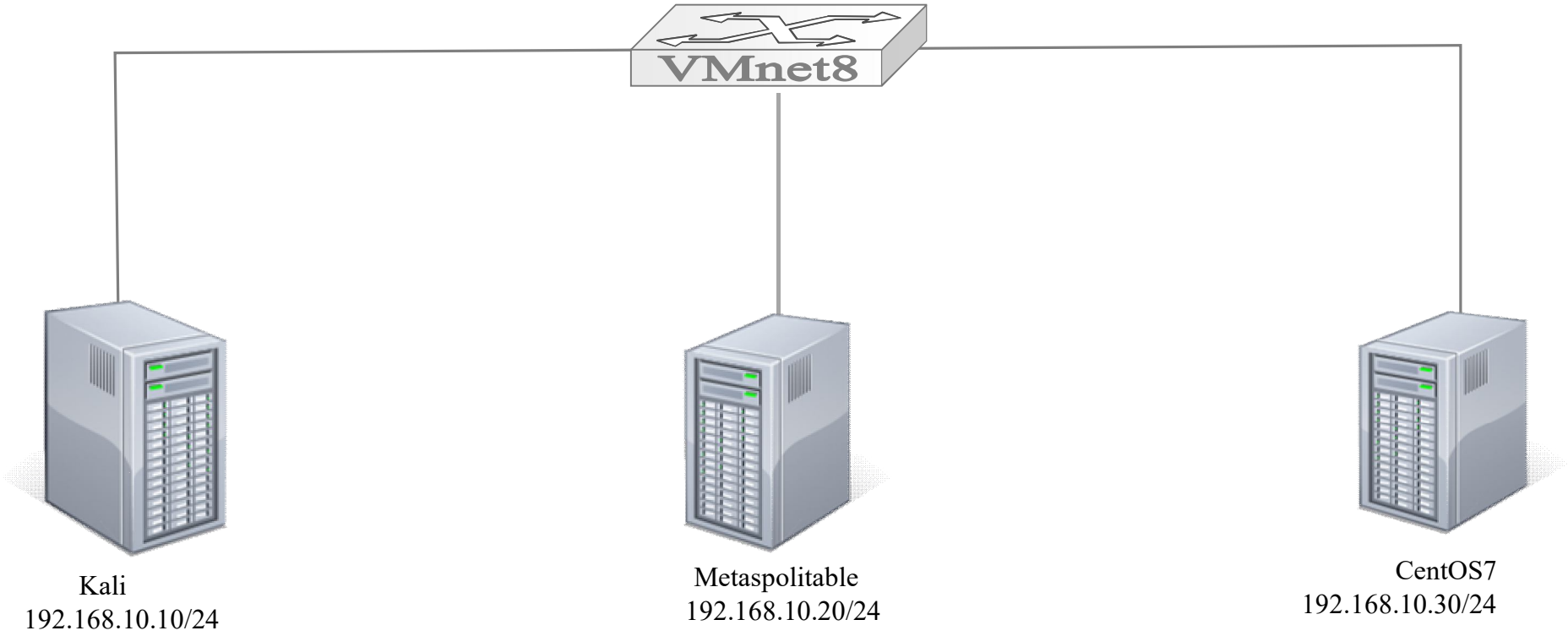
시스템 보안

목차

0. 시스템 보안 실습환경 & Linux 구조

* 실습 환경


VMnet8
Kali
192.168.10.10/24
Metaspolitable
192.168.10.20/24
CentOS7
192.168.10.30/24

다운로드 파일 ❶ VMware Workstation Pro Download

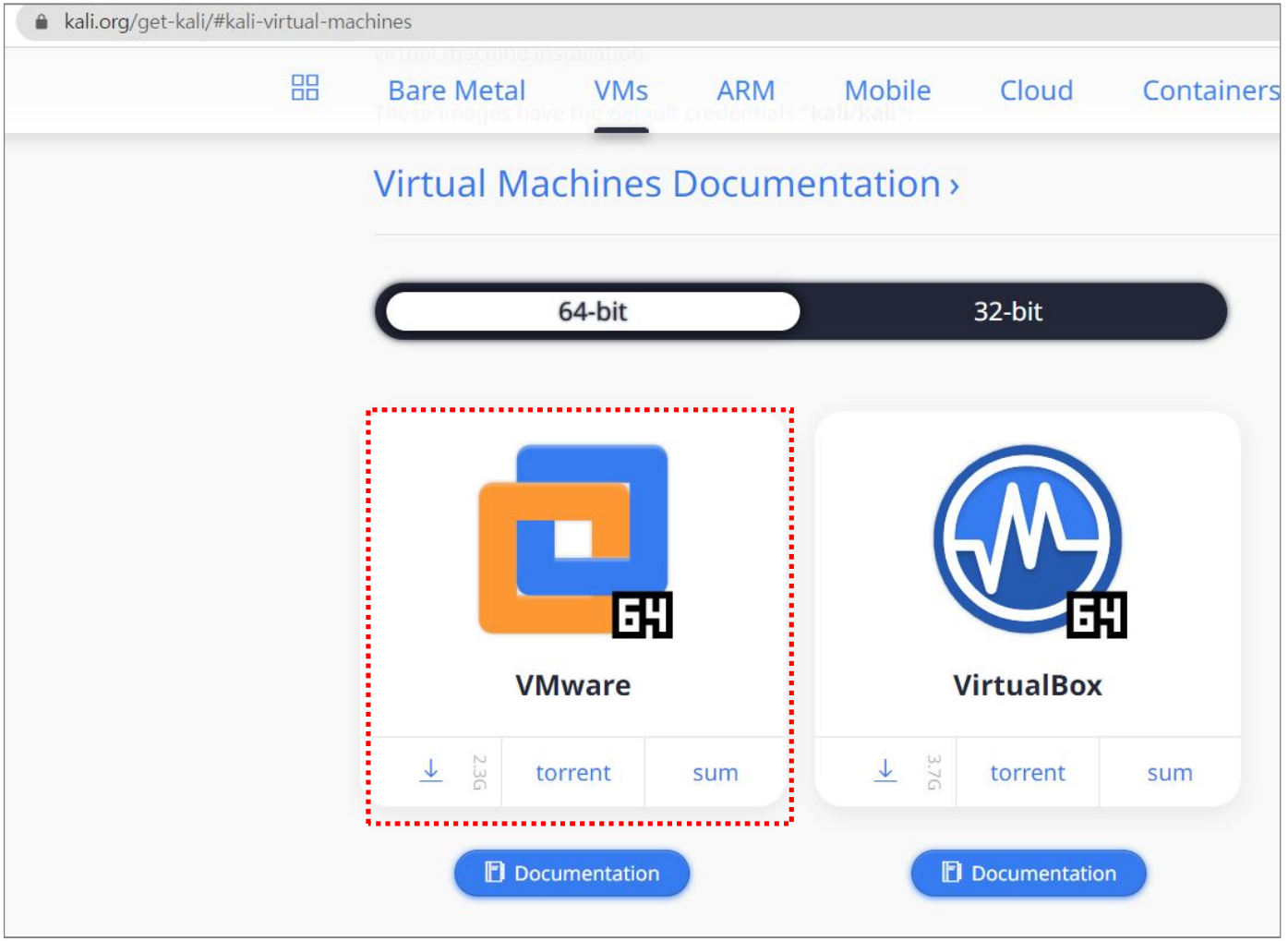
- https://www.vmware.com/kr/products/workstation-pro/workstation-pro-evaluation.html

  ➔ **VMware-workstation-full-17.0.0-XXXX.exe**

다운로드 파일 ❷

Kali Download

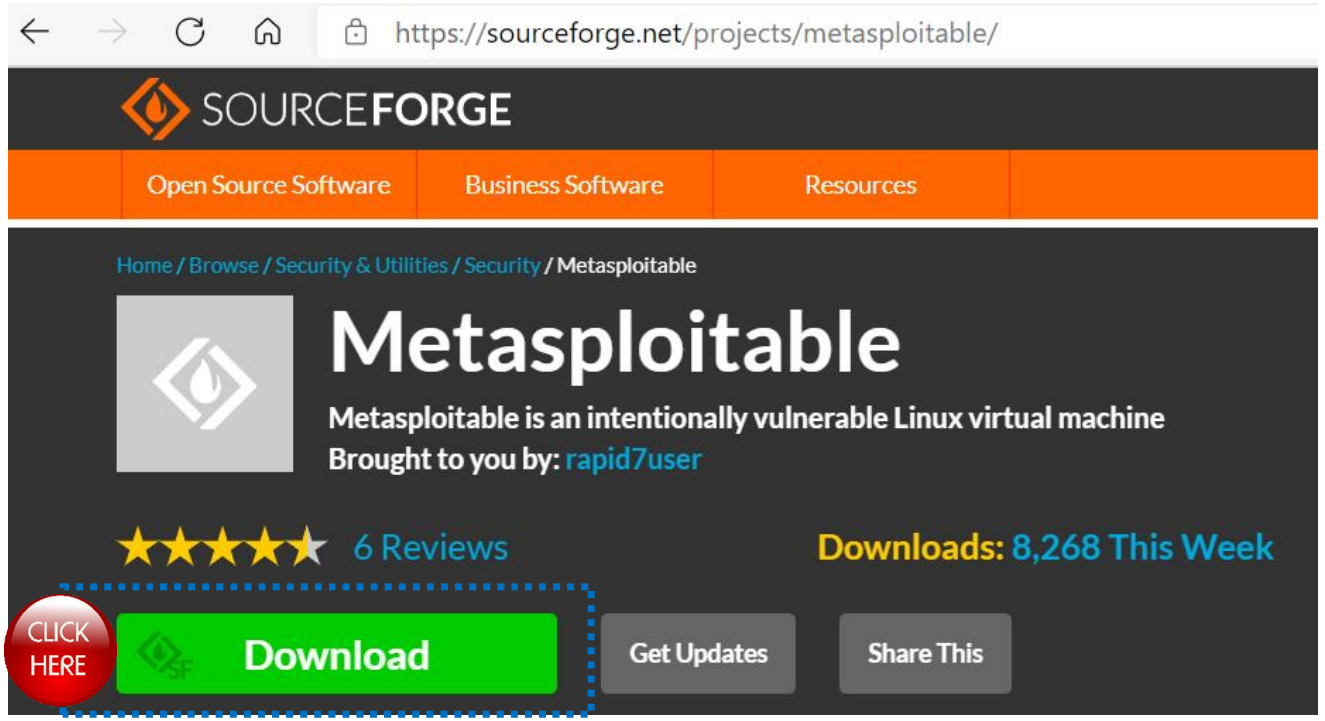
https://www.kali.org/get-kali/#kali-virtual-machines



다운로드 파일 ❸ Metasploitable Download

- https://sourceforge.net/projects/metasploitable

  ➔ **metasploitable-linux-2.0.0.zip**



다운로드 파일 ❹ CentOS7 Download

https://archive.kernel.org/centos-vault/7.0.1406/isos/x86_64/

1) 운영체제 **(OS: Operating System)** 기능

- 컴퓨터 하드웨어와 컴퓨터 사용자 간의 매개체 역할을 하는 시스템 소프트웨어
- 사용자가 프로그램을 수행할 수 있는 환경을 제공

기능	설명
작업관리(Task Manager)	작업의 생성, 실행, 상태 관리, 스케쥴링, 시그널 처리 , 프로세스간 통신
메모리 관리(Memory Manager)	물리메모리와 가상메모리 관리
파일 시스템 관리 (File System Manager)	파일 생성/삭제, 접근제어, 디렉터리 관리, 슈퍼블록 관리
네트워크 관리(Network Manager)	소켓관리, 프로토콜 스택 관리
장치 관리 (Device Manager)	드라이버 관리 서비스

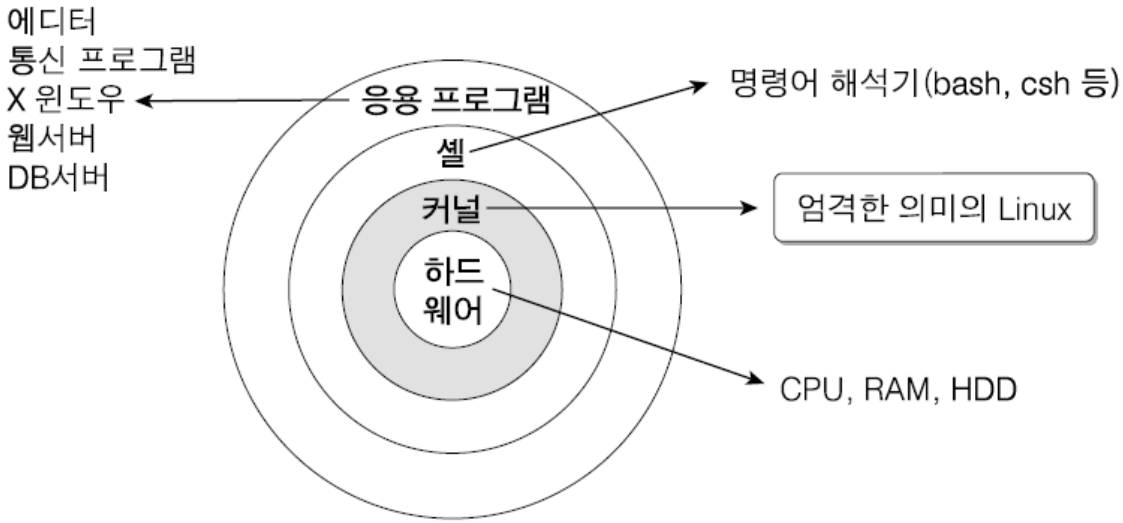
[참고] 운영체제 종류 - 데스크톱 운영체제

- 유닉스(UNIX)
- 유닉스 계열(Unix-like) 운영체제
  - 유닉스라는 이름은 상표권이 설정되어 있어서 해당 이름을 임의로 사용할 수가 없었기 때문에 각 업체들은 독자적인 이름 부여

구분	제품명	개발회사
유닉스 계열	Oracle Solaris	Oracle
	AIX	IBM
	HP-UX	HP
리눅스	Fedora	RedHat
	Ubuntu	Canonical

- 윈도(Windows)
- Mac OS X

2) Linux OS 구성 요소

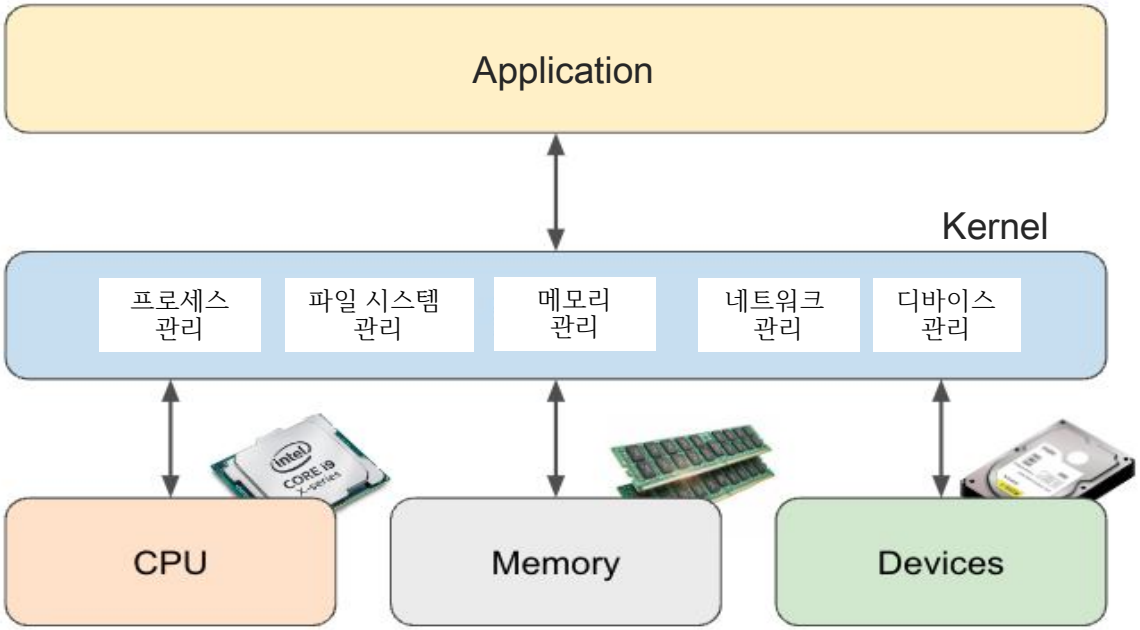


구성요소	기능
커널(kernel)	운영체제의 핵심 역할 프로세스, 메모리, 입출력(I/O), 파일 관리 등을 수행
쉘(shell)	명령어 해석기 사용자 명령의 입출력을 수행하며 프로그램을 실행
파일시스템(file system)	시스템을 관리를 위한 기본 환경 제공 정보를 저장하는 구조 제공

2) Linux OS 구성 요소

❶ Linux Kernel

- 하드웨어와 응용 프로그램간의 다리 역할을 하는 커널(Kernel)을 의미
- 시스템이 부팅 될 때 load 되며 주된 역할은 시스템의 하드웨어 제어
- 메모리, CPU, 디스크, 단말기, 프린터 등 시스템 자원 활용도를 높이기 위한 스케쥴링과 프로그램 관리, 자료 관리 등을 수행

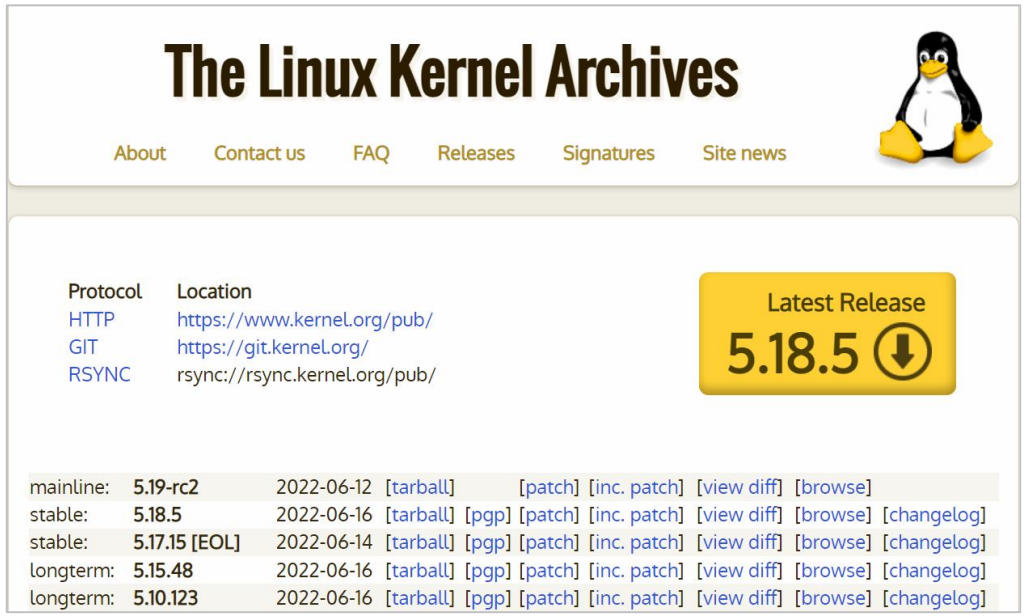


2) Linux OS 구성 요소

❶ Linux Kernel

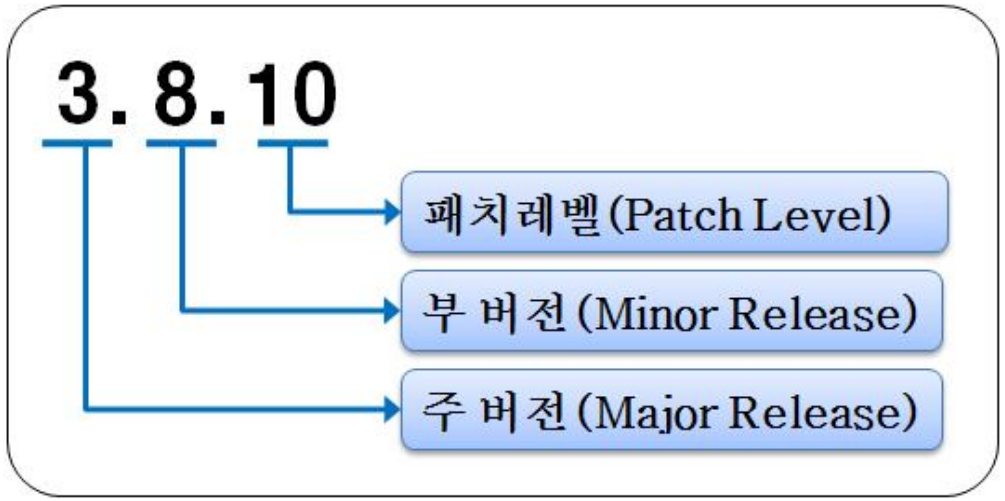
- http://www.kernel.org 에서 최신버전을 무료로 다운로드
- 커널 변천사

커널 버전	0.01	1.0	2.0	2.2	2.4	2.6	3.0	3.8	3.19	4.0	4.6
발표 연도	1991	1994	1996	1999	2001	2003	2011	2013	2015	2015	2016



2) Linux OS 구성 요소

❶ Linux Kernel



<< Kernel 표기 예>>

- 커널 2버전까지는 부번호가 짝수인 경우 안전버전, 홀수인 경우 개발 버전을 의미
- 커널 3버전부터는 구분이 없어지고 순사적으로 저번이 올라가면서 배포
- 배포판에 포함된 기본 커널을 사용자가 직접 최신의 커널로 업그레이드할 수 있음 (커널 업그레이드)

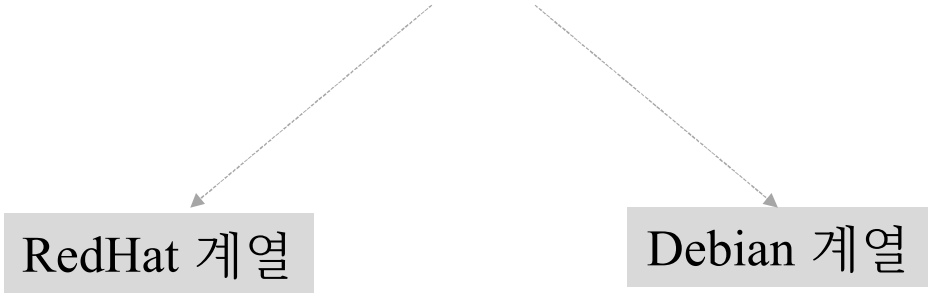
2) Linux OS 구성 요소

❷ Linux Shell

- 사용자 명령어 해석기
  - 사용자가 프롬프트에 입력한 명령을 해석해서 운영체제에 전달
- 셸(Shell)은 커널(Kernel)과 사용자간의 다리역할을 하는 것
- 사용자로부터 명령을 받아 그것을 해석하고 프로그램을 실행하는 역할
- 셸은 사용자가 시스템에 로그인(login)을 하게 되면 각 사용자에게 설정된 셸이 부여되면서 다양한 명령 수행
- 셸을 부여하지 않게 되면 시스템에 로그인하더라도 명령을 수행할 수 없게 되므로 로그인을 막는 효과와 동일

3) Linux 배포판

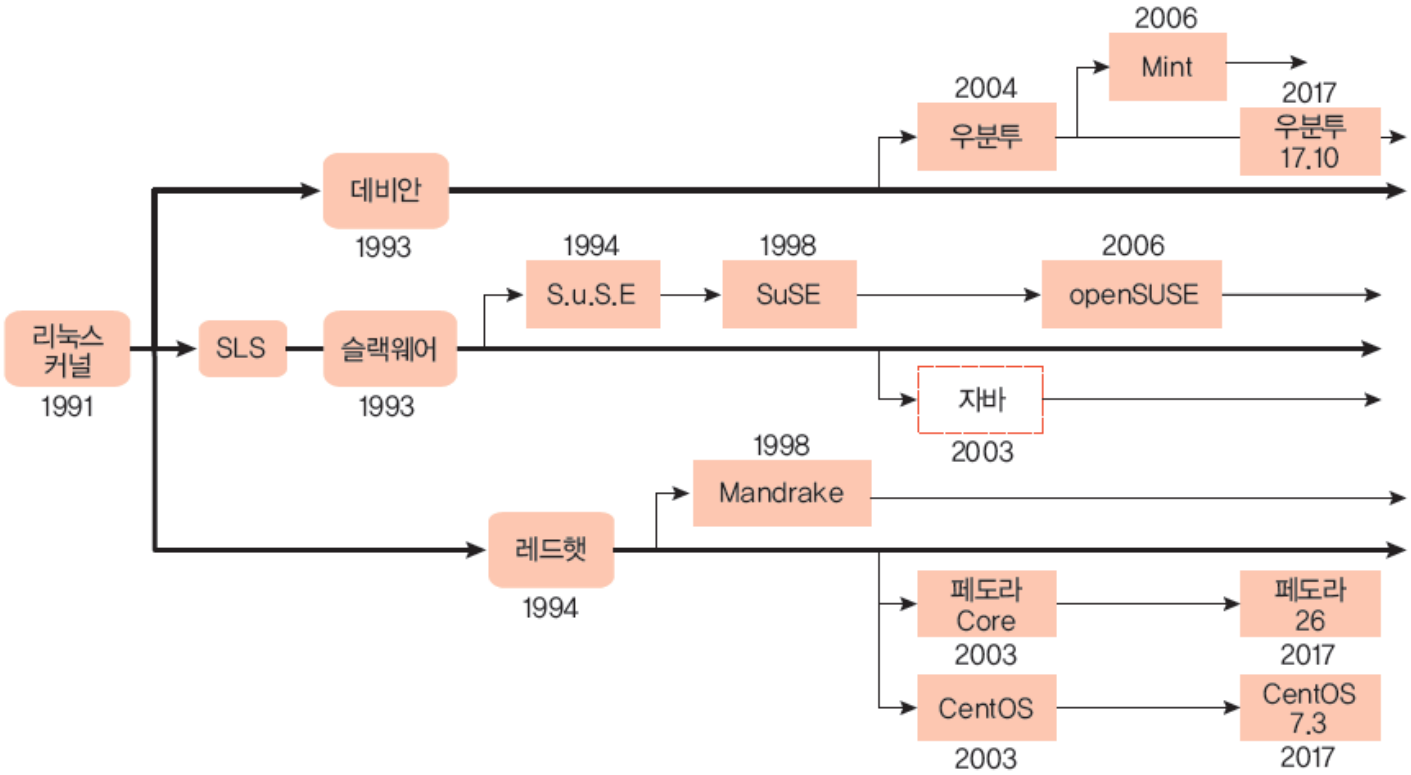
리눅스 배포판 = ‘Kernel + GNU 소프트웨어(shell) + 자유 소프트웨어’



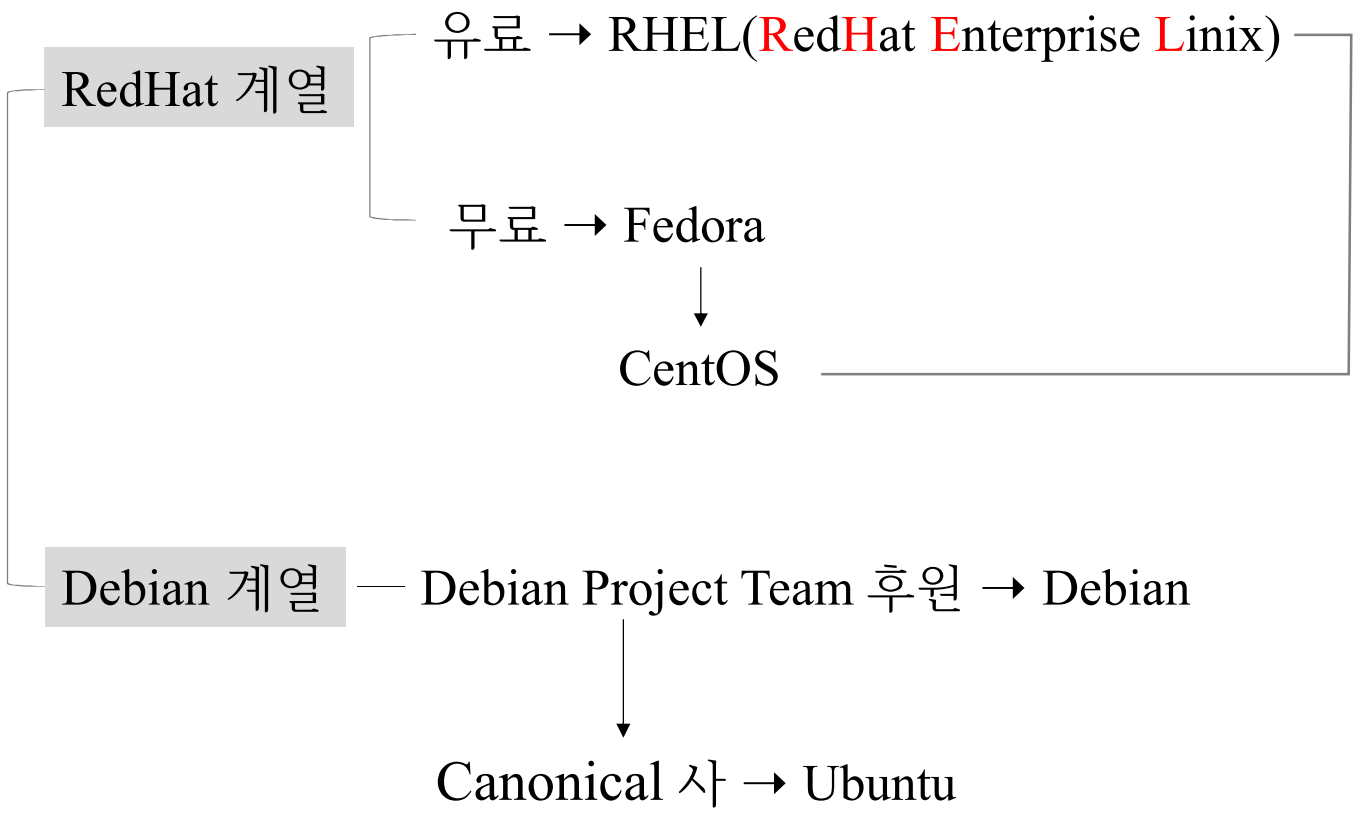
3) Linux 배포판

· 배포판 = 리눅스 커널 + Shell + 응용프로그램

· 전 세계에 300여 가지의 배포판이 있으며, 배포판을 구성하는 소프트웨어도 자유롭게 구성



3) Linux 배포판


RedHat 계열
유료 → RHEL(RedHat Enterprise Linix)
무료 → Fedora
CentOS
Debian 계열
Debian Project Team 후원 → Debian
Canonical 사 → Ubuntu

4) 시스템 보안 주체

- **권한이 없는 (허가받지 않은) 사용자가 파일이나 폴더, 장치 등을 사용하지 못하게 제한하여 시스템을 보호하는 기능**

계정 관리	사용자를 식별하는 가장 기본적인 인증 수단은 아이디와 패스워드로 이를 통한 계정 관리는 시스템 보안의 시작
세션 관리	일정 시간이 지나면 세션을 종료하고 비인가자의 세션 가로채기를 통제하는 것
접근 제어	네트워크 안에서 시스템을 다른 시스템으로부터 적절히 보호할 수 있도록 네트워크 관점에서 접근을 통제하는 것
권한 관리	시스템의 각 사용자가 적절한 권한으로 적절하게 정보 자산에 접근하도록 통제
로그 관리	시스템 내부나 네트워크를 통해 외부에서 시스템에 어떤 영향을 미칠 경우 내용을 기록하여 관리하는 것
취약점 관리	시스템 자체의 결함을 체계적으로 관리하는 것