | grep http

Listen 10.0.2.20:80 -> 해당 IP를 가진 사용자만 접근 허용(?)

systemctl status httpd

systemctl

port numbers -> 8080
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=8080
System Ports (0-1023), User Ports (1024-49151), and the Dynamic and/or Private Ports (49152-65535)
-> 1000번대 이상은 일반 사용자도 사용 가능
8080 포트를 웹할 때 많이 사용한다.
FQDN 에서 :80은 생략 되어있는 것
회사 내부에서 사용하는 포트(회사 직원들만 사용하는 포트) ->보안 때문에 비표준으로 사용하는 포트들도 많이 있다.

-> Lestens 80
systemctl restart httpd
-> systext error -> journalctl -XE

firewall -cmd --add-port=8080/tcp : 방화벽이 임시적으로 8080 포트를 열어줌

listen 8080
systemctl restart httpd -> 오류발생
systemctl status httpd 0l
failed
**permission denied ~ make sock : could not bind to address -> bind port : 어떤 **

semanage port -l | grep http
포트레이블 프로토콜 포트번호

http_cache_port_t tcp 8080
http 라는 3가지 레이블에만 접근이 가능하다.

semanage port -b

p. 80)
semanage port_t -p tcp 8088
semanage port -l | grep http -> 8088 port 추가된 것을 볼 수 있다.

systemctl is-active httpd

ss -tnlp | grep http : 현재 연결되어 있는 포트를 확인
firewall-cmd --add-port=8088/tcp -> success

desktop)
curl http://10.0.2.20:8088/a.html

///
ssh의 포트를 묶어라
semanage port -l | grep ssh
ssh_port_t -> tcp 22 밖에 없음
semanage port

systemctl restart sshd
systemctl status sshd

ss -tnlp | grep

semanage port -a http_port_t -p tcp 8088 // 8088 추가
semanage port -l | grep httpd
firewall-cmd --add-port=2022/tcp
// desktop) curl 10.0.2.20:8080/a.html

semanage port -d -t ssh_port_t -p tcp 2222
semanage port -l | grep http -> history 등으로 찾아서 해본다.
semanage port -d -t http_port_t -p tcp 8088
semanage fcontext -d -t httpd_sys_content_t '/web-content(/.*)?'
semanage fcontext -d -t httpd_sys_content_t '/web/app(/.*)?'
semanage boolean -m -0 httpd_enable_homedirs
firewall -cmd --reload
사진 확인

apache(httpd 프로세스)
//이전까지는 루트가 실행
//퍼미션 제어를 받지 않기 때문에 DAC기법에서는 막을 수 없다,
//레이블을 이용해서 접근 제어

//
<원래대로 돌리기>
1. sshd_config.bak => sshd_config 복사
2. httpd.conf.bak => httpd.conf 복사
3. userdir.conf.bak => userdir.conf 복사

semanage port -d -t ssh_port_t -p tcp 2222

semanage port -l | grep ^http
semanage port -d -t http_port_t -p tcp 8080
semanage port -d -t http_port_t -p tcp 8088

semanage fcontext -d -t httpd_sys_content_t '/web_content(/.*)?'
semanage fcontext -d -t httpd_sys_content_t '/web/app(/.*)?'

semanage boolean -m -0 httpd_enable_homedirs

firewall-cmd --reload
//
p. 82) SELinux 문제 해결

1. enforcing mode -> permissive mode 전환
2. 파일의 보안 레이블 확인
3. 포트 레이블 확인
4. 부울 확인
   -> 모든 문제는 이 3가지로 확인 가능하다.

어떤 log파일에 기록되는 가?
-> /var/log/messages : 대부분의 log파일은 messages 에 남는다.

auditing -> 감사
audit 안에 AVC 정책이 남는다.

accounting -> 회계, 보안) 감사추적

p. 84)
audit log 파일 확인
grep denied /var/log/audit/audit.log : 정책 위반한 것들을 차단한 것 찾기

name bind
permissive=0 -> enforcing

grep “SELinux is preventing” /var/log/messages
sealert -l <a2tg44fff4w21bd223128…> 명령어 -> 마우스 휠 복사
Target RPM
Raw Audit messages

type=SYSCALL msg=audit… success=no

grep “SELinux is preventing” /var/log/messages | grep sealert -l

sealert -b (GUI 환경 제공)
ignore : 경고창 무시
delete : 경고창 삭제
troubleshoot : 문제 해결 방식이 나옴

DNS

FQDN : IP 변환 //도메인을 IP Fh

우분투)
cat /etc/hosts //대부분의 유닉스 계열은 /etc/안에 존재

윈도우)
c:\windows\system32\drivers\etc\hosts

cat /etc/hosts :

ARPA
DARPA(Defense Advanced Research Projects Agency) -> 미군의 방어에 관한 연구를 하는 연구기관 -> 하부 기관 : ARPA -> ARPANET : internet을 최초로 만든 기관 -> 현재 인터넷으로 발전. ARPANET은 보통 네트워크라는 의미로 많이 사용됨

PDP :시스템
유닉스를 만든 시스템이 PDP7

hosts file 검색
ARPANET에서 만든(사용하는) 파일로, IP가 아닌 도메인명으로 통신을 하게 되었다~
그렇다~
호스트이름 : desktop
FQDN : desktop.cccr.net
-> standford Research institute에서 hosts file 주기적으로 업데이트시켜준다.
-> 로컬 호스트만 등록한다.

-> 시스템에서 도메인명으로 검색할 때 DNS서버에 먼저 묻기 전에 hosts file을 먼저 확인하여 ip로 변환해준다. (우선순위 : hosts file > DNS서버)
-> 악성코드가 hosts file을 조작하는 경우가 많다. 똑같은 국민은행 홈페이지 -> 공인인증서, 보안카드 입력 -> 사이버 범죄에 이용된다.

p. 98)
DNS 명령어
host 명령어
nslookup 명령어
dig 명령어
-> 세 가지 명령어 모두 DNS에 질의(query)를 한다.

DNS Query : FQDN으로 질의
DNS Answer : IPv4 전송

host www.naver.com
-> www.naver.com is an alias for www.naver.nheos.com. : 네이버는 네이버.nheos의 별칭이다.

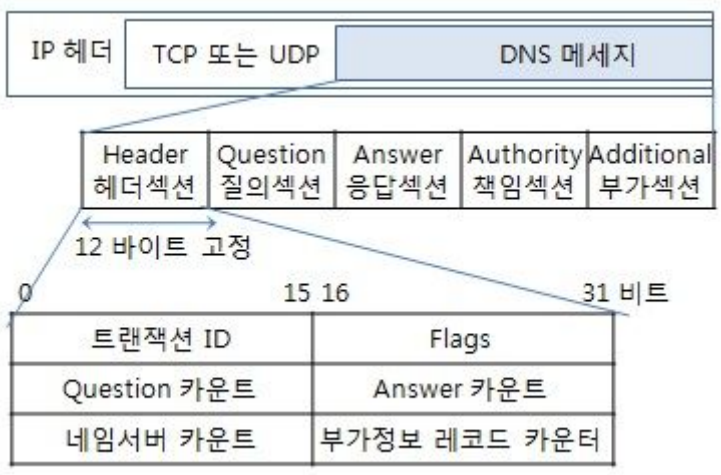
네이버는 ping을 막아놓았다.

host www.daum.net
-> www.daum.net is an alias for www.g.daum.net

www.google.co.kr
www.google.com
-> 이 두 가지의 IP주소는 다르다.

host -v : DNS Header를 보는 것. v = verbose

DNS Header 검색
http://www.ktword.co.kr/abbr_view.php?m_temp1=2194



http://www.networksorcery.com/enp/protocol/dns.htm -> 더 자세한 헤더 내용 확인 가능 사이트

host -v www.google.com
IN(internet)
p. 96)
A(DNS 레코드 -> A : ipv4 , AAAA -> ipv6)
264초 후 삭제

우분투는 특이하다.
cat /etc/resolv.conf -> 127 : 자기자신

host -v -t A www.google.com
-t : 레코드 타입 A= ipv4
ipv4만 들어온다.
-t MX
-t NS
-t PTR
-t SOA
…

host -v -t A www.google.com
-> 질의 1번 -> 응답 3번(DNS 서버 설정에 따라 개수는 다르다.)
CNAME : 호스트의 별칭 -> www.naver.com, www.daum.net
원래의 호스트 명을 쓰면? 바로 응답온다!
www.naver.nheos.com.
www.g.daum.net.

SOA(Start Of Authority)

영역(zone)을 시작할 수 있는 권한을 가지고 있는 사람에 대한 정보

host -t A www.daum.net
NS(Name Server) : 도메인 서버 -> DNS 서버
host -t A ns1.daum.net :NS서버의 ip 주소 알아오기

MX: Mail eXchange server)
host -t MX daum.net

아침@naver.com
이슬@google.com

MX서버는 Gmail Mail server로 던져준다.
host -t MX gmall.com

TXT -> 보고 알수 있는 것은 전혀 없다!
PTR : 포인터 ->IP주소를 물어봤을 때 FQDN를 알려 주는 것
host -v -t PTR www.naver.com
host -t PTR 210.89.164.90

A/AAAA : FQDN -> IP (정방향, Forward lookup)
PTR : IP -> FQDN (역방향, Reverse lookup)
in-addr.arpa. : 역방향으로 질의할 때 사용
Host 90.164.89.210 : 원래 ip주소의 역방향으로 전송한다.

역방향이 왜 필요할까?
UDP 53을 쓴다. -> UDP는 세션이 없음. 누구랑 통신하는 지 모름 -> 돌아오는 응답을 검증할 수 있는 방식이 없다.(가짜 응답(조작 응답)이 돌아와도 검증할 수 없음)
GUI 환경에서 검증하는 방법은 DNS서버에 해당 IP주소로 재질의 해보고 응답 없으면 이상함을 감지할 수 있다.(가짜 사이트일 수도 있다는 것을 인식)

nslookup
dig
host -t A www.google.com 8.8.8.8 : FQDN 다음으로 DNS서버를 지정할 수 있다.

host -t NS daum.net
host -t A ns1.daum.net

host -v -t A www.daum.net >

p.90 ~ 107 내용이해하기
p. 93)
DNS Query

1. 재귀 쿼리(recursive query
2. 순환 쿼리

DNS Response(=Answer)

1. 권한이 있는 응답
2. 권한이 없는 응답

DNS 계층 구조

Root Hint

DNS Record Type