[Linux] Chapter 11 , 15

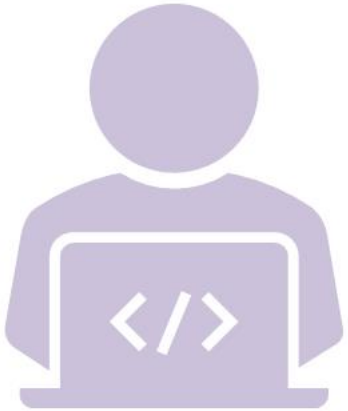
[GBC20190027] Linux(+USP)

27기 최하영

Agenda

Chapter 11. 네트워크 설정

Chapter 15. 리눅스 보안의 기초



11. 네트워크 설정

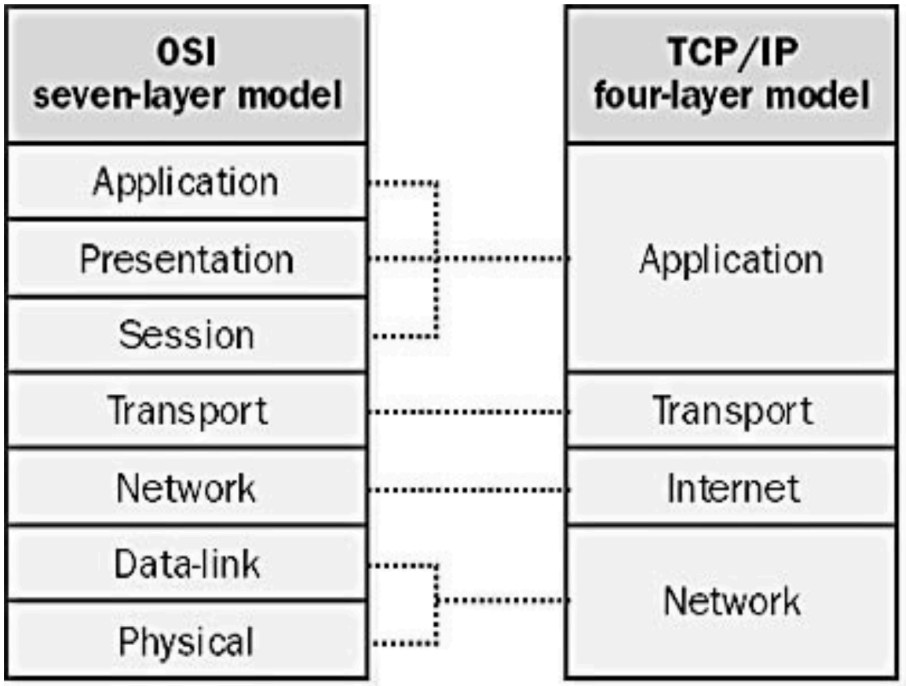
[GBC20190027] Linux(+USP)

11-1. 네트워크의 기초

1. TCP/IP프로토콜

-프로토콜 : 컴퓨터와 컴퓨터 사이에서 데이터를 어떻게 주고받을 것인지를 정의한 통신규약 (같은 프로토콜을 사용하는 기기 간에는 통신이 가능함)

- 인터넷 네트워크 → TCP/IP
- 다섯 계층으로 구성됨
- 각 계층별로 다양한 서비스 제공
- 전송 계층의 TCP와 네트워크 계층의 IP로 전체 프로토콜을 대표하여 TCP/IP 프로토콜이라 부름



11-1. 네트워크의 기초

1. TCP/IP프로토콜

계층	기능	프로토콜	전송 단위
응용 계층	서비스 제공 응용 프로그램	DNS, FTP, SSH, HTTP, Telnet	메시지
전송 계층	응용 프로그램으로 데이터를 전달, 데이터 흐름 제어 및 전송 신뢰성 담당	TCP, UDP	세그먼트
네트워크 계층	주소 관리 및 경로 탐색	IP, ICMP	패킷
링크 계층	네트워크 장치 드라이버	ARP	프레임
물리 계층	케이블 등 전송 매체	구리선, 광케이블, 무선	비트

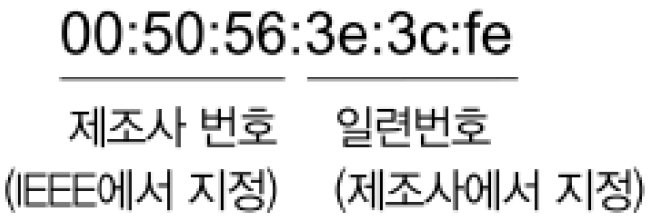
11-1. 네트워크의 기초

2. 주소

- 일반 사용자들이 유선이나 무선 네트워크에서 사용하는 인터페이스
  → 이더넷 방식 사용

1) MAC 주소 (Media Access Control)

- MAC 주소는 하드웨어를 위한 주소
- 이더넷 주소, 하드웨어 주소, 물리 주소라고 함
- 네트워크 인터페이스 카드(랜 카드)에 저장된 주소
- 네트워크 인터페이스 카드가 만들어질 때 부여되며, 원칙적으로 수정 X,
  but, 일부 네트워크 인터페이스 카드의 경우 사용자가 MAC주소 수정 허용
- MAC 주소 -→ 각 하드웨어를 구별하는 역할 수행
- 쌍점(:)이나 붙임표(-)로 구분되는 여섯 개의 16진수로 구성됨, 총 48비트



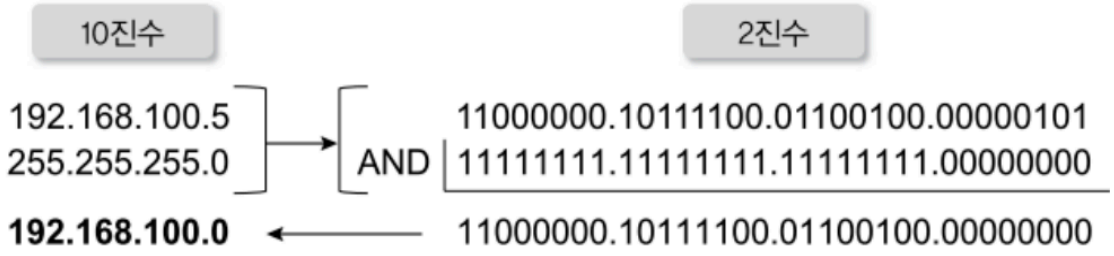
11-1. 네트워크의 기초

2) IP주소 (Internet protocol)

- 인터넷으로 연결된 네트워크에서 각 컴퓨터를 구분하기 위해 사용됨
- IP주소는 1바이트 크기의 네 자리 숫자로 구성되므로 총 4바이트 (32bit)
- IP주소는 네트워크를 구분하는 네트워크 주소, 해당 네트워크 안에서 특정 컴퓨터를 식별하는 호스트 주소로 나뉨
- 총 32비트 중 몇 비트를 네트워크 부분을 사용하고, 나머지 몇 비트를 호스트 부분으로 사용하는지에 따라 A, B, C 클래스로 구분함

3) 넷마스크와 브로드캐스트 주소

- 넷마스크 : IP주소와 AND연산을 수행하여 네트워크 부분만 남기는 역할
- 브로드캐스트 주소 : 같은 네트워크에 있는 모든 컴퓨터에 메시지를 보낼 때 사용하는 것으로 호스트 부분을 모두 1로 설정함 (ex. 192.168.100.255)



11-1. 네트워크의 기초

4) 호스트 이름

- 호스트 이름도 IP주소처럼 네트워크/호스트 부분으로 구분됨

  ex) www.naver.com //www→ 네트워크, naver.com → 호스트

5) 포트 번호

- 각 서비스를 구분하는 번호
- 사용자가 네트워크 서비스를 이용할 때 사용자의 패킷은 IP 주소를 보고 해당 서버 컴퓨터를 찾아감 ☛ 서버 컴퓨터에 도착한 사용자의 패킷은 어떤 서비스를 요청한 것인지 확인한 다음 해당 데몬에 패킷 전달 → 사용자가 어떤 서비스를 요청했는지 구분해 주는 것이 '포트 번호'임.
- 전송 계층에서 사용하는 번호
- /etc/services : 각 서비스별로 포트 번호가 무엇인지 정의

11-2. 네트워크 설정

0. 네트워크 사용하기 위해 설정해야 할 것

- IP 주소
- 넷마스크와 브로드캐스트 주소
- 게이트웨이 (라우터) 주소
- DNS 주소

1. 호스트 이름 설정하기

- 호스트 이름은 해당 기관의 도메인 이름에 서버에서 제공하는 대표적인 서비스 이름을 붙이는 것이 편리함

  ex) 도메인 이름이 han.server 이고 주로 메일을 서비스하는 서버라면
  mail.han.server라고 하는 것

- 붙인 이름은 호스트 이름 설정 파일에 저장 + DNS에 등록해야만
  ➔ 서비스를 제공할 수 있음

11-2. 네트워크 설정

* 호스트 이름 확인하기 : uname -n, hostname

$ uname : 시스템 정보 출력
-n 옵션 : 호스트 이름을 출력함
-a 옵션 : 호스트 이름 포함하여 시스템 관련 정보 출력

$ hostname : 호스트 이름을 출력 + 설정
hostname [new hostname] : 호스트 이름을 변경할 수 있음

* 호스트 이름 설정 파일
→ **/etc/hostname** : 단순히 도메인 이름을 포함한 호스트 이름만 저장하고 있음
이 파일의 내용을 수정하면 재시작해도 호스트 이름을 유지할 수 있음
[!] 호스트 이름을 새로 정의할 때, 한 네트워크에서 같은 이름을 사용하는 다른 호스트가 있으면 안된다

11-2. 네트워크 설정

2. 네트워크 인터페이스 설정하기

- 리눅스 시스템을 네트워크에 연결하려면 → IP 주소를 할당 받아야 함
- 같은 네트워크 내에서 동일한 IP주소를 가지고 있는 시스템이 있으면 안됨!
- 네트워크 인터페이스 설정 시 → IP주소, 넷마스크, 브로드캐스트 주소 함께 설정

* 현재 설치된 네트워크 인터페이스 설정 확인하기 : **ifconfig**
  - 보통 시스템에 네트워크 인터페이스는 하나지만 경우에 따라 두 개 이상 장착할 수도 있음

* 특정 네트워크 인터페이스 설정 확인하기
  $ ifconfig eth0
* 네트워크 인터페이스 사용 해제하기 : down 옵션
  $ sudo ifconfig eth0 down
* 네트워크 인터페이스 활성화하기 : up 옵션

* /etc/network/interface 파일에 IP주소와 넷마스크를 지정해야, 부팅할 때 네트워크가 설정됨

11-2. 네트워크 설정

3. 게이트웨이 설정하기

- 인터넷 : 네트워크와 네트워크를 연결한 것
- 게이트웨이 : 네트워크를 다른 네트워크와 연결할 때 연결점이 되는 장치
- 게이트웨이도 하나의 컴퓨터 → 보통 라우터라고 부름
- 게이트웨이는 패킷을 보고 같은 네트워크로 보내는 것이 아니면 외부로 전송함
- 게이트웨이 주소가 설정되어 있지 않으면, 같은 네트워크가 아닌 컴퓨터와는 접속이 불가능함
- 게이트웨이의 설정과 확인 ➔ **route** (라우팅 테이블 편집하는 명령)

* 라우팅 테이블 보기 : route
* 기본 게이트웨이 삭제하기 : route del
* 기본 게이트웨이 설정 : route add

* 라우팅 : 어떤 네트워크 안에서 통신 데이터를 보낼 경로를 선택하는 과정
* 라우팅 테이블 : 패킷이 목적지까지 가는 거리와 가는 방법 등을 명시하고 있음

11-2. 네트워크 설정

4. DNS 설정하기

- DNS(Domain Name Service)는 호스트 이름을 IP주소로 바꾸는 역할을 수행함
- DNS가 설정되어 있지 않을 경우 → 직접 IP주소를 사용해야 접속 가능

* DNS 서버 지정하기
  - 리눅스는 DNS 서버의 주소를 **/etc/resolv.conf** 파일에 저장함

* DNS 서버에 질의하기
  $ **nslookup** : DNS 서버와 대화식으로 질의하고 응답을 받는다
  nslookup [도메인명]

11-3. 네트워크 상태 확인

0. 네트워크의 상태 확인

- 외부와 통신이 잘되는지 확인하는 명령
- 라우팅 및 열려 있는 포트 확인하는 명령
- 네트워크의 이상 유무를 점검하기 위해 패킷을 캡처하는 명령

1. 통신 확인하기

- 네트워크에서 통신이 가능한지 확인하는 명령 : ping
- ping은 해당 시스템이 외부와 통신되는지 + 외부 서버가 동작하는지 확인
- -c 옵션 : 보낼 패킷 수를 지정할 수 있음
- -q 옵션 : 아무 메시지도 출력되지 않다가 ctrl + c로 종료하면 통계 정보만 출력
- 도메인 이름을 사용하는 경우 : ping + [도메인 이름]

11-3. 네트워크 상태 확인

2. 통신 경로 확인하기

- $ traceroute : 목적지 시스템까지의 네트워크 경로 추적
  (= 목적지까지 패킷이 거치는 경로 출력)
- 정상적으로 경로가 확인되는 경우
- 정상적으로 경로가 확인되지 않는 경우 → * 출력

```
choehayeong-ui-MacBookPro:~ hayeong$ traceroute handong.edu
traceroute to handong.edu (211.253.29.84), 64 hops max, 52 byte packets
 1  172.17.220.1 (172.17.220.1)  2.375 ms  2.836 ms  1.583 ms
 2  10.0.1.254 (10.0.1.254)  1.294 ms  1.178 ms  1.080 ms
 3  118.41.84.126 (118.41.84.126)  3.839 ms  2.543 ms  2.013 ms
 4  119.202.127.21 (119.202.127.21)  1.911 ms  1.484 ms  1.543 ms
 5  * * *
 6  112.190.135.177 (112.190.135.177)  5.899 ms  2.433 ms  3.583 ms
 7  112.190.189.101 (112.190.189.101)  8.747 ms  5.873 ms  5.232 ms
 8  * * *
 9  112.174.62.234 (112.174.62.234)  11.812 ms
    112.174.62.226 (112.174.62.226)  11.121 ms
    112.174.62.198 (112.174.62.198)  12.850 ms
10  112.188.240.202 (112.188.240.202)  9.829 ms  10.091 ms  9.088 ms
```

11-3. 네트워크 상태 확인

3. 네트워크 상태 정보 출력하기

- $ netstat : 네트워크 연결 상태, 라우팅 테이블, 인터페이스 관련 통계 출력
  현재 시스템에 열려 있는 포트도 확인 가능
- 라우팅 테이블 확인하기 : -r 옵션
- 현재 열려 있는 포트 확인하기 : netstat -an | grep LISTEN
- 현재 열려 있는 포트를 사용 중인 프로세스 확인하기 : -p 옵션
- 인터페이스별 네트워크 통계 정보 확인하기 : -i 옵션
- 프로토콜별 네트워크 통계 정보 확인하기 : -s 옵션

```
choehayeong-ui-MacBookPro:~ hayeong$ netstat -r
Routing tables

Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            172.17.220.1       UGSc           69       40     en0
127                localhost          UCS             0        0     lo0
localhost          localhost          UH              2   397368     lo0
169.254            link#6             UCS             2        0     en0      !
169.254.11.188     c8:ff:28:26:da:f1  UHLSW           0        0     en0      !
```

```
choehayeong-ui-MacBookPro:~ hayeong$ netstat -an | grep LISTEN
tcp4       0      0  127.0.0.1.59354        *.*                    LISTEN
```

11-3. 네트워크 상태 확인

4. MAC 주소와 IP 주소 확인하기

- $ arp : 같은 네트워크에 연결된 시스템들의 MAC 주소와 IP 주소 확인하기
  (address resolution protocol)
  ARP 캐시 정보를 관리함
- 현재 같은 네트워크에 연결되어 있는 시스템의 맥 주소와 IP 주소를 출력함

```
hayeong@hayeong-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Ifac
e
_gateway                 ether   52:54:00:12:35:02   C                     enp0
s3
```

11-3. 네트워크 상태 확인

5. 패킷 캡처하기

- $ tcpdump : 네트워크의 상태를 확인하기 위해 패킷을 캡처하여 분석할 때 사용
  (= 네트워크상의 트래픽을 덤프한다)
- 옵션 X : 현재 시스템에서 주고받는 모든 패킷을 캡처하여 패킷의 헤더 부분 정보를 출력함

```
choehayeong-ui-MacBookPro:~ hayeong$ sudo tcpdump
Password:
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pktap, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
18:12:32.809885 IP 52.109.76.36.https > 172.17.220.149.60307: Flags [P.], seq 54
3869793:543869900, ack 4102209349, win 122, options [nop,nop,TS val 1378401292 e
cr 1148396226], length 107
18:12:32.809934 IP 172.17.220.149.60307 > 52.109.76.36.https: Flags [.], ack 107
, win 2046, options [nop,nop,TS val 1148396521 ecr 1378401292], length 0
18:12:32.810334 IP 172.17.220.149.60307 > 52.109.76.36.https: Flags [P.], seq 1:
374, ack 107, win 2048, options [nop,nop,TS val 1148396521 ecr 1378401292], leng
th 373
18:12:32.810472 IP 172.17.220.149.60307 > 52.109.76
4:1067, ack 107, win 2048, options [nop,nop,TS val
ength 693

36 packets captured
137 packets received by filter
0 packets dropped by kernel
```

11-3. 네트워크 상태 확인

- 캡처할 패킷 개수 지정하기 : -c 옵션
- 캡처한 패킷 정보를 파일로 저장하기 : -w 옵션
- 캡처한 패킷 파일 읽기 : -r 옵션
- 특정 포트로 송수신되는 패킷 캡처하기 : tcp port 옵션
- 캡처한 내용을 ASCII로 보기 : -X 옵션

명령어	설명
ping	통신 가능 여부
traceroute	통신 경로 확인
netstat	네트워크 상태 확인
arp	MAC주소와 IP주소 확인
tcpdump	패킷 캡처

15. 리눅스 보안의 기초

[GBC20190027] Linux(+USP)

15-1. 정보 보안의 기초

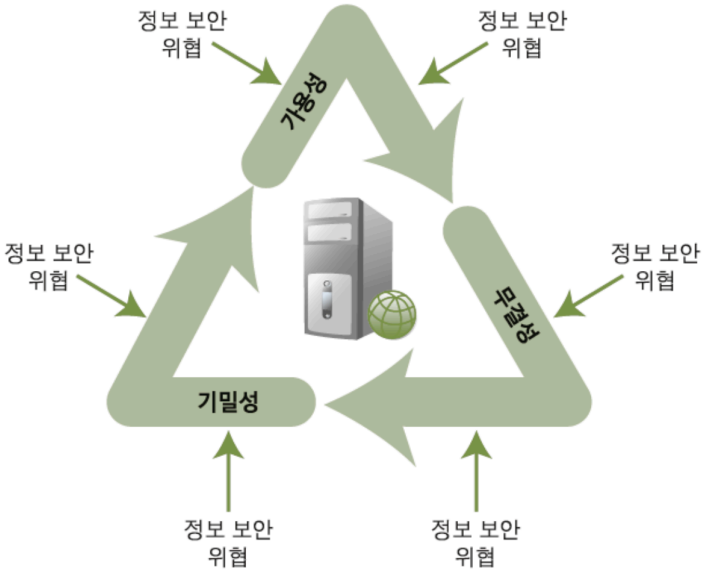
1. 정보 보안의 정의

- 정보 자산을 여러 가지 위협으로부터 보호하여 기밀성, 무결성, 가용성을 유지

1) 기밀성 (Confidentiality)
- 허가 받은 사용자만이 해당 정보에 접근할 수 있도록 하는 것
- 사용자를 인증하는 것과, 접근 권한 제어, 데이터 암호화 등

2) 무결성 (Integrity)
- 정보가 무단으로 변조되지 않았음을 의미함
- 해당 정보가 완전하며 정확하다는 것을 보장
- 정보가 원본과 동일하다는 것을 보증하는 전자 서명 기법을 활용함

3) 가용성 (Availability)
- 필요할 때 인가 받은 사용자가 정보나 서비스에 접근할 수 있는 것을 말함
- 디도스 공격 → 가용성을 제공하지 못하도록 하는 공격



15-1. 정보 보안의 기초

2. 보안 기본 조치

1) 불필요한 서비스 통제하기
- 보안 위협은 네트워크를 통해 발생하므로, 꼭 필요하지 않은 서비스 포트는 모두 막는 것이 좋음 → 일반적으로 모든 포트 막고, 서비스 제공하려는 포트만 열어주는 것이 좋음
- 서비스 통제 → 불필요한 서비스 자체를 제거하는 방법 + 방화벽에서 패킷을 필터링하는 방법 함께 사용

2) 소프트웨어 패치 설치하기
3) 주기적으로 점검하기
4) 백업하기
5) 공부하는 시스템 관리자

15-2. 시스템 로그

0. 로그

- 커널과 리눅스 시스템이 제공하는 여러 서비스와 응용 프로그램이 발생시키는 메시지를 뜻함
- 로그 파일 : 로그를 저장하고 있는 파일 (→ 시스템의 상태 확인할 수 있음)

1. 주요 로그 파일

- 대부분의 로그 파일이 /var/log 디렉터리에 있다
- 공통적인 로그를 기록 : /var/log/syslog

2. 로그 관리 데몬

- rsyslog 서비스를 제공하는 데몬 ➔ rsyslogd
- rsylog 서비스를 설정하는 파일 ➔ /etc/rsylog.d 디렉터리에 있는 *.conf

15-3. 방화벽 관리

1. 방화벽 동작 확인하기
- 방화벽의 서비스 이름 : ufw
- 방화벽 시작 : sudo ufw enable
- 방화벽 종료 : sudo ufw disable

2. GUI 도구로 방화벽 설정하기
-gufw 이용

3. 방화벽 관리 명령
- 방화벽 설정 : ufw
- 방화벽의 상태보기 : ufw status
- 규칙 추가하기 / 특정 IP접속 설정 : ufw allow [서비스명/IP]
- 서비스 거부하기 : ufw deny [서비스명]
- 규칙 삭제하기 : ufw delete [서비스명]
- 포트 추가하기 : ufs allow [포트 번호]

15-4. 보안 관리 도구

1. NMap : 포트 스캔 도구

- 자신의 서버나 원격의 서버가 사용 중인 포트, 운영체제 등을 스캔하여 출력함
- 네트워크 관리용 / 취약한 포트가 사용 중인지 확인하기 위한 보안용
- 스캔하는 것만으로도 보안 침입을 위한 준비과정으로 간주됨

- $ nmap : 네트워크를 탐색하고 보안을 점검함
- 지정한 호스트에서 현재 열려 있는 포트를 요약해서 출력 해줌
- 특정 서버 스캔하기 : -O 옵션 (root 권한 필요)
  → 시스템 동작 여부, 운영체제, TCP 포트 번호 알 수 있음
- UDP 포트 스캔하기 : -sU 옵션
- 특정 네트워크 대상으로 포트 스캔 : 네트워크 주소 지정

15-4. 보안 관리 도구

2. PAM

- PAM (Pluggable authentication modules) : 삽입형 인증 모듈
- 각 서비스 별로 인증 파일 (PAM 파일)을 설정함
- PAM 설정 파일 위치 : /etc/pam.d 디렉터리에 설정 파일을 가지고 있음
- PAM 설정 파일 형식 : <모듈 종류> <제어 플래그> <모듈 이름> <모듈 인자>
- 모듈 인터페이스
  1) auth : 사용자 인증 + 그룹 지정에 사용
  2) account : 접근이 허용되는지 여부 확인
  3) password : 사용자 계정의 암호 변경
  4) session : 사용자의 세션을 설정하고 관리 + 접근 허용 부가 작업 수행
- 제어 플래그 : 특정 모듈의 성공과 실패를 어떻게 처리할 것인지를 알려줌
- 모듈 이름 : 삽입 가능한 모듈의 이름 지정
- 모듈 인자 : 인증 과정에서 정보가 필요한 일부 모듈에 정보 전달