제 1 장 시스템보안

1. 운영체제

1.1 운영체제 개요

1.1.1 운영체제의 주요 기능

o 핵심가이드
  - 운영체제의 목적 이해
  - 운영체제의 기능 이해
    · 프로그램 수행, 입출력 동작, 파일시스템 조작, 통신, 오류 탐지, 계정관리

(1) 운영체제의 목적

o 운영체제의 목적은 컴퓨터 시스템의 자원(하드웨어 자원, 정보)을 최대한 효율적으로 관리, 운영함으로써 사용자들에게 편의성을 제공하고자 하드웨어와 사용자 프로그램 사이에 존재하는 시스템 프로그램으로 사용자 인터페이스 제공, 성능 향상 등 한정된 자원을 효율적으로 사용하는데 있다. 즉, 신뢰도의 향상, 처리량의 향상, 응답 시간의 단축, 단순한 계산 능력만을 제공하는 하드웨어를 유저가 쉽게 접근할 수 있도록 제공, 제한된 시스템 소스를 효율적으로 통제하고 운영함으로써 보다 높은 성능을 발휘할 수 있도록 지원하는 것이다.
  - 처리 능력 향상 : 단위 시간 내에 최대한 많은 양의 일을 처리할 수 있게 하는 것
  - 응답 시간 단축 : 사용자가 어떤 일의 처리를 컴퓨터 시스템에 의뢰하고 나서 그 결과를 얻을 때까지 소요되는 시간으로, 짧을수록 좋음
  - 신뢰도 향상 : 시스템이 주어진 문제를 어느 정도로 정확하게 해결하는가를 의미
  - 사용 가능도 향상 : 컴퓨터 시스템을 각 사용자가 요구할 때 어느 정도로 신속하게 시스템 자원을 지원해 줄 수 있는가를 나타내는 것

(2) 운영체제의 기능

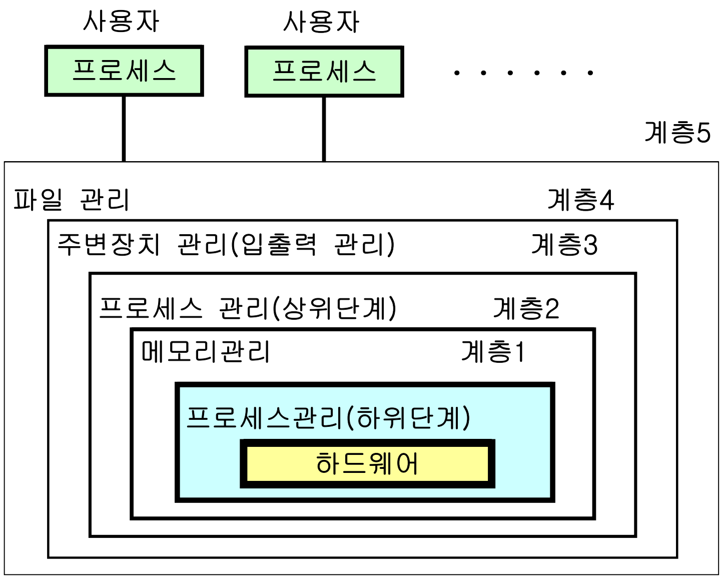
o 운영체제의 기능은 프로그램 생성(Program Creation), 프로그램 실행(Program Execution), 입출력동작(I/O Operation), 파일 시스템 조작, 통신, 오류 발견 및 응답, 자원할당(Resource Allocation), 계정관리(Accounting), 보호(Protection) 등의 기능이 있다.

1.1.2 운영체제의 구조

(1) 커널과 유틸리티

o 핵심가이드
- 운영체제의 계층 구조 및 계층별 특징을 이해
- 시스템 호출에 대한 이해

o 운영체제의 구조는 컴퓨터 시스템 자원관리 계층에 따라 분류하면 일반적으로 5가지 기능을 수행하는 것으로 볼 수 있다.



(그림 1-1) 운영체제의 5계층 구조

- 프로세서 관리(계층1) : 동기화 및 프로세서 스케줄링 담당
- 메모리 관리(계층2) : 메모리의 할당 및 회수 기능을 담당

- 프로세스 관리(계층3) : 프로세스의 생성, 제거, 메시지전달, 시작과 정지 등의 작업
- 주변장치 관리(계층4) : 주변장치의 상태파악과 입출력 장치의 스케줄링
- 파일(정보)관리(계층5) : 파일의 생성과 소멸, 파일의 열기와 닫기, 파일의 유지 및 관리 담당

o 커널은 하드웨어 특성으로부터 프로그램들을 격리시키고, 하드웨어와 직접적으로 상호작동함으로써, 프로그램들에게 일관된 서비스를 제공한다. 커널의 기본 개념은 프로세스와 파일의 관리이다. 그밖에 입출력장치 관리, 메모리 관리 및 시스템호출 인터페이스 등이다. shell이나 유틸리티 또는 응용 프로그램들은 정의된 시스템호출을 통해서 커널과 통신한다. UNIX 계열의 시스템이 부팅될 때 가장 먼저 읽혀지는 운영체제의 핵심부분으로 주기억 장치에 상주하게 되며 프로세스 스케줄링, 기억 장치 관리, 파일 시스템 관리, 운영체제의 고유 기능을 제공한다.

o 시스템 호출(System call)
- 이중모드에서 사용자 모드는 특권 명령어를 사용할 수 없으며 이런 경우에 사용자 프로세스는 운영체제에게 도움을 요청하게 되는데 이를 시스템 호출이라 한다. 즉, 시스템 호출은 실행중인 프로그램과 운영체제 사이에 인터페이스를 제공하는 것이다.

(2) 이중 모드(dual mode) 구조

o 핵심가이드
- 이중모드의 개념 이해
- 일반모드(사용자모드)와 관리모드(모니터모드)의 특징 이해

o 다중 프로그래밍 환경에서는 실행 중인 하나의 프로그램의 오류가 실행 중인 다른 프로그램에게 영향을 줄 수 있으므로 적절한 보호가 필요하다. 이중 모드는 이런 보호 메커니즘 중 하나로서, 두 가지 동작 모드를 제공하여 문제를 일으킬 소지가 있는 명령들을 함부로 실행할 수 없도록 제어한다.
- 사용자 모드 : 사용자 모드의 소프트웨어는 특권이 부여되지 않은 상태로 동작하며 시스템 리소스에 제한적으로만 액세스할 수 있다. 보호 받는 하위 시스템들은 각자가 소유하고 있는 보호 받는 공간에서 실행되며 서로 간섭하지 않는다. 즉, 사용자 모드에서는 제한적인 명령의 사용만 가능하다.
- 모니터 모드 : 커널 모드, 슈퍼바이저 모드라 하며 문제를 일으킬 소지가 있는

명령들은 특권 명령으로 분류하고, 이런 명령들은 모니터 모드에서만 수행되도록 제한한다. 이 모드에서는 모든 명령어 사용이 가능하다.

(3) 프로세스 관리

o 핵심가이드
- 프로세스 관리 이해

o 하드웨어에 의존된 가장 하위 단계 수준으로 프로세스 스케줄링을 통해 실행 가능한 프로세스 추적 관리

(4) 주기억장치 관리

o 핵심가이드
- 주기억장치 관리 이해

o 주기억장치의 접근을 관리, 제어하는 처리 장치의 부분으로 주소 변환, 기억 보호, 버퍼 기억 등의 기능을 수행

(5) 보조기억장치 관리

o 핵심가이드
- 보조기억장치 관리 이해

o 하드디스크나 디스켓 등의 기억장치에 대한 접근 관리, 제어 등을 수행하는 기능

(6) 입출력 시스템 관리

o 핵심가이드
- 장치구동기의 기능 이해
- 인터럽트 방식과 DMA 방식 이해
- 버퍼링과 스풀링 이해

o 컴퓨터의 입출력장치(Input/Output device: I/O장치)는 중앙 시스템과 외부와의 효율적인 통신방법을 제공한다. 입출력장치는 일명 주변장치라고도 하는데, 가장 기본적인 것으로 키보드, 디스플레이장치, 프린터와 보조저장장치인 자기

테이프나 자기 디스크 등이 있다.

o 장치 구동기

- 운영체제와 응용프로그램 및 하드웨어간의 인터페이스를 담당하는 프로그램으로 하드웨어와 운영체제 응용프로그램의 연결 고리가 되는 프로그램으로 하드웨어 구성 요소가 운영체제 아래서 제대로 작동하는데 꼭 필요한 프로그램이며, 장치제어기 또는 드라이버라고 말하기도 한다. 장치 제어기는 명령어를 장치 제어기에 입력하기 위해 하나 이상의 장치 레지스터를 갖고 있는데 장치 구동기는 이들 명령어를 발생시키고 적절하게 수행되는지를 점검하는 기능을 수행한다. 디스크 구동기는 디스크 제어기가 가지고 있는 많은 레지스터의 사용량, 용도를 관리하게 되며 섹터, 트랙, 실린더, 헤드, 암의 움직임, 디스크 인터리브 계수, 모터 구동기, 헤드 설정 시간 등 디스크가 적절하게 작업할 수 있는 모든 기계적인 정보들을 알고 있다.

o 인터럽트와 DMA

- 컴퓨터 시스템에서 사용하는 데이터의 입출력 방식에는 프로그램에 의한 입출력, 인터럽트에 의한 입출력, DMA에 의한 입출력 등이 있다.
- 프로그램에 의한 입출력은 데이터의 입출력 동작이 CPU가 수행하는 프로그램의 I/O 명령에 의해 수행된다. 따라서, 프로그램 제어 하에서 데이터전송을 수행하려면, 입출력을 수행할 준비가 되어있는가를 알기 위해 CPU가 주변장치의 상태를 계속 감시하고 있어야 한다.
- 인터럽트에 의한 입출력은 프로그램에 의한 입출력의 단점을 개선하기 위한 방식이다. 즉 CPU가 계속해서 입출력 상태를 검사하고 있는 것이 아니라 입출력 장치가 데이터를 전송할 준비가 되면 CPU에 인터럽트를 발생시킨다. 따라서 CPU가 다른 프로그램을 수행하고 있는 동안에, 인터페이스가 외부소자를 모니터한다. CPU가 인터럽트 신호를 받으면 프로그램 카운터에 있는 복귀주소를 메모리 스택에 저장한 다음, 입출력 전송을 위한 서비스 루틴으로 제어를 이동한다.
- DMA(Direct Memory Access)는 CPU를 거치지 않고 주변장치와 메모리 사이에 직접 데이터를 전달하도록 제어하는 인터페이스 방식으로서, 고속 주변장치 (M/T, DISK 등)와 컴퓨터간의 데이터 전송에 많이 사용한다.

o 버퍼링과 스풀링

- 버퍼링(Buffering) : 입출력 장치와 보조 기억장치는 기계적 요인 때문에 CPU와 비교할 때 매우 느린 속도로 작동한다. 이와 같은 입출력 장치의 느린 속도를 보완하는 한 가지 방법으로 버퍼링이 있다. 한 레코드가 읽혀 CPU가 그

것에 대한 연산을 시작함과 동시에 입출력 장치가 곧 다음에 필요한 레코드를 미리 읽어서 주기억장치에 저장함으로써 CPU가 필요한 레코드를 기다림이 없도록 하는 것이다. 이때 이와 같이 미리 읽혀진 레코드들이 존재하는 곳은 주기억장치의 일부인데 이를 버퍼라 하고, 이와 같은 일련의 과정을 버퍼링이라 한다.

- 스풀링(Spooling) : 버퍼링은 주기억장치를 버퍼로 사용하는 반면, 스풀링은 디스크를 매우 큰 버퍼처럼 사용하는 것이다. 프로세스들은 입력 또는 출력을 실제 입출력 장치(Physical Device)를 통하지 않고 가상적 입출력 장치(Virtual Device)인 디스크를 매체로 이용한 후, 이 들을 다시 실제의 입력 장치나 출력 장치가 행하도록 한다.

(7) 파일 관리

o 핵심가이드
  - 파일관리 기능 이해
o 운영체제는 프로그램이나 데이터를 파일단위로 관리하며 저장장치에 파일단위로 저장한다. 파일에 대한 조작, 저장방식, 접근방법 등에 대한 관리 수행

(8) 인터럽트

o 핵심가이드
  - 인터럽트 개념 이해
  - 인터럽트 종류 및 특징 이해
o 인터럽트는 시스템에 예기치 않은 상황이 발생하였을 때 그것을 운영체제에 알리고 이를 해결하는 매커니즘이다. CPU는 인터럽트 발생을 알리는 신호를 받으면 프로그램 카운터(Program Counter)의 내용과 프로그램 수행 상태에 관한 모든 정보를 저장한 후에, 문제의 해결을 위한 처리 과정이 기술된 프로그램인 인터럽트 루틴의 시작 주소를 프로그램 카운터로 옮긴다. 그 후 인터럽트 루틴을 수행하여 해당 상황을 처리하고, 인터럽트가 발생하기 이전에 수행하던 프로그램을 계속한다.
o 인터럽트의 종류
  - 입출력 인터럽트(I/O interrupts) -프로세스가 요청한 입출력의 완료등과 관련하여 발생

- 클럭 인터럽트(clock interrupts) - 프로세스의 시간 할당량 종료와 관련하여 발생
- 콘솔 인터럽트(console interrupts) - 콘솔 터미널에서 인터럽트 키(interrupt key)를 누를 때에 발생
- 프로세스간 통신 인터럽트(interprocess communication interrupt) - 임의의 프로세스가 지역 호스트 또는 원격 호스트의 다른 프로세스로 부터 통신 메시지를 받을 경우
- 시스템 호출 인터럽트(system call interrupts, SVC interrupts) - 시스템 호출을 하였을 때 발생
- 프로그램 오류 인터럽트(program check interrupts) - 프로그램의 실행중 논리적인 오류로 인하여 발생
- 하드웨어 검사 인터럽트(machine check interrupt) - 하드웨어 상의 오류가 있을 때 발생

(9) 기타 관련 용어

o 핵심가이드
  - 기타 중요 용어 이해

o 주요 용어 정의
  - 기아현상, 디스패처, 에이징, 유휴상태, 큐잉 등

1.1.3 운영체제의 기술 발전 흐름

o 핵심가이드
  - 운영체제의 기술 발전 흐름 및 기술별 특징 이해
  - 초기 운영체제의 JCL
  - 시분할 운영체제의 타임 슬라이스

(1) 초기 운영체제

o 단순모니터(상주모니터)
  - 프로그래머가 상주 모니터(resident monitor)에게 전달될 정보를 작업 제어 카드(JCL)에 의해 전달하고 상주 모니터는 작업 제어 카드(job control card)에

의하여 지시하는 대로 자동 작업 순서를 제공하게 되며 제어 카드가 하나의 프로그램이 실행될 것이라는 것을 나타내면 상주 모니터는 프로그램을 기억장치에 적재하고 제어를 프로그램으로 전달하며 프로그램이 수행을 완료하면 제어는 모니터로 복귀하게 된다. 모니터는 다음 제어 카드를 읽고 적합한 프로그램을 적재하는 일 등을 수행한다.

(2) 일괄처리와 대화식

o 초기의 컴퓨터는 작업자가 작업 준비 과정에서부터 실행에 이르기까지 직접 관여해야 했다. 테이프를 준비하거나 작업자가 콘솔을 조작하고 있는 동안 CPU는 유휴 상태가 되기 때문에 작업 준비 시간은 커다란 문제가 되었다. 요구사항이 비슷한 작업들을 함께 묶어서 일괄적(Batch)으로 수행함으로써 준비시간 및 작업간의 전이시간을 줄일 수 있게 한 운영체제

(3) 오프라인과 온라인

o 입력의 경우에는 CPU가 직접 카드를 읽기 보다는 카드에 있는 내용을 먼저 테이프에 복사하여 테이프가 차게 되면, 테이프를 컴퓨터로 옮겨 프로그램이 테이프로부터 내용을 읽고 테이프상에 기록한 후 나중에 테이프의 내용을 출력한다. 카드 판독기와 라인 프린터는 주 컴퓨터에 의해 운영되는 것이 아니라 오프라인으로 수행

- 온라인 시스템 : CPU와 주변장치(카드판독기와 라인프린터)가 1:1로 직접 연결됨
- 오프라인 시스템 : CPU와 주변장치가 1:1로 직접 연결되지 않고, 실행시 주변장치(테이프와 디스크)와 연결

(4) 단일 사용자용과 다중 사용자용

o 단일 사용자 운영체제는 한 컴퓨터 시스템에 대해 한 순간에 한 사용자만이 사용하는 시스템. 예로 MS-DOS

o 다중 사용자 운영체제는 동시에 여러 사용자들이 사용할 수 있도록 구성된 시스템. 예로, UNIX, LINUX, 윈도우 2000 계열 등

(5) 다중 프로그래밍 운영체제

o 입출력 장치와 CPU 사이의 속도 차이를 이용하여 CPU를 항상 이용하기 위한 방안으로 주기억장치 내에 2개 이상의 여러 프로그램을 적재하여 그중 하나가 실행될 경우 그 작업은 실행 중에 자기 테이프나 입출력 장치 등의 조작으로 인해 CPU의 유휴시간이 발생하면 운영체제가 다른 작업으로 전환하여 새로운 작업을 수행하므로 CPU의 유휴시간을 줄여 CPU의 이용률을 향상시키는 방법이다.

(6) 시분할 운영체제

o 시분할 운영체제는 다중 프로그래밍 방법의 변형된 형태로서 많은 사용자가 동시에 컴퓨터를 공유하도록 하는 것이다. 시분할 시스템은 아주 짧은 일정시간 동안만 CPU를 사용하고 다음 사용자에게 사용 권한을 전환한다. 그러므로 각 사용자는 자신이 컴퓨터 시스템을 독점하고 있는 것처럼 생각할 수 있다.
o 타임 슬라이스는 실행 프로그램을 연산 처리장치의 할당 시간을 돌아가며 부여받아 동작하는 방식

(7) 분산 운영체제

o 분산처리 시스템은 여러 개의 물리적 처리기들 사이에서 연산을 지역적 또는 기능적으로 분산시켜 처리하고자 하는 것이다. 분산 처리 시스템은 정보의 전송을 위한 통신 네트워크에 의하여 상호 연결된 여러 개의 처리기 사이에 기능적인 분산 및 상호 협동적인 처리를 통하여 연산 속도와 신뢰성을 향상시키고 컴퓨터 자원을 효율적으로 공유하는 시스템이다.

(8) 다중 처리기용 운영체제

o 여러 개의 프로세서(Processor)가 공용 기억장치(Shared Memory)를 통해 제어 및 자원을 공유하면서 수행하는 시스템이다. 이를 위해서 운영체제는 여러 프로세서간의 기억장치 공유를 지원할 방법, 여러 프로세서의 사용을 스케줄링 방법 등이 중요하다.

1.2 운영체제의 주요 구성 기술

1.2.1 프로세스 관리

(1) 프로세스 개념

o 핵심가이드
  - 프로세스 상태 변화 종류 및 특징
  - 프로세스 제어 블록 특징

o 프로세스는 시스템 작업의 기본 단위이며 현재 수행 상태에 있는 프로그램을 의미한다. 예를 들면 수행중인 응용프로그램, 운영체제의 일부인 CPU 스케줄러 등이 프로세스가 될 수 있다.

o 하나의 프로세스는 생성되어 완료될 때까지 상태변화를 거치게 된다.
  - 생성(New) : 프로세스가 생성되었지만 아직 운영체제에 의해서 실행 가능한 프로세스 집합에 들어가지 못한 상태
  - 실행(Running) : 현재 CPU를 차지하여 실행중인 상태
  - 준비(Ready) : 프로세스가 실행되고 있지 않지만 즉시 CPU를 사용할 수 있는 상태로 대기하고 있는 상태
  - 대기(Block) : 어떤 사건이 발생하기 전까지는 실행될 수 없는 상태
  - 보류(Hold) : 프로세스가 디스크 등에 보관되어 있는 상태
  - 교착(Deadlock) : 프로세서가 결코 일어날 수 없는 사건을 기다리는 상태
  - 종료(Exit) : 운영체제에 의해서 실행 가능한 프로세스 집합으로부터 해제된 상태

o 프로세스 제어 블록
  - 프로세스는 프로세스 제어블록(PCB)으로 나타내며 운영체제가 프로세스에 대한 중요한 정보를 저장해 놓은 저장소를 의미한다. 운영체제가 제어를 다른 프로세스에 넘겨줄 때 현재 실행중인 프로세스의 정보를 해당 PCB에 저장한 후 제어를 넘겨주게 된다. 제어가 다시 프로세스에게 넘겨질 경우 운영체제는 PCB에 있는 정보를 이용해서 실행을 한다.

(2) 병행 처리와 프로세스

o 핵심가이드

- 프로세스 생성과 종료
- 프로세스들간의 관계
- 쓰레드(thread)와 태스크(task) 개념

o 프로세스를 생성하는 데 필요한 작업
- 프로세스 이름을 결정
- 프로세스 리스트에 생성된 프로세스를 추가
- 생성된 프로세스에 초기 우선 순위를 부여
- 생성된 프로세스에 PCB를 생성
- 생성된 프로세스에 초기 자원 할당

o 쓰레드
- 프로세스가 논리적으로 운영체제가 해야 하는 작업을 의미한다면, 스레드는 그 작업을 성취하는데 필요한 가능한 많은 하위 작업 중의 하나이며 하나의 프로세스는 하나의 쓰레드로 구성될 수도 있고 여러 개의 쓰레드로 구성될 수도 있다. 따라서 프로세스보다는 작은 단위이며 자원의 할당에는 관계하지 않고, 프로세서 스케줄링의 단위로서 사용하게 된다.

o 태스크
- 태스크는 자원 할당의 단위로 정의될 수 있으며 프로세스와 같은 개념으로 이해할 수 있다. 즉, 쓰레드는 프로세스처럼 독립된 주소공간을 가질 수 없고, 프로세스처럼 독립적으로 자원 할당을 요청할 수 없다.

(3) 프로세스 스케줄링

o 핵심가이드
- 다중 프로그래밍과 스케줄링 개념 및 특징
- 프로세스 큐 개념
- 스와핑(swapping) 개념

o 프로세스 스케줄링이란 멀티 프로세스 시스템 내에 존재하는 여러 개의 프로세스 중 어떤 프로세스에게 CPU 사용권을 넘겨줄 것인가를 결정하는 일이다. 멀티 프로세스 시스템에서는 생성된 프로세스는 일단 준비상태로 넘어가게 되고 준비 상태에서는 여러 개의 프로세스가 실행되기를 기다리고 있는 상태를 운영체제가 이들을 큐에 보관하고 관리(대기 큐)하면서 CPU가 사용 가능해 지게 되면 운영체제는 대기 큐에서 기다리고 있던 몇 개의 프로세스 중 한 프로세스에게 CPU 사용권을 넘겨준다. 이와 같이 어떤 기준을 가지고 이 기준에 입각해서

프로세스의 실행순서를 결정하는 일을 프로세스 스케줄링이라 한다.

o 스케줄링 큐 (Scheduling Queue)는 다음과 같은 상태로 구분한다.

- 준비큐(ready queue)
  - ㆍ주기억 장치에 적재되어 있으면서 CPU에 의해 실행되기를 준비하는 프로세스들로 구성된 리스트
  - ㆍ첫 번째와 마지막 PCB(프로세스 제어블록)를 가리키는 큐 헤더와 각 프로세스의 정보와 다음 프로세스의 PCB를 가리키는 포인터 필드를 포함한 PCB로 구성
- 작업큐(job queue)
  - ㆍ주기억장치의 할당을 기다리며 대용량의 기억장치에 있는 프로세스들로 구성된 리스트
- 장치큐(device queue)
  - ㆍ특정한 입출력 장치를 기다리고 있는 프로세스로 구성된 리스트

o 스와핑(swapping) :

- 프로세스 스케줄링은 준비 완료(Ready) 상태에 있는 프로세스들 중 어느 것을 CPU에 할당시킬 것인가를 결정하는 문제를 취급하는 것으로서, CPU 효율 및 처리량(Throughput)의 최대화와 반환 시간(Turnaround Time)의 최소화에 그 목적을 두고 있다.
  - ㆍ장기 스케줄러(또는 작업 스케줄러) : 저장소(큐)에서 프로세스들을 선택하여 실행하기 위해 기억장치로 적재한다.
  - ㆍ단기 스케줄러(또는 CPU스케줄러) : 실행 준비가 되어 있는 프로세스 중에서 선택하여 이들 중 하나에게 CPU를 할당하는 것이다.
  - ㆍ중기 스케줄링 : 기억장치에서 프로세스들을 제거하여 다중 프로그래밍의 정도를 완화하는 것이 바람직할 때가 있다는 것에서 유래한 것으로 프로세스는 중기 스케줄러에 의하여 교체되어 나가고 후에 다시 교체되어 들어온다.
- 중기 스케줄러의 아이디어는 메모리에서 프로세스들을 제거하고 따라서 다중 프로그래밍의 정도를 완화하는 것이 종종 바람직할 수 있다는 것이다. 차후에 다시 프로세스를 메모리로 불러와서 중단되었던 지점으로부터 실행을 재개하는 기법을 스와핑이라 한다.

(4) 스케줄링 알고리즘 기술

o 핵심가이드

- 사용되는 기준
- 선업 선처리(FCFS, FIFO), 최소작업(SJF, short-job-first), 최소잔여시간(SRT, shortest remaining time), 우선순위(priority), 순환 할당(RR, round-robin), 다단계 큐(multi-level queue), 다중 프로세서 스케줄링 이해

o 스케줄링 기준

- CPU 이용률(CPU utilization)
  - ･프로세스들이 CPU를 사용하는 비율로 실제로는 CPU가 쉬는 시간을 측정하여 그 시간을 제외한 나머지 시간을 사용한다.
- 시스템 처리율(Throughput)
  - ･단위시간당 완료된 프로세스의 개수
- 반환시간(Turnaround time)
  - ･프로세스들이 시스템에 들어간 시간과 마친 시간의 차이를 말하며 출력장치의 속도에 제한을 받는다.
- 대기시간(Waiting time)
  - ･프로세스가 준비 큐에서 대기하는 시간으로 큐의 길이에 의해 측정될 수 있다.
- 응답시간(Response time)
  - ･프로세스의 요구한 시간으로부터 첫 번째 응답이 나올 때까지의 시간

o 스케줄링 방법 분류

- 선점/비선점(preemptive. non-preemptive) 스케줄링
  - ･비선점 : 프로세스에게 할당된 프로세서를 빼앗을 수 없는 방식(선입선출(FIFO), FCFS, 기한부 스케줄링, SJF)
  - ･선점 : 현재 프로세스로부터 프로세서를 빼앗을 수 있는 방식으로 높은 우선순위의 프로세스로부터 긴급 처리 요구에 유용하며, 특히 실시간 프로세스, 대화식 시분할 시스템에서 빠른 응답이 가능하다.(순환 할당 스케줄링)
- 우선순위 스케줄링
  - ･프로세스에 부여된 우선순위대로 처리하는 방식으로 우선순위는 프로세스의 특성 및 종류에 따라 시스템에 의해 자동 부여되거나 외부적으로 부여 가능하다.
- 기한부(deadline) 스케줄링
  - ･작업들이 명시된 시간 내에 완료되도록 계획하는 방식으로 실시간 시스템과 같은 제한된 응답시간 요구 분야에 유용하다.

o 선입선출(FIFO) 스케줄링

- 가장 간단한 스케줄링 기법으로서 프로세스들은 대기 큐에 도착한 순서대로 적재되어 차례로 CPU를 할당받는다. 중요하지 않은 작업이 중요한 작업을 기다리게 할 수 있으며 대화식 시스템에는 부적합하다.

o 최소 작업 우선(SJF) 스케줄링

- 프로세스들의 CPU 사용시간을 비교하여 가장 작은 CPU 사용시간을 가진 프로세스에게 CPU를 할당하는 방법이다. 평균 대기 시간을 줄일 수 있는 장점이 있으나 빠른 응답 시간을 제공해야 하는 대화식 시분할 시스템에는 부적합하다. 이 방식은 선점 방식과 비선점 방식 모두 사용할 수 있다.

o 우선 순위(Priority) 스케줄링

- 우선 순위 스케줄링 알고리즘은 각 프로세스에게 우선 순위를 부여하여, CPU를 최고의 우선 순위를 가진 프로세스에게 할당하는 방법이다. 시간 제한, 메모리 요구, 프로세스의 중요성 등을 기준으로 우선 순위를 결정하게 되며 무한 정지되거나 기아 상태가 될 수 있는 문제가 있으나 기아 상태는 오랫동안 시스템에서 대기하는 프로세스들의 우선 순위를 점진적으로 증가시키는 에이징(Aging)기법을 사용하여 해결할 수 있다.

o 순환 할당(Round-Robin) 스케줄링

- 시분할 시스템에서 특히 많이 사용되는 방법으로 일정한 시간량 동안 한 프로세스에게 CPU를 할당한 후 준비 큐의 다음 프로세스에게 CPU를 다시 할당한다. 시스템이 사용자에게 적합한 응답 시간을 제공해 주어야 하는 대화식 시분할시스템에 적합하다.

o 다단계 귀환(Multilevel Feedback) 스케줄링

- 다단계 귀환 스케줄링 알고리즘은 큐들 사이를 프로세스가 이동한다. 어떤 프로세스가 CPU시간을 많이 사용하면 낮은 순위의 큐로 이동하고 낮은 우선순위의 큐에서 오래 대기한 프로세스는 높은 우선 순위의 큐로 이동한다. 짧은 작업에 우선권을 주게되며 입출력 장치의 효율적인 이용을 위해 입출력 위주의 작업에 우선권을 준다.

(5) 프로세스간 협조

o 핵심가이드

- 생산자-소비자 모델
- 경쟁조건(race condition)

- 임계영역(critical section) 문제
- 동기화 하드웨어(test-and-set)
- 세마포(semaphore)
- 프로세스간 통신(IPC)

o 생산자와 소비자 문제(Producer and Consumer)

- 두 개의 프로세스는 하나의 고정된 크기의 버퍼를 공유하는 상태에서 하나의 프로세스는 그 버퍼에 정보를 써넣는 생산자이고, 또 다른 프로세스는 버퍼에 있는 정보를 꺼내어 사용하는 소비자 프로세스이다. 이들이 정확하게 같은 속도로 진행된다면 별문제가 없겠지만 이 둘의 속도가 다를 때 문제가 발생하게 된다. 즉, 버퍼가 비어있는데 소비자 프로세스가 버퍼에서 데이터를 읽어가려 하는 경우 또는 버퍼가 가득 차있는데 생산자 프로세스가 버퍼에 데이터를 써넣으려 하는 경우가 문제가 발생한다.

o 임계영역 문제

- 임계영역(critical section) : 하나의 프로세스가 공유 자원을 변경하는 코드를 실행하고 있을 때, 그 프로세스는 임계영역에 있다고 한다. 어떤 프로세스가 임계 영역에 있을 때 다른 프로세스는 임계 영역 내에 들어가지 못한다. 또한 조건부 임계 영역이란 임계 영역 내에 들어가려는 프로세스가 있을 경우 주어진 조건에 만족할 때에만 임계 영역안으로 들어갈 수 있도록 하는 기법
- 임계 구역 문제 해결을 위한 3가지 조건
  · 상호배제
  · 진행(progress): 임계구역에 들어가려고 하는 프로세스들만이 순서 결정에 참여
  · 한계대기(bounded waiting): 무한정 대기해서는 안된다

o 프로세스간 통신

- 운영체제가 프로세스 간의 통신을 위해 제공하는 방법은 크게 두 가지가 있다.
  · 공유 메모리 방식 : 어떤 변수들을 공유함으로써 프로세스들간의 통신이 이루어지는 기법으로 프로세스들은 공유변수를 통해 정보를 교환하며 운영체제는 공유메모리만 제공한다. 프로그래머는 공유메모리를 통해 통신기능을 구현할 수 있다.
  · 메시지 시스템 방식 : 프로세스들이 메시지를 교환하도록 허용하는 기법이다.

(6) 교착 상태(Deadlock)

o 핵심가이드
- 교착상태(deadlock) 발생 조건
- 자원할당 그래프
- 교착상태의 예방, 회피, 탐지, 회복

o 다중 프로그래밍 시스템에서 아무리 기다려도 결코 일어나지 않을 사건을 기다리고 있는 프로세스를 교착 상태(deadlock)에 빠져있다고 한다. 교착 상태란 다중 프로그래밍 시스템 하에서 서로 다른 프로세스가 일어날 수 없는 사건을 무한정 기다리며 더 이상 진행되지 못하는 상태를 말한다. 각 프로세스는 상대 프로세스가 사용하는 자원을 놓아줄 것을 기다리면서 자신이 가진 자원은 놓아주지 않음으로써 서로 상대방의 자원을 기다리는 상태가 된다. 이러한 상태를 환형 대기(circular wait)라고 하며 교착 상태의 한 예이다.

o 교착상태의 4가지 발생 조건
- 상호배제(Mutual Exclusion)
  · 프로세스들이 각각 필요 자원에 대해 배타적 통제권을 요구할 때
- 점유와 대기(Wait)
  · 프로세스가 다른 자원을 요구하면서 자신에게 할당된 자원을 해제하지 않을 때
- 비중단 조건(Non-preemption)
  · 프로세스에 할당된 자원을 끝날 때까지 해제할 수 없을 때
- 환형 대기 조건(Circular Wait)
  · 프로세스들이 순환을 이루어서 존재하여야 하며, 이를 구성하는 각 프로세스는 순환 내의 이전 프로세스가 요청하는 자원을 점유하고 다음 프로세스가 점유하고 있는 자원을 요구

o 교착 상태 해결 방안
- 교착 상태 예방 : 교착 상태의 필요 조건을 부정함으로써 교착 상태가 발생하지 않도록 미리 예방하는 방법
- 교착 상태 회피 : 교착 상태 가능성을 배제하지 않고 적절하게 피해나가는 방법
- 교착 상태 탐지 : 교착상태 발생을 허용하고, 발생시 원인을 규명하여 해결하는 방법
- 교착 상태 복구 : 교착 상태 발견 후 환형 대기를 배제시키거나 자원을 중단

시켜 해결하는 방법

1.2.2 기억장치 관리

(1) 계층적 기억장치 구조

o 핵심가이드
- 계층적 기억장치 구조 이해

o 주 기억 장치의 구성과 관리는 운영체제에 가장 중요한 영향을 미친다. 모든 컴퓨터는 계층적인 기억 장치를 가진다. 크게 주 기억 장치와 보조 기억 장치로 나눌 수 있다. 모든 프로그램은 주 기억 장치에 탑재되어야만 실행이 가능하다. CPU가 주 기억 장치의 프로그램을 가져와서 실행하기 때문이다. 주 기억 장치는 비교적 비싼 자원이며 소량의 자료를 임시로 기억할 수 있고 영구히 저장할 수는 없다. 이러한 주 기억 장치 용량의 한계는 주 기억 장치 관리를 필요로 하게 되었다. 프로그램 중에서 현재 실행되지 않는 부분은 보조 기억 장치에 두는 개념이 요구된다. 이러한 요구는 기억 장치를 계층적으로 구성할 필요성이 대두되게 되었다. 계층적인 기억장치의 구성은 주 기억 장치보다 훨씬 빠른 기억 장치를 요구하게 되었는데 이것은 CPU 내에 존재하게 된다. 이것을 캐시(cache) 기억 장치라고 한다. 캐시 기억장치는 시스템에서 왕복 작업의 수준을 하나 더 증가시킨다. 주기억 장치에 있는 프로그램을 실행하기 전에 고속의 캐시 기억 장치로 프로그램을 적재함으로써 보다 빠르게 프로그램을 실행할 수 있다

(2) 메모리 할당 기법

o 핵심가이드
- 최초 적격(first-fit)
- 최상 적격(best-fit)
- 최악 적격(worst-fit)

o 메모리 할당 기법은 기억장소에 프로그램이나 데이터가 들어올 경우 기억장소의 위치를 결정하는 기법
- 최적 적합 (Best Fit) : 입력된 프로그램을 수용할 수 있는 공간 중 가장 작은 공간을 할당함
- 최초 적합 (First Fit) : 입력된 프로그램을 수용할 수 있는 공간 중 가장 먼저

발견된 공간을 할당함

- 최악 적합 (Worst Fit) : 입력된 프로그램을 수용할 수 있는 공간 중 가장 큰 공간을 할당함

(3) 메모리 단편화 문제

o 핵심가이드

- 단편화의 원인
- 압축을 통한 단편화 제거

o 단편화는 기억장치 관리에서 각 작업에 필요한 기억장치 공간들을 계속적으로 할당 및 회수를 반복할 때, 주 기억장치 중에서 실제로 작업에 사용되지는 않으면서 유용하게 사용될 수도 없는 공간을 의미한다. 예로, 100 바이트를 요청하여 데이터를 저장하려고 하는데 128 바이트의 공간(4블럭*32바이트/블럭의 경우)이 할당된다. 결국, 메모리에서 28바이트는 사용하지 않게 되는 것인데 이를 메모리 단편화라 한다. 좀더 세부적으로 이렇게 블록 내부에서 생기는 단편화를 내부 단편화라 한다. 또한 외부 단편화도 있는데 간단하게 정의하면 내부 단편화는 하나의 분할에 작업을 할당하고 남은 빈 공간이고 외부 단편화는 대기 중인 작업이 분할영역보다 커서 분할 전체가 빈 공간으로 있을 때의 상태를 말한다.

o 압축(Compaction)은 산재한 기억장소를 한 군데로 모아 최대의 연속된 빈 공간을 확보하는 것을 말한다. 기억장치 내에 흩어져 있는 공백들이 상당한 양의 메모리를 차지하고 있는 경우가 있다. 때때로 하나의 작업이 일정 양의 기억 장치를 요청할 때, 모든 공백의 합은 그 작업이 요구하는 기억 장치 보다 클지라도 각 공백은 그 작업을 수용할 만큼 크지 않은 경우가 있다. 메모리 압축은 사용되고 있는 기억 장치의 공간을 주 기억 장치의 한쪽 끝으로 옮기는 것이다. 이렇게 하면 가변 분할 기법에서 발생하는 수많은 작은 공백들 대신 하나의 커다란 공백이 남게 된다. 그러므로 모든 이용 가능한 메모리는 연속해 있으므로 대기 중인 작업이 저장 장치의 압축으로 생긴 하나의 공백보다 작으면 그 작업을 실행할 수 있다.

o 단편화의 문제를 해결하는 또 다른 방법으로는 페이징과 세그먼테이션이 있다.

(4) 페이지 기법

o 핵심가이드

- 페이징의 개념 이해
- 페이징 하드웨어와 테이블, 공유 페이지 이해
- 메모리 교체(swapping), 메모리 보호(protection)

o 페이지 개념이 나타나기 전까지는 한 프로그램이 연속적으로 적재되어야 수행 가능하다고 생각했으나 외부 단편화 문제의 궁극적인 해결책이 필요하게 되었다. 페이징이란 주소공간을 페이지 단위로 나누고, 실제 주소공간은 페이지 크기와 같은 페이지 프레임(Page Frame)으로 나누어 사용하는 것이다.

o 페이징 테이블은 논리적 주소 공간으로부터 물리적 기억장치로의 주소변환을 위해서 페이지 테이블이 필요

o 페이지 하드웨어 : 페이징을 수행하기 위해 필요한 하드웨어의 지원

- 명령어를 수행하기 위해 필요한 주소(명령어 주소, 데이타 주소)는 페이지 번호와 페이지 옵셋으로 표현

o 페이지 공유는 시스템에서 여러 사용자가 동일한 프로그램을 수행하는 경우에 중복된 데이터를 여러 개 가지는 문제를 해결하기 위해서 공유가 필요하다.

(5) 세그먼테이션 기법

o 핵심가이드

- 세그먼테이션 하드웨어
- 세그먼트 테이블
- 세그먼트 페이징 기법

o 일반적으로 사용자가 작성하여 실행하는 프로그램은 서브루틴과 함수, 프로시져 또는 모듈의 집합으로 구성되어 있고, 아울러 각종 테이블, 행렬 또는 스택 등과 같은 여러 가지 형태의 자료 구조들이 있다. 이때 이러한 논리적 단위가 되는 프로그램 모듈이나 자료 구조 등을 세그먼트(Segment)라 한다.

o 세그먼트는 세그먼트 번호와 세그먼트 오프셋으로 구성된 주소를 사용하는데 사용자가 사용하는 주소와 물리적 주소간의 변환을 책임질 하드웨어의 지원이 필요하게 되고 세그먼트 테이블을 이용하여 주소 변환을 한다.

(6) 가상기억장치(virtual memory)

o 핵심가이드

- 가상 기억장치의 개요 및 특징
- 요구 페이징 기법
- 페이지 교체(replacement) 알고리즘
  · 선입선출(FIFO), 최적 페이지 교체(optimal), LRU, LRU 근접, 기타 알고리즘
- 다중 프로그래밍과 스래쉬(thrashing)
- 작업 설정(work set) 모델

o 가상기억장치는 시스템에 설치된 물리적 기억장치의 효율적 사용을 위해 사용자에게서 물리적 기억장치를 숨기고 논리적으로 확장된 기억장치를 제공하는 기법으로 물리적 기억장치와 논리적 기억장치 사이의 대응관계를 관리 및 유지하는 시스템 구조와 운영체제의 협력관계가 수행되어야 한다.

o 요구 페이징
- 실행할 프로그램 일부만 메모리에 적재하는 것으로 프로그램이 순차적으로 실행되는 특성과 프로그램 일부가 자주 사용될 때 다른 부분은 거의 활용하지 않는 점을 이용하여 요구페이징 기법에서 프로그램의 일부만을 메모리에 적재하여 실행할 수 있게 함으로써 프로그램의 최대 크기에 대한 제한이 사라지게 된다.

o 페이징 교체 알고리즘
- 선입선출(FIFO: First-In-First-Out) 알고리즘
  · 주기억장치에서 가장 많은 시간을 보낸 페이지부터 교체하는 알고리즘으로 페이지들의 주기억장치 적재 순서를 기록하여 선입선출 큐를 유지 관리
- 최근 최소 사용(LRU: Least Recently Used) 알고리즘
  · 가장 오랜 기간 사용되지 않았던 페이지를 교체하는 알고리즘으로 일반적으로 선입선출 알고리즘보다 적은 페이지 부재율을 나타낸다.
- 최적교체(OPT: optimal) 알고리즘
  · 가장 오랫동안 참조되지 않을 페이지를 희생 페이지로 선택하는 방식
- 클럭(clock) 알고리즘
  · 선입선출 알고리즘과 최근 최소 사용 알고리즘을 결합한 방식으로 각 상주 페이지와 연관된 참조 비트가 해당 페이지가 참조될 때마다 세트되고 주기적으로 소거되는 방식으로 참조비트가 소거된 페이지는 해당 페이지가 최근에 참조되지 않았음을 나타냄

o 스래쉬(thrashing)
- 스래쉬은 전역 페이지 교체 알고리즘 시스템에서 물리적 기억장치가 한계에

도달했을 때 새로운 프로세스가 실행을 요청하게 되고 기억장치 관리자는 교체 알고리즘을 통해 희생 페이지를 선택해 새 프로세스에 할당되고 할당된 페이지들은 모두 사용되던 것이기 때문에 페이지 부재율 증가를 처리하기 위해서 CPU의 활용도가 저하하면 다시 새로운 프로세스를 실행하게 됨으로써 CPU의 활용도를 떨어뜨리는 것이다.

- 방지기법
  - ㆍ프로세스에게 필요한 만큼의 페이지 프레임 할당함으로써 방지
  - ㆍ작업설정(work set) 기법을 통해 프로세스가 필요로 하는 프레임의 수를 파악

(7) 디스크와 디스크 스케줄링

o 핵심가이드
- 디스크의 구조
- 가용 공간 관리 기법
- 할당 방법 : 연속할당, 연결할당, 색인할당
- 디스크 스케줄링 알고리즘
  - ㆍ선입선처리(FIFO) 스케줄링
  - ㆍ최소 탐색 우선(SSTF) 스케줄링
  - ㆍ스캔(SCAN) 스케줄링
  - ㆍLOOK 스케줄링 등

o 디스크 공간 할당 기법
- 연속 할당 : 연속 공간이 없으면 파일은 생성될 수 없다.
- 연결 할당 : 각 파일에 할당된 블록들이 여러 곳에 흩어지게 적재하여 연결 리스트로 관리하는 기법. (섹터 지향, 블록 할당, 블록 연결 할당)
- 인덱스 할당

o 디스크 스케줄링 기법
- 디스크 스케줄링은 다수의 사용자가 서로 다른 작업을 처리하기 위해서 디스크의 입출력을 요구할 때 좀 더 효율적으로 요청을 처리하기 위한 기법이다. 대부분의 사용자 작업은 디스크에 입출력을 필요로 하기 때문에 효율적이며 빠른 디스크 액세스 기법이 필요하다. 운영 체제는 빠른 디스크 액세스 기법을 제공하기 위하여 디스크 스케줄링을 한다.
  - ㆍFCFS 기법 : 입출력 요청 대기 큐에 들어온 순서대로 서비스를 하는 방법.

(선입 선처리)

· SSTF 기법 : 탐색 거리가 가장 짧은 요청이 먼저 서비스를 받는 기법.(최소 탐색 우선)

· SCAN 기법 : SSTF와 같은 동작을 하지만, 진행 방향상의 가장 짧은 거리에 있는 요청이 먼저 서비스를 받는다.

· C-SCAN 기법 : 헤드가 항상 바깥쪽 실린더에서 안쪽 실린더로 이동하면서 가장 짧은 탐색 시간을 갖는 요청을 서비스하는 방법.

1.2.3 파일 시스템 관리

(1) 파일과 디렉토리

o 핵심가이드

- 파일 조작 : 생성, 기록, 판독, 재설정, 삭제 등

o 파일

- 서로 연관성이 있는 데이터의 집단을 파일(file)이라고 하며 파일은 각기 이름이 있고, 보통 디스크나 테이프 등의 보조 기억 장치에 저장된다.

o 파일의 구조

- 파일의 구조란 파일을 구성하는 레코드들이 보조 기억 장치 내에 배치되는 방식을 말한다.
- 순차 파일(sequential file)
  · 레코드들은 물리적인 순서에 따라 저장된다. 즉, 다음 레코드는 현재의 레코드 바로 뒤에 저장되어 있는 레코드를 의미한다. 이러한 구조를 가진 매체에는 자기 테이프, 종이 테이프, 천공 카드 및 프린터 출력 등이 있다.
- 인덱스된 순차 파일(indexed sequential file)
  · 레코드는 각 레코드의 키 값에 따라 논리적인 순서대로 배열되어 있다. 시스템은 일부 주요 레코드의 실제 주소가 저장된 인덱스(index)를 관리한다. 인덱스된 순차 레코드는 키 값의 순서에 따라 순차적으로 액세스될 수도 있고, 시스템에 의해 생성된 인덱스의 검색을 통해 직접 액세스될 수도 있다. 일반적으로 인덱스된 순차 파일은 보통 디스크에 저장된다.
- 직접 파일(direct file)
  · 레코드가 직접 액세스 기억 장치의 물리적 주소를 통해 직접 액세스한다.

o 파일의 조작 : 운영체제는 파일의 생성, 기록, 판독, 재설정, 삭제, 절단 등을 위

한 시스템 호출(system call) 제공

(2) 디렉토리 구조

o 핵심가이드
- 다단계(1,2단계) 디렉토리 구조
- 트리 구조 디렉토리
- 그래프 디렉토리
- 파일 시스템 이해 : FAT16, FAT32, NTFS, EXT2, EXT3

o 디렉토리
- 디렉토리(directory)란 레코드의 각 필드에 대한 배열을 보관하는 파일로서, 한 파일 내 레코드의 배치 상황을 서술해 놓은 곳이다.

o 디렉토리의 역할
- 디렉토리는 디스크에 수록된 프로그램이나 파일을 찾기 위한 색인이며, 제어 프로그램으로서 참조된다. 또한 디렉토리는 시스템이 가지고 있는 파일의 일람표로서 파일의 명칭, 위치, 날짜 등이 저장되어 파일 관리의 중심이 된다.

o 디렉토리 구조
- 1 단계 디렉토리(Single Level Directory)
  · 모든 파일이 같은 디렉토리에 있어 유지 및 이해가 용이
  · 디렉토리 내의 모든 파일의 이름이 구별되어야 한다. 일반적으로, 파일명의 크기에 제한이 있다.
- 2 단계 디렉토리(Two Level Directory)
  · 각 사용자마다 별도의 사용자 파일 디렉토리가 배정된다.
  · 부팅시 마스터 파일 디렉토리(MFD)를 먼저 탐색한다.
- 트리 구조 디렉토리(Tree Structured Directory)
  · 사용자들이 자신의 종속 디렉토리(subdirectory)를 생성하며, 각 파일은 유일한 경로를 가짐
  · 파일(0)과 종속 디렉토리(1)의 구분 : 각 항목에 한 비트 지정
  · 디렉토리의 생성, 삭제, 변경 : 시스템 호출
  · 경로 이름 : 완전 경로 이름(루트 디렉토리부터 지정된 파일까지의 경로 명시), 상대 경로 이름(현재 디렉토리를 기준으로 지정)
- 비순환 그래프 디렉토리(Acyclic-Graph Directory)
  · 디렉토리들이 종속 디렉토리나 파일을 공유할 수 있도록 허용하는 구조

· 공유 파일/공유 디렉토리 구현 방법 : 새로운 디렉토리 항목 사용, 공유 파일에 관한 모든 정보를 복사하여 필요로 하는 디렉토리에 두는 방법

- 일반적인 그래프 디렉토리(General Graph Directory)
  · 순환 가능 구조

o 파일시스템 분석

- 파일시스템은 운영체제가 파티션이나 디스크에 파일들을 연속적으로 배열하기 위한 자료 구조이다. 즉, 파일들을 디스크에서 구성하는 방식이다. 파일들은 디스크에 파일시스템에 따라 조직적, 체계적으로 기록, 보존된다. 파일시스템은 파일시스템의 형태와 데이터가 저장되어 있는 디스크나 파티션을 참조할 때에 쓰여진다.
- Windows 파일시스템
  · FAT(File Allocation Table) : Windows에서 사용하는 파일 시스템으로 하드디스크에 파일 조각들이 저장된 위치를 가지고 있는 테이블을 말한다. 일반적으로 파일이 하드디스크에 저장되려면 이 파일을 일정한 크기의 작은 조각으로 나누어 저장을 한다. 왜냐하면 하나의 파일을 찾기 위하여 디스크 전체를 한 바이트씩 모두 찾는다면 시간이 많이 걸리므로 하드디스크를 검색할 때 일정한 크기 단위(클러스터)로 건너뛰며 검색하도록 하여 검색 속도를 증가시키기 위하여 파일을 조각으로 나누어 저장을 하고 해당 조각들의 위치를 저장한 테이블이 바로 FAT이며 FAT 16과 FAT 32가 있다.
  · FAT 16을 사용할 경우 클러스터가 65,535개 정도 사용될 수 있는데 하드디스크의 용량이 작으면 문제가 없지만 하드디스크의 용량이 커지면 클러스터의 크기도 덩달아서 커지므로 큰 클러스터에 작은 파일이 들어가게 되어 나머지는 낭비가 생기게 된다.
  · FAT 32는 클러스터를 4,294,967,000개의 공간으로 나눌 수 있다. 그러므로 용량이 큰 하드디스크라도 클러스터의 크기가 작아지므로 하드디스크의 낭비를 줄일 수 있다. 즉, 작은 클러스트 사이즈를 사용함으로써 FAT 16에 비해 더 효율적으로 하드디스크를 사용할 수 있으며 물리적 드라이브의 크기에 따라서 클러스트 사이즈가 다르게 설정된다.
  · NTFS는 매우 큰 하드디스크에서 효율적으로 파일을 저장할 수 있다. 클러스터의 개수는 2^64개로서 FAT 32보다 더 많다. NTFS는 파일을 항상 연속적인 블록에 저장하여 더 빨리 파일을 엑세스할 수 있다. NTFS는 Hot Fixing이라는 하드디스크 결함을 교정하는 기법을 제공하여 데이터를 저장하다가 에러가 발생하여도 안전하게 데이터를 보호할 수 있고 파일 압축 기

능이 파일 시스템의 고유한 기능으로 구현되어 있다.

- Unix 계열 파일시스템
  · 유닉스 파일시스템에서 슈퍼블럭(superblock)은 디스크의 크기와 같은 파일 시스템에 관한 일반적인 정보를 저장하는 부분이다. 이곳의 정확한 정보는 파일시스템 전반에 큰 영향을 미친다. 아이노드(inode)는 파일 이름을 제외한 파일에 관한 모든 정보를 저장하는 곳이다. 파일 이름은 inode 영역의 파일번호와 함께 디렉토리 영역에 저장된다. 아이노드 부분은 파일 내의 데이터를 보관하고 있는 데이터 블럭의 개수에 대한 정보도 가지고 있다. 아이노드에는 몇 개의 데이터 블럭을 위한 공간이 있다. 그러나 개수가 한정되어 있어서 만약 더 필요로 한다면 데이터 블럭 포인터를 위한 공간이 동적으로 할당된다. 바로 그 공간이 indirect block이다. indirect block이란 명칭은 데이터 블럭을 찾기 위한 공간임을 지칭한다. 시스템은 일차적으로 indirect block에서 파일번호를 찾게 된다.
  · ext2 : ext의 상위버전으로 리눅스를 위한 확장성있고 강력한 파일 시스템으로 가장 성공적인 파일 시스템일 뿐만 아니라 현재 배포되고 있는 모든 리눅스 배포판의 기반을 이루고 있다. 다른 파일 시스템과 마찬가지로 EXT2 파일 시스템은 파일에 들어있는 데이터의 데이터 블럭에 저장되며 모든 데이터 블럭의 크기는 같고 ext2 파일 시스템의 블럭크기는(mke2fs 명령을 통해) 파일 시스템이 만들어 질 때 결정된다. ext2는 파일 시스템 배치도를 정의하기 위하여 시스템내의 각 파일을 inode 자료구조로 표현한다.
  · ext3 : 캐시에 저장되어 있는 데이터들을 디스크로 저장하는 도중 만약 시스템이 다운되거나 여러 가지 문제가 발생할 경우 파일 시스템이 손상되는 단점을 가지고 있었다. 이를 위해 ext2는 fsck(File System Check)라는 파일 시스템 복구 기능을 제공하지만 시간이 만이 소요되고 시스템의 크기가 크다면 복구하는데 오랜 시간이 걸릴 뿐만 아니라 복구하는 동안 시스템을 사용하지 못하는 등의 문제점이 있는데 이를 보완하기 위한 ext3파일 시스템은 저널링(Journaling)이라는 기능을 추가 해서 소개된 파일 시스템이다. EXT3는 시스템의 무결성은 물론 뛰어난 복구 기능까지 가질 수 있게 되었다. 저널링 기술은 데이터를 디스크에 쓰기 전에 로그에 데이터를 남겨 시스템의 비정상적인 셧다운에도 로그를 사용해 fsck보다 빠르고 안정적인 복구기능을 제공하는 기술이다

(3) 파일 접근 방법

o 핵심가이드
  - 순차 접근
  - 직접 접근
o 파일 접근 방법
  - 순차 접근
    · 순차적으로 읽거나 쓰며 현재 파일 위치 포인터는 자동적으로 증가
    · 파일 내에서 순차적으로만 판독하거나 기록할 수 있음
    · 특정 시스템에서는 n개(통상 1개) 단위의 레코드 앞뒤로 이동 가능
  - 직접 접근
    · 파일을 블록 혹은 레코드의 집합으로 간주하고, 판독이나 기록의 순서에 제약이 없음(대규모 정보 접근에 유용)
    · 특히 대규모 정보의 경우, 파일명에 대한 해쉬 함수(hash function)를 사용하거나, 주기억장치내의 색인표(in-core index)를 이용하여 파일 탐색
  - 색인 접근(Index Access)
    · 각 파일마다 색인(index)을 두는 방법
    · 각 색인에는 여러 블록을 가리키는 포이터들로 구성됨
    · 파일 접근 방법 : 색인 탐색 후 포인터에 의한 직접 접근
o 파일 디스크립터(File descriptor)
  - 파일 디스크립터(file descriptor) 또는 파일 제어 블록(file control block)은 파일을 관리하기 위해 시스템이 필요로 하는 정보를 보관하고 있다.
  - 파일 디스크립터 내용 : 파일 식별 번호, 위치, 크기, 구조, 보조기억장치의 유형 등
  - 파일 디스크립터의 특징
    · 파일 디스크립터는 시스템에 따라 다른 구조를 갖는다. 보통 파일 디스크립터는 보조 기억 장치 내에 저장되어 있다가, 파일이 개방될 때 주기억장치로 옮겨진다. 파일 디스크립터는 파일 시스템이 관리하므로 사용자가 직접 참조할 수 없다.

1.2.4 분산 시스템

(1) 네트워크 운영체제(NOS-network operating system)

o 핵심가이드

- 네트워크 운영체제 개념 이해

o 네트워크 운영체제(NOS)는 통신을 제어하고 분산된 자원의 공유를 위해 널리 분산된 네트워크 시스템에 대하여 전역적인 관점에서 관리한다. 일반적인 네트워크 운영체제가 제공하는 기능에는 파일 서비스, 프린트 서비스, 주변 장치 공유, 원격 처리, 전자 우편, 네트워크 관리 등이 있다. 네트워크 운영체제의 분류는 운영 방식에 따라 C/S(client/server) 모델, Peer-to-Peer 모델이 있으며 네트워크상의 각 노드(node)의 자율성을 보장하고 이기종 시스템에 적합하지만 자원 공유 및 투명성 제공에 있어서 문제점을 갖고 있다.

- C/S 모델에서 : 서버에서 전역 자원을 관리하는데 중규모 이상의 LAN에 적합하다.
- Peer-to-Peer 모델 : 각 컴퓨터가 서버이면서 클라이언트로 동작하며 소규모 LAN에서 주로 사용한다.

(2) 분산 운영 체제의 주요 특징

o 핵심가이드

- 자료 이동
- 연산 이동
- 프로세스 이동

o 분산 운영 체제

- 분산 시스템은 각 사이트(site)가 컴퓨터에서부터 워크스테이션, 미니컴퓨터, 범용 컴퓨터 등 다양한 시스템으로 연결되어 구성할 수 있다. 분산 시스템의 목적은 자원의 공유, 연산 속도의 향상, 신뢰성과 컴퓨터 통신 등에 있다. 이러한 분산 시스템의 자원을 효율적으로 관리하기 위한 운영 체제를 분산 운영 체제라고 한다. 분산 운영 체제는 분산된 컴퓨터 간의 자원을 이용자가 쉽게 공유하여 액세스할 수 있도록 한다.

o 자료 이동(Data Migration)

- 사이트 A에 있는 사용자가 사이트 B에 있는 파일 등의 자료에 접근하려 할 때, 시스템이 자료를 이동하는 두 가지 기본적인 방법이 있다.
  · 파일 전체를 이동하는 방식
  · 실제 필요한 파일 일부를 이동하는 방식

o 연산 이동(Computation Migration)

- 대용량 파일의 접근이나 분석의 경우, 자료가 아닌 연산을 이동하는 것이 효율적이며 파일이 위치하는 사이트에 접근하여 연산 후 결과를 반환 받는 것이 바람직하다.
  · 원격 프로시저 호출(remote procedure call; RPC) : 프로세스가 원격 사이트에 프로시저를 통지하고, 이 프로시저는 실행 후 결과를 반환
  · 메시지 전송 : 프로세스가 원격 사이트에 작업 메시지를 보내면, 원격 사이트에서는 해당 업무를 위한 프로세스를 생성하고, 결과를 메시지 시스템으로 반환

o 프로세스 이동(Process Migration)

- 프로세스의 전체 혹은 일부를 다른 사이트에서 수행 가능하며 연산 이동의 논리적 확장이다.
- 사용하는 목적
  · 부하 균등화(load balancing) : 부하를 균등하게 하기 위해 프로세스를 분산함
  · 연산 속도 향상(computation speedup) : 프로세스가 동시에 다른 사이트에서 수행될 수 있는 부분 프로세스들로 분리될 수 있다면, 전체 반환 시간이 축소됨
  · 하드웨어 선호성(hardware preference) : 특정 프로세스는 특정 프로세서에 의해 수행되는 것이 적합할 수 있음
  · 소프트웨어 선호성(software preference) : 특정 프로세스는 특정 사이트의 소프트웨어에 의해 수행하는 것이 적합할 수 있음
  · 데이터 접근(data access): 데이터의 양이 많은 경우 데이터의 이주보다 프로세스의 이주가 바람직함
- 프로세스 이주를 위한 두 가지 상호 보완적인 기법
  · 시스템은 프로세스가 이동되었다는 사실을 사용자로부터 숨긴다. 즉, 사용자가 이주 명령을 명시할 필요가 없으며 주로 부하 균형, 연산 속도 향상 목적에 사용
  · 사용자가 프로세스의 이주를 명시하는 경우 특정 하드웨어 선호성이나 소프트웨어의 선호성 목적에 사용

(3) 분산 시스템에서의 운영체제 기술

o 핵심가이드

- 사건 순서화(event ordering)
- 상호 배제(mutual exclusion)
- 교착 상태의 예방과 탐지
- 선출(election) 알고리즘

o 사건 순서화(Event Ordering)

- 중앙 집중형 시스템에서는 하나의 공유 메모리와 클럭을 사용하므로 두 개의 사건이 발생해도 그 순서를 결정하는 것이 가능하지만 분산 시스템에서는 공유 메모리와 공유 클럭이 없기 때문에 사건의 순서 예측이 어렵다.
- 사건의 전후 관계(happened-before relation) : 분산 시스템에서 사건의 부분적인 순서만을 정의한다. 전체 사건의 순서를 결정하는 것은 전후 관계를 일관성있는 전체 순서화로 확장하는 분산 알고리즘을 사용한다.

o 상호 배제(Mutual Exclusion) : 분산 환경에서의 상호배제 구현

- 중앙 집중형 접근(Centralized Approach)
  - ･시스템 내의 프로세스 중 하나가 임계구역의 출입구를 관리하는 조정자 역할을 수행
  - ･특성 : 상호 배제 보장. 조정자의 스케줄링 알고리즘이 공정(FCFS)하면 기아 상태도 발생하지 않음. 조정 프로세스의 고장 시 새로운 프로세스가 대신하게 됨
- 완전 분산형 접근(Fully Distributed Approach)
  - ･사건 순서화 정책에 기반을 둔 알고리즘: 임계 구역에 대한 모든 요청을 전역 순서화하고 FCFS 순서로 프로세스를 처리하는 방법
  - ･특성 : 상호 배제 보장. 교착 상태 미발생 보장. 타임스탬프 순서로 스케줄 되므로(FCFS 방식), 기아 상태 미발생 보장.
- 토큰 패싱 접근(Token-Passing Approach)
  - ･시스템내의 프로세스들 간에 토큰을 순환시키고, 유일하게 존재하는 토큰을 소유한 프로세스만이 임계 구역에 들어가게 하는 방법. 토큰(token)은 시스템에서 전달되는 일종의 특정한 메시지 형태
  - ･임의의 프로세스가 토큰을 받으면, 그 토큰을 보유하고 해당 임계 영역에 진입할 수 있으며 그 프로세스가 임계 구역을 나오면, 토큰을 다시 전송함.
  - ･토큰을 받은 프로세스가 임계 구역에 진입하는 것을 원치 않으면, 그 토큰을 단지 이웃에 전송함

o 교착상태는 동일한 자원을 공유하고 있는 두 개의 컴퓨터 프로그램들이 서로 자원에 접근하는 것을 방해함으로써 두 프로그램 모두 기능이 중지되는 상태를

말한다.

- 교착상태 처리 방법
  - ·교착 상태가 되지 않도록 보장하기 위한 프로토콜 사용
  - ·교착 상태가 되도록 허용한 다음에 회복시키는 방법
  - ·교착상태가 시스템에서 발생하지 않도록 하는 방법 : 교착 상태 예방(교착 상태 발생 필요조건 중 하나를 가지지 않도록 보장), 교착 상태 회피(프로세스 수행중 부가적인 정보의 요구로 어떤 프로세스를 대기해야 하는지 결정)
- 교착상태 예방
  - ·상호 배제 : 공유 가능한 자원은 배타적인 접근을 요구하지 않으므로 교착 상태도 될 수 없다.
  - ·점유와 대기 : 프로세스는 수행 전에 모든 자원을 요청하거나 프로세스가 자원을 전혀 갖고 있지 않을 때만 자원을 요청
  - ·비선점 : 자원 요청이 거부되면 현재 점유하고 있는 모든 자원들은 선점(암시적 해제).
  - ·순환 대기 : 모든 자원 형태들에게 전체 순서를 부여하여, 각 프로세스가 열거된 상태에서 오름차순으로 자원을 요청.
- 교착상태 회피 : 순환 대기 조건으로 되지 않도록 자원 할당 상태(가용한 자원의수, 할당된 자원의 수, 프로세스들의 최대 요구 수에 의해 정의)를 검사.
  - ·안정 상태 : 특정한 순서대로 각 프로세스에 자원을 할당할 수 있고 교착상태를 방지할 수 있는 상태. 초기에 시스템은 안정상태에 있다. 프로세스가 가용한 자원을 요청해 올 때마다 시스템은 자원이 즉시 할당될 수 있는지 또는 프로세스가 대기해야 되는지를 결정해야 한다. 자원 할당 후에도 시스템이 항상 안정 상태에 있을 때만 요청을 허용한다.
  - ·자원 할당 그래프 알고리즘 : 자원 할당 그래프의 변형은 교착 상태 회피를 위해 사용된다.
  - ·은행가 알고리즘 : 다수개의 자원을 가진 시스템에 적용될 수 있지만, 자원 할당 그래프 방법보다는 덜 효과적이다.
- 교착상태 탐지 : 교착상태 예방이나 방지 알고리즘을 사용하지 않는다면 시스템의 상태를 탐지하는 알고리즘과 교착상태로부터 회복하는 알고리즘을 지원해야 한다.
  - ·각 자원 형태마다 자원이 한 개씩 있는 경우 : 대기그래프를 사용해 교착 상태 탐지 알고리즘을 정의.
  - ·자원 형태마다 여러 개의 자원이 있는 경우 : Available(각 자원 형태마다

사용 가능한 자원의 수를 표시하는 길이가 m인 벡터), Allocation(각 프로세스에 현재 할당된 각 형태들의 자원의 수를 표시하는 n×m 행렬), Request(: 각 프로세스 현재 요청을 표시하는 n×m 행렬)

· 탐지 알고리즘 사용 : 교착 상태의 발생 빈도수와 교착 상태가 발생하였을 때 영향을 받는 프로세스의 수에 요인하여 탐지 알고리즘 호출 결정.

o 선출 알고리즘(Election Algorithms)

- 조정자 프로세스(coordinator process)의 역할
  · 상호 배제 보장
  · 교착 상태 탐지를 위한 전역 대기 그래프의 유지
  · 시스템내의 입출력 장치의 조정 : 사이트의 결함으로 조정자 프로세스의 수행이 불가능해지면, 다른 사이트에 조정자 기능을 새로이 복사하여 시스템을 계속 동작시킬 수 있음
- 선출 알고리즘 종류 : 조정자의 새로운 복사를 어느 곳에 하는가를 결정하는 알고리즘
  · Bully 알고리즘: 프로세스가 다른 모든 프로세스에 메시지를 보낼 수 있는 시스템에 적용
  · 링 알고리즘: 논리적 또는 물리적으로 구성된 링 구조의 시스템에 적용

(4) 분산 파일 시스템

o 핵심가이드

- 명칭 부여 구조(naming scheme)
- 원격 프로시저 호출(RPC)
- 캐시 기법
- 파일 중복(replication) 기술

o 네이밍(Naming) 구조

- 네이밍 : 논리적인 객체들과 물리적인 객체들 간의 사상.
  · 사용자 : 파일의 이름에 의해서 표현되는 논리적인 자료 객체를 사용.
  · 시스템 : 디스크에 저장되어 있는 물리적인 자료 블록을 조작.
- 네이밍 구조 : 네이밍 사상에 관한 두 가지 중요 개념
  · 위치 투명성(location transparency) : 파일의 이름에 그 파일의 물리적 기억장소에 대한 정보를 나타내지 않음.
  · 위치 독립성(location independency) : 파일의 물리적 기억장치의 위치가 변

경되어도 파일 이름을 변경할 필요 없음

- 네이밍 기법(Naming Schemes)
  - 파일의 이름을 호스트 이름(host name)과 지역 이름(local name)의 조합으로 구성하는 방법
  - 원격 디렉토리들을 지역 디렉토리에 붙일 수 있게 하는 방법
  - 구성 파일 시스템들을 전체적으로 통합하는 방법

o 파일 중복(File Replication)

- 여러 기계에 파일을 중복시키는 것은 접근 요청에 대해 가장 가까운 복사본을 선택하여 사용할 수 있으므로 전체 시스템의 가용성을 증가시키고 성능을 향상 시킬 수 있다.
- 파일 중복의 문제점 : 복사본의 갱신(사용자의 관점에서 복사본들은 동일한 논리적인 존재이므로, 임의 복사본에 대한 갱신은 다른 모든 복사본에게 반영되어야 한다.
  - 일관성 유지 방법 : 일관성 유지를 위해 프로세스의 무한정 대기 상태를 초래할 수 있는 방법
  - 일관성 무시 방법 : 프로세스 수행을 보장하기 위해 일관성 파괴로 인한 오류를 감수하는 방법

o 캐싱 기법(Basic Caching Scheme)

- 캐싱의 개념
  - 만일 어떤 접근 요구를 만족하는 자료가 캐시되어 있지 않으면 이 자료의 복사본을 서버로부터 클라이언트 시스템으로 이동시키고, 접근은 캐시된 복사본상에서 행해짐
  - 동일한 정보에 대한 반복된 접근은 부가적인 네트워크 접근 없이 지역적으로 처리될 수 있음
  - 요구 페이지 가상 기억장치와 유사
- 캐시 위치(Cache Location)
  - 캐시된 자료의 저장 위치 : 디스크 캐시(비휘발성이므로 기억장치의 오류 발생시에도 자료가 지역에 보관됨). 주기억장치 캐시(디스크가 없어도 됨)
- 캐시 갱신 전략(Cache Update Policy)
  - 수정된 자료 블록을 서버의 마스터 복사본에 갱신하기 위한 전략(즉시 기록 : 수정 직후 즉시 기록하는 방법. 교체 기록/지연 기록 : 수정은 캐시에서 이루어지고, 마스터 복사본의 수정을 지연하는 방법)
  - 지연 기록 기법의 종류 : 클라이언트의 캐시에서 블록이 나오기 직전에 반

영하는 방법. 정규 기간마다 캐시를 조사하여 지난 조사 이후 갱신된 블록을 반영하는 방법. 파일이 폐쇄될 때 반영하는 방법

1.3 운영체제 사례별 특징과 주요 기능

1.3.1 유닉스

(1) 유닉스의 특징과 주요 계보

o 핵심가이드
- 운영체제로서의 유닉스 특징
- SVR과 BSD 개념
- 유닉스 운영체제의 계보 : AIX, SunOS(Solaris), IRIX, DEC UNIX, HP UX 등

o 유닉스는 AT&T를 통해 상업적으로 허가해주는 SVR(System V Release) 계열과 버클리 대학에서 나온 연구 개발 운영체제인 BSD 계열로 크게 나누어 발전해 왔다. 점차 각자의 고유한 특성을 가지게 되었으며 이후 POSIX를 통하여 SVR, BSD에서 동시에 동작하는 표준을 제공하여 여러 시스템에서 동작하는 프로그램을 만들수 있게 된 것이다.

o 운영체제로써의 유닉스의 특징
- 대화식 운영체제(Shell) : 사용자에게 명령어를 입력받기 위해서 유닉스는 쉘 프롬프트를 화면에 나타낸다. 프롬프트가 나타난 상태에서 사용자가 명령어를 기술하면 그 명령어는 명령어 해석기(shell)를 통하여 시스템에 전달되고 시스템은 명령어를 처리하여 정상적인 명령인지 오류 명령인지에 대하여 답변해 주면서 동시에 시스템의 고장 원인에 대한 답변도 알려주는 방식으로 사용자가 마치 시스템과 대화하는 것과 같은 방식으로 사용된다.
- 멀티태스팅 : DOS와의 커다란 차이점인 멀티태스킹(Multi-Tasking)은 하나의 명령어 처리가 완료되지 않은 상태에서 다른 명령어를 처리할 수 있다는 뜻으로, 즉 여러 개의 명령어를 동시에 처리할 수 있는 방식을 의미한다.
- 멀티유저환경 : 멀티태스킹과 같은 기능이 가능함으로써 멀티유저(Multi-User) 시스템으로 쓰여 질수 있는 것이다. 멀티유저는 다중 사용자라는 뜻으로 여러 사용자가 시스템을 동시에 사용할 수 있도록 되어 있다.
- 계층적 파일 시스템 : UNIX 파일 시스템은 트리구조로 구성되어 있는데 이 트리는 디렉토리이다.

- 이식성(Portability) : 이식성이란 하드웨어의 종류에 상관없이 운영되는 특성을 말한다.
- 유연성 : 동일 기종 간 또는 타기종 간의 통신(communication)상의 유연성을 가지고 있다. 따라서 전자우편이나 통신망이 많이 이용되고 있으며 최근에는 PC통신에 많이 사용되고 있는데, 통신망의 유연성이라는 것은 기종간의 자료를 보내고 받아들임에 있어서 자료의 손상이 적고 어느 기종이든 편리하게 통신할수 있다는 것을 의미한다.
- 호환성 : 타 기종에 자유로이 사용되므로 호환성이 높다.
- 입・출력 방향 전환 및 파이프 기능 : 표준 입・출력을 다시 지정하여(<, >) 키보드로부터 입력받는 것이 아니라 파일로 부터 직접 파일 내용을 입력받을 수 있고, 출력 역시 모니터로의 출력이 아닌 선택된 어떤 파일로 출력 방향의 지정이 가능하며 파이프(|)는 2개 이상의 명령어를 연결하여 다음 명령어의 입력값으로 지정될 수 있다.
- 보안 및 보호 기능
- 각종 디바이스의 독립성 : 모든 주변장치는 하나의 파이로 간주된다.

o 유닉스 운영체제 종류
- UNIX System V R4.0 : 유닉스의 표준이 되는 버전으로 벨 연구소에서 개발된 유닉스 시스템의 정식 이름
- SunOS : Sun사의 가장 잘 알려진 BSD 중심의 운영체제
- Solaris : Sun의 SVR4 구현
- HP-UX : UNIX의 휴렛-팩커드 버전은 OSF/1의 많은 특성들을 도입한 SVR4의 변형이다. HP-UX 9 버전은 몇가지 확장성을 가진 SVR3 와 비슷하고 HP-UX 10은 SVR4 운영체제
- AIX : IBM의 System V 운영체제로 SVR4, BSD, OSF/1의 특징들을 고루 가지고 있다.
- Linux : 인텔 프로세서를 위한 Free UNIX 방식의 운영체제이다. 리누스 토발즈가 만들었으며 이름의 의미는 Linus의 UNIX라는 뜻이다. Linux는 BSD 방식이다. 기술적으로 Linux라는 이름은 기본적인 core(커널과 일부드라이버 등)를 말하지만 일반적으로 Linux 보급판을 구성하고 있는 다양한 소스로부터 전체적인 프리웨어를 말한다.

(2) 유닉스 쉘

o 핵심가이드

- 쉘(shell)의 기능과 종류별 특징 : sh, csh, ksh
- 간단한 쉘프로그래밍
  - ㆍ특정 폴더의 내용을 정기적으로 백업
  - ㆍ반복적으로 수행해야하는 명령어를 쉘프로그램으로 간단하게 수행
  - ㆍ기타

o 쉘(shell)의 기능

- 쉘이란 명령어 해석기(command proccessor)로서 사용자가 입력하는 명령을 읽고 해석하는 것을 의미하며 사용자가 프로그램을 수행하고 프로세스들의 파이프라인을 만들고 출력을 파일에 저장하며, 동시에 하나 이상의 프로그램이 수행되도록 한다. 이처럼 명령어 해석기로서의 역할뿐만 아니라, 쉘은 또한 프로그래밍 언어이기도 하여 쉘이 해석할 수 있는 "스크립트(scripts)"라는 프로그램을 작성할 수 있고 유닉스 명령뿐만 아니라 특별한 쉘 프로그래밍 언어도 포함할 수도 있다.
- 쉘의 종류 : sh, csh, ksh
  - ㆍsh(Bourne shell) : 1979년에 발표된 UNIX System V release와 함께 제공된 쉘로써 개발자인 Stephen Bourne의 이름을 따서 Bourne shell이라고 부른다.
  - ㆍcsh(C shell) : Berkeley UNIX version과 같이 개발되었으며 다양한 하드웨어에 이식할 수 있는 장점을 지니고 있다.
  - ㆍksh(Korn shell) : 벨 연구소의 David Korn이 개발한 콘쉘은 Bourne 쉘의 기능에 C 쉘에서 처음으로 도입된 몇 가지 유용한 기능들을 추가한 것이다. Bourne쉘로 작성된 스크립트와 프로그램들을 수정하지 않고도 Korn쉘에서 사용할 수 있다.
  - ㆍtcsh : tcsh은 코넬대학에서 Korn쉘의 매끄러운 히스토리 편집 기능을 포함시킨 C쉘의 수정본을 개발한 것이다. tcsh은 95%의 C 쉘과 5%의 새로운 기능으로 구성되었다.

o 간단한 쉘프로그래밍

- 쉘프로그램은 간단하지 않는 설정사항을 반복적으로 수행하여야 하는 경우나 정기적인 시스템 관리업무 등을 자동으로 수행하는 경우에 자주 사용하며, 정기적인 쉘프로그램 수행을 위해서는 crontab에 등록하는 방법도 이해해야 한다.

(3) 일반 사용자를 위한 유닉스 활용법

o 핵심가이드

- 일반사용자 수준의 로그인, 디렉토리 관리, 파일압축 및 관리, 패스워드변경, 계정관리 등 주요 유닉스 명령 사용방법
- 일반사용자 수준의 vi 에디터 등 주요 유틸리티

o 일반사용자용 주요 유닉스 명령

- cd : 현재 디렉토리를 바꿈
- cp : 지정된 파일을 다른 이름으로 복사
- mv : 디렉토리 또는 파일의 이름을 변경
- rm : 파일 혹은 디렉토리를 삭제
- mkdir : 새로운 디렉토리를 만듬
- rmdir : 지정된 디렉토리를 제거
- pwd : 현재의 작업디렉토리를 화면에 출력
- cat : 파일의 내용을 표준 출력 장치로 내보내는 명령어
- chmod : 지정된 파일에 대한 사용 권한을 변경하고자 할 때 사용
- ps : 컴퓨터 시스템에서 활동중인 프로세서의 상태를 알려주는 명령
- tar : 파일들을 자기 테이프에 저장 또는 불러오기 위한 명령어
- passwd : 자신의 암호를 등록하거나 변경할 때 사용
- chgrp : 지정된 파일의 소유권자 그룹을 바꾸는 명령
- chown : 지정된 파일에 대한 소유 권한을 변경하고자 할 때 사용
- su
- useradd/userdel

(4) 유닉스 시스템 관리법

o 핵심가이드

- 유닉스 시스템의 내부 구조 및 구성요소 특징
- 시스템 관리자용 주요 유닉스 명령

o 유닉스 시스템의 내부 구조

- UNIX 시스템을 이루고 있는 구성 요소를 크게 나누면 본체를 구성하는 여러 가지의 하드웨어와 시스템의 운영을 담당하는 운영체제(OS) 그리고 사용자의 명령어를 해석하는 명령어 해석기(Shell), 유닉스 명령어, 커널(kernel)등의 소

프트웨어로 구성되어 있다.

- 유닉스의 내부구조로 커널의 역할
  · 프로세서 컨트롤러 : 프로세서를 제어하는 것으로 여러개의 프로세서들을 실행, 중지하는 등 실행 프로그램을 제어하는 역할이다.
  · 서브시스템 : 시스템을 제어하는 데 관련된 여러가지 정보와 참고자료로 구성된 형태로 커널 자체적인 호출에 사용되는 것이다.
  · 내부 프로세스 통신 : 유닉스 내부에서 운영되는 프로그램들을 연결하는 역할이다.
  · 스케쥴러 : 스케줄에 관한 것으로 유닉스 내부에서의 프로그램 처리순서 등을 관리하는 역할에 관한 내용으로TSS방식의 시스템에서는 필수적인 내용이다.
  · 메모리 관리자 : 메인 메모리에 읽혀진 프로그램들의 크기라든가 남아있는 영역의 효율적인 관리를 목적으로 운영되는 프로그램이다.

o 시스템 관리자용 주요 유닉스 명령
- df : 슈퍼블록에서 카운트하고 있는 마운트된 파일 시스템, 디렉토리에서 사용 가능한 디스크블록과 free inode수를 알려줌
- file, find, grep, script, tty, ps, kill 등

1.3.2 윈도우

(1) 윈도우의 특징과 주요 계보

o 핵심가이드
- 운영체제로서의 윈도우 특징
- 윈도우 9x 계열과 윈도우 NT 계열의 발전 흐름 및 종류별 주요 특징

o 운영체제로서의 윈도우 특징
- 32bit 운영체제 : 16bit로 처리되던 DoS보도 처리속도가 빠르다.
- GUI 환경 : 아이콘이라는 그림명령을 통하여 쉽게 프로그램에 접근할 수 있다.
- Plug & Play : 하드웨어를 새롭게 추가하는 경우 자동으로 인식하여 환경을 설정해 주는 기능으로 해당 하드웨어가 Plug & Play 기능을 지원하는 장치이어야 한다.
- 단축아이콘(Short Cut)/바로가기 : 프로그램이나 데이터를 빠르고 편리하게 실

행시키기 위해서 원하는 위치에 원본 파일을 연결한 아이콘을 만들 수 있다

- 멀티태스킹 : 한번에 여러 가지 작업을 동시에 수행할 수 있다. 윈도우를 사용하면 몇 개의 강력한 응용 프로그램을 즉시 작동시킬 수 있는 대기상태로 만들 수 있고 또한 그들 사이의 빠른 전환(switching)이 가능해 진다
- OLE(Object Linking Embedding) : 개체 연결 포함 기능으로 프로그램간에 개체(그림, 표등)를 교환할 수 있다.
- 멀티미디어 가능 향상
- 네트워크 기능 향상 : 다양한 프로토콜을 제공하기 때문에 네트워크 설치나 인터넷 연결 등을 편리하게 할 수 있으며, 특히 Netbios라는 프로토콜을 사용하여 네트워크 공유가 편리하다.
- 다중 모니터 지원 : 한대의 컴퓨터에 최대 8대의 모니터를 연결하여 사용할 수 있다.
- 정보의 전송 통합 : 두개 또는 그 이상의 응용 프로그램에서 작업하여 상호간에 정보를 한 응용 프로그램으로부터 다른 응용 프로그램으로 전송 통합할 수 있다. 이것은 클립보드라고 불리우는 Desktop accessory를 통해 이루어진다.

o 윈도우 9x 계열과 윈도우 NT 계열

- 윈도우 95
  - ㆍ윈도우 운영체제 중 최초의 GUI 환경의 운영체제
- 윈도우 98
  - ㆍ윈도우 95 버그 수정/업데이트
  - ㆍ익스플로러 4.0을 자체적으로 탑재
  - ㆍPNP 기능 업데이트
- 윈도우 NT
  - ㆍ서버용 UNIX를 모든 서버에서 채용하고 있었는데.. 이에 대항하기 위하여 만든 운영체제
- 윈도우 2000
  - ㆍProfessional, Server, Advance Server, Datacenter Server로 분류
  - ㆍ기존의 운영체제보다 상당히 안정된 운영체제
  - ㆍ보안성 강화
- 윈도우 XP
  - ㆍ클라이언트용 OS
  - ㆍ홈에디션, 프로페셔널 등으로 분류

· 그래픽 기능, 뛰어난 PNP 기능, 뛰어난 네트워크, 뛰어난 보안성, 뛰어난 안정성 업데이트

- 윈도우 2003
  · 웹 에디션, 스탠다드 에디션, 엔터프라이즈 에디션
  · 안정적
  · 보안기능 강화

(2) 윈도우 종류별 주요 활용법

o 핵심가이드
- 윈도우 종류별 공통적인 기능 활용법 및 특징적인 기능 활용법 이해

o 윈도우 종류별
- 윈도우 2000
  · NTFS 파일시스템 사용 가능
  · 파일 시스템 암호화 : 임의로 생성된 키를 사용하여 각 파일을 암호화한다.
  · IPSec 기능
  · 그룹 정책 : 그룹 정책 설정은 관리자가 사용자와 개체를 부서 또는 위치 같은 논리 단위로 구성한 다음 동일한 설정(예: 보안, 모양 및 관리 옵션)을 해당 그룹의 모든 직원에게 할당할 수 있도록 해주므로 사용자와 개체의 관리가 단순해집니다.
- 윈도우 XP(Professional)
  · NTFS 파일시스템 사용 가능
  · 시스템 복원 : 시스템 복원 기능을 사용하면 사용자와 관리자는 데이터 손실 없이 컴퓨터를 이전 상태로 복원할 수 있다. 이 기능은 시스템을 이전 시점으로 복원할 수 있는 쉽게 식별되는 복원 지점을 자동으로 생성한다.
  · 인터넷 연결 방화벽 : 일반적인 인터넷 공격으로부터 소규모 기업을 보호할 수 있는 방화벽 클라이언트이다.
  · 다중 사용자 지원이 포함된 파일 시스템 암호화(EFS) : 임의로 생성된 키를 사용하여 각 파일을 암호화한다. 윈도우 XP Professional에서 EFS는 여러 사용자가 암호화된 문서에 액세스하는 것을 허용할 수 있다.
  · IPSec 기능
  · 동적 업데이트를 사용한 설치 : Windows XP Professional 설치 루틴은 운영 체제 파일이 최신 상태를 유지하게 한다. 파일을 설치하기 전에

Windows XP Professional은 웹에서 중요한 시스템 업데이트를 확인하여 설치에 필요한 업데이트를 다운로드한다.

· 원격 지원 : 원격 지원을 사용하면 네트워크 또는 인터넷상의 다른 사용자와 컴퓨터 제어를 공유할 수 있다.

· 그룹 정책 : 그룹 정책 설정은 관리자가 사용자와 개체를 부서 또는 위치 같은 논리 단위로 구성한 다음 동일한 설정(예: 보안, 모양 및 관리 옵션)을 해당 그룹의 모든 직원에게 할당할 수 있도록 해주므로 사용자와 개체의 관리가 단순해집니다. 윈도우 2000에 비하여 수많은 정책 사용 가능하다.

· 통합된 CD 굽기 기능 : Windows XP Professional은 CD-R 및 CD-RW 드라이브에서 CD를 굽기 위한 통합 지원을 제공한다.

1.3.3 리눅스

(1) 리눅스의 특징과 주요 배포판

o 핵심가이드
- 리눅스의 차별화된 특징
- X-윈도우 시스템 특징
- 다양한 리눅스 종류별 특징 : 터보리눅스, 레드햇, 데비안, 수세, 칼데라, 맨드레이크, 슬랙웨어, FreeBSD 등

o 리눅스의 차별화된 특징
- 오픈 소스 운영체제
- 다중 사용자 환경
- 다중작업 및 가상 터미널 환경
- GUI 방식의 X윈도우
- CPU에 구애 없는 운영체제
- 강력한 네트워크 환경
- 다양한 드라이버 지원

o X-윈도우 시스템
- X window 시스템은 리눅스를 비롯해 대부분의 유닉스에 채용되어 있는 혁신적이면서 네트워크 투명성을 보장하는 그래픽 환경 기반의 시스템 소프트웨어이며 현재의 리눅스에 있어 표준으로 사용되는 것은 XFree86 프리웨어 프로그램이다. X 윈도우 시스템은 서버／클라이언트로 구성되어 있으며 X

프로토콜에 의해 상호작용이 이루어진다.

- X 윈도우의 특징
  - ·네트워크 기반의 그래픽 환경이다.
  - ·프로그램 작성시 가장 많은 종류의 컴퓨터에서 구동될 수 있을 정도로 이식성이 뛰어나다.
  - ·스크롤바, 아이콘, 색상 등의 그래픽 환경에 필요한 자원들이 특정한 형태로 정의되어 있지 않다.
  - ·서로 다른 이 기종을 함께 사용한다.
  - ·디스플레이 장치에 의존적이지 않다.
- 서버/클라이언트 방식
  - ·기본적으로 클라이언트는 응용프로그램을 말한다. X 윈도우 클라이언트는 직접적으로 사용자와 통신할 수 없다. 클라이언트는 서버로부터 키보드나 마우스 입력같은 사용자의 입력을 얻을 수 있다. 즉 X클라이언트는 X서버가 제공하는 기능들을 이용하도록 작성된 하나의 응용프로그램이다. 서버는 응용 프로그램에서 수행된 결과를 출력장치에 표시하는 역할을 맡고 있다.
- 통신을 위해서 X 프로토콜을 이용한다.

o 리눅스 종류 : 리눅스는 공개소프트웨어로 제공되므로 GPL에 있는 제한들이 준수되는 한 거의 모든 사람들이 리눅스를 사용하거나 배포하는 것에 제재를 받지 않는다. 해외 배포판의 종류로는 슬랙웨어(Slackware), 레드햇(Red Hat), 데비안(Debian), 오픈 리눅스(Open Linux), Linux-Mandrake, SuSE-Linux, Fedora 등이 있으며, 국내 배포판도 다수 있다.

- 레드햇 리눅스는 배포판중에서 가장 널리 알려진 것으로 레드햇 소프트웨어사에 의해 공급되고 있는데, 가장 큰 특징은 알기 쉬운 인스톨러와 관리툴이라고 할 수 있다.
- Debian : 데비안은 비영리조직에 의해 전 세계의 다양한 개발자들이 참여할 수 있도록 만든 데비안 프로젝트에 의해 발전되어왔는데, 버그를 보고하거나 패키지를 개발하는 형태로 참가할 수 있다. 따라서 데비안 프로젝트는 Linux가 개발된 과정을 거쳐 왔다. 이러한 배경에서 데비안의 가장 큰 특징은 패키지에 보안 취약점이 발견되면 바로 업데이트가 가능하다.
- 오픈 리눅스 : 미국에서 인기가 높은 오픈 리눅스의 가장 큰 특징은 Netware와 접속성에 뛰어나다는 것으로 구체적으로 NetWare에 탑재되어 있는 디렉토리 서비스인 NDS(Novell Directory Service)의 클라이언트 기능을 갖추고 있다.

- K 리눅스 : K리눅스는 레드햇 기반으로 만들어졌으며, 이전 버전에 비해 HTTP를 통한 설치, 새로운 인증 설정 화면, 그리고 설치시 Xconfigurator를 추가했습니다. K리눅스의 가장 큰 특징은 리눅스 인터내셔널이 독자적으로 개발한 한글 입력기 K-input, 인터넷을 통해 자동으로 소프트웨어를 업그레이드 해주는 K-linux 업데이트 인스톨러를 들 수 있다.
- 엑셀 리눅스 : 엑셀 리눅스는 레드햇을 기반으로 한글화한 배포판이다. 엑셀 리눅스 6.0은 사용자 측면을 최대로 수용하여 한글화 작업을 하였고, 많은 어플리케이션에서의 한글화의 문제점을 최소화 했습니다.
- 알짜 리눅스 : 알짜리눅스는 한국의 리눅스 사용자들이 설치 즉시 쉽게 자신의 업무에 활용 할 수 있는 배포판을 만들고자 하는데서 출발하였습니다. 현재 알짜리눅스는 기업 상용버전으로 많은 주목을 받고 있다.
- 미지리눅스 : 기존의 리눅스들이 서버용으로 개발된 것과는 달리 데스크탑용으로 만들어져 있기 때문에 문서작성 뿐만 아니라, PC통신, 웹브라우저, 그래픽툴 등을 기본적으로 제공하는 것이 특징이다.
- 파워리눅스 : 리눅스의 엔터프라이즈급 버전으로 서버 최적화 기능과 관리를 실현하고 암호화 및 보안을 강화했다. 사용자 편이성에 중점을 둔 파워리눅스는 기업 전산환경에 적합하도록 개발되었으며, 웹을 기반으로 사용자들에게 통합된 관리시스템을 제공한다.

(2) 리눅스 쉘

o 핵심가이드
- 쉘(shell)의 기능과 bash의 특징
- 간단한 쉘프로그래밍
  · 특정 폴더의 내용을 정기적으로 백업
  · 반복적으로 수행해야하는 명령어를 쉘프로그램으로 간단하게 수행

o 특정 폴더의 내용을 정기적으로 백업하는 스크립트 예제
- vi 에디터를 이용하여 backup.sh로 쉘프로그래밍 저장

```
#! /bin/bash
export today=" 'date '+ %y-%m-%d' ' "
cd /backupdata/
tar cvfpz $today-etc.tar.gz  /etc/
```

- 파일로 저장한 쉘프로그램을 crontab에 등록

(3) 리눅스 시스템 관리법

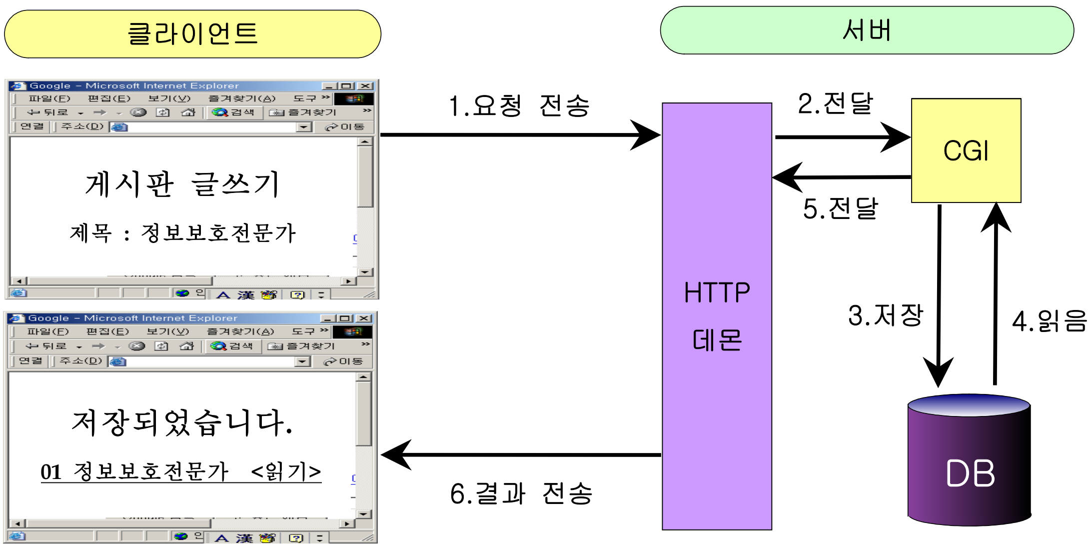
o 핵심가이드
- 시스템 설치 및 장치 설정
- 사용자 등록 및 제거 방법 이해
- 인터넷 및 네트워크 서비스를 제공하기 위해서 IP 설정, service 포트 설정 등록 등의 네트워크 환경 설정
- 웹서버의 구조 및 구성요소, 웹서버의 동작원리 : Apache, PHP, MySQL 등
  · 웹서버 구성에 필요한 form 태그, post와 get, 세션과 쿠키, 웹애플리케이션 프로그래밍 등 기술

o 시스템 설치 및 장치 설정
- 장치 각각의 환경설정 명령을 실행하던지, 아니면 루트 계정으로 로그인한 후 'setup'명령을 실행시키면 된다. 'setup'명령을 실행시키면 다음과 같은 화면이 나타난다. 설정하고자 하는 항목을 선택하여 설정하고 'Run Tool'버튼을 누르면 된다.
- 키보드 설정
  · 리눅스를 설치할 때 한번 했지만, 키보드를 바꾸거나 설정을 바꾸고 싶을 때 사용한다. 'setup' 메뉴의 'Keyboard configuration'을 선택하거나 '/usr/sbin/kbdconfig'을 실행시킨다. 그러면 리눅스를 설치할 때 본 화면과 같은 화면이 나타난다. 여기에서 원하는 키보드를 선택하고 'OK'를 누르면 된다.
- 마우스 설정
  · 'setup'메뉴의 'Mouse configuration'을 선택하거나 '/usr/sbin/mouseconfig'을 실행시킨다.
- 프린터 설정
  · 'setup'메뉴의 'Printer configuration'을 선택하거나 '/usr/sbin/printer-config'을 실행시킨다.
- 사운드카드 설정
  · 'setup'메뉴의 'Sound card configuration'을 선택하거나 '/usr/sbin/snd-config'를 실행시킨다.

o 웹서버 구조 이해
- 웹서버는 웹서비스를 제공하는 주체가 되며 클라이언트가 웹브라우저를 이용하여 웹서버에 접속하여 웹서비스를 이용하고 이때는 http 프로토콜을 이용한

다. 대부분의 웹서버는 IIS나 아파치 등의 서버 프로그램, 회원정보 등의 중요한 데이터를 저장하기 위한 데이터베이스 프로그램, 그리고 PHP, ASP, JSP, CGI 등과 같이 웹서버와 데이터베이스를 연동시키는 웹애플리케이션으로 구성된다.

- 웹서버 동작 원리



(그림 1-2) 웹서버 동작원리

· 클라이언트가 웹브라우져를 이용하여 로그인을 시도한다.

· 웹브라우저는 클라이언트가 입력한 계정정보를 서버로 전송한다. 이때, 웹브라우져에서 입력한 계정정보는 form 태크에 설정된 CGI, PHP 등의 웹페이지로 설정된 전송방식(예로, post 또는 get)으로 전송한다.

· 서버는 전송받은 계정정보를 확인하기 위해서 지정되었던 CGI, PHP 등의 웹페이지에서 기능을 수행하며, 첫번째로 데이터베이스에 로그인하고 쿼리를 날려서 계정 정보가 동일한지 확인한다.

· 계정정보를 확인했을 때 정상적인 사용자라면 로그인 화면을 클라이언트에게 전송한다. 이때, 서버는 클라이언트를 지속적으로 인식하기 위해서 쿠키나 세션 등을 이용할 수 있다.

· 클라이언트는 로그인한 웹페이지를 웹브라우져를 이용하여 볼 수 있다.

- 웹서버 구성요소 특징

· 웹서버 : IIS, Apache 등

· 웹애플리케이션 : PHP, CGI, JSP, ASP 등

· 데이터베이스 : 오라클, My-sql, MS-sql 등

2. 클라이언트 보안

2.1 윈도우 보안

2.1.1 설치 및 관리

o 핵심가이드
- 윈도우 운영체제별 설치 시 선택사항의 중요 개념 및 업데이트
- 윈도우 운영체제를 설치할 수 있는 파일시스템 종류 및 특징 이해
- 제어판 및 시스템 도구와 통신의 주요 기능에 대한 활용

(1) 윈도우 운영체제별 설치 및 업데이트

o 윈도우 운영체제별 설치시 중요사항
- 파티션 나누기
  · 파티션이란 하나의 물리적인 하드디스크에 논리적으로 분할 영역을 만드는 것을 말한다. 즉, 하드디스크에 칸막이 공사를 하여 하나의 하드디스크를 서로 별개의 하드디스크처럼 쓰기 위해서 분할하는 것이다. 파티션을 나누면 서로 다른 드라이브로 인식하기 때문에 설사 C 드라이브에 심각한 오류가 발생해도 D 드라이브에 있는 파일들은 안전하게 보존할 수 있으며, 윈도우를 2개 이상 설치해서 사용하는 멀티부팅이 가능하고, 중요한 데이터만 저장할 목적으로 파티션을 나누는 경우도 있다.
  · 하나의 하드디스크는 4개의 주 파티션을 포함할 수 있으며 각각의 주 파티션은 4개의 확장 파티션을 포함할 수 있다. 또한, 각각의 확장 파티션은 또 다시 확장 파티션을 포함할 수 있다.
  · 운영체제는 주파티션에 설치하여야 한다.
- 라이센스 모드 설정
  · 서버에 연결하는 클라이언트들을 위해 라이센스를 구입해야 하며, Per Server과 Per Seat 두 종류가 있다.
  · Per Server : 서버에 동시에 연결하는 사용자의 숫자 만큼의 라이센스를 구입해야 한다. 이것은 서버에 동시에 연결하는 사용자들의 숫자를 의미한다. 이 방식은 서버가 1대 있고 다수의 클라이언트 접속이 필요한 경우 주로 사용된다.

· Per Seat : 이 방식은 클라이언트 라이센스를 각 클라이언트에게 적용하는 것이다. 라이센스가 있는 클라이언트는 서버의 숫자에 상관없이 모든 서버에 접속할 수 있다.

- 도메인과 워크그룹 설정에 대한 특징 및 차이 이해

o 윈도우 파일시스템은 FAT 및 NTFS 파일시스템이 있으며, FAT는 MS에서 발표한 DOS에서 사용하던 파일 시스템이다. 나중에 Windows 95 OSR 버전부터 FAT32를 지원한다. 하드디스크에서 데이터를 저장하는 최소 단위는 섹터이지만 운영체제가 저장할 때는 파일을 기본 단위로 한다. 그런데 파일의 크기가 제각각 다르므로 전체 사용 중인 섹터의 크기도 달라진다.

- FAT 파일시스템에서는 하나의 파일을 저장할 때, 이 파일의 크기와 하나의 섹터보다 작거나 같은 경우는 섹터의 위치 정보만으로 데이터를 다시 찾아 읽을 수 있다. 그러나 하나의 섹터보다 클 경우에는 여러 개의 섹터에 나누어 저장된다. 때문에 각각의 섹터에는 다음 섹터의 포인터(물리저인 위치정보)가 같이 저장된다. 디스크에 저장된 파일 정보는 모두 FAT에 존재하기 때문에 이것이 손상되면 끝장이다. 따라서 FAT 파일 시스템은 2개를 가지고 있는데 이것을 FAT0, FAT1로 부른다. 즉 FAT1을 백업용으로 사용하는 것이다. 파일 시스템의 성능은 데이터 저장 위치에 대한 검색 속도에 따라 좌우되는데 FAT에서는 순차적인 검색을 한다. 400MB 이상인 하드디스크를 사용한다면 NTFS를 권장한다.
  - · FAT16 : 저용량(2GB이하) 하드디스크에 사용, DOS와 Windows 95에 지원
  - · FAT32 : 고용량(2GB이상) 하드디스크에 사용, Windows 95 OSR 이후부터 지원

- NTFS 파일시스템은 Windows NT Server의 전용 파일 시스템으로 MS-DOS, Windows 3.1/9x/Me에서는 사용할 수 없다. Windows 2000에서는 버전이 5로 업그레이드되었으며, 클러스터 정보를 이진트리로 구성하여 파일정보를 MFT(Master File Table)라고 하는 파일 테이블에 저장한다. 또한 데이터 검색시 순차적인 검색보다 검색 효율이 높은 이진 검색을 사용하고, 디스크 용량도 16EB(Exa Byte)까지 사용 가능하다. 디스크를 NTFS로 포맷하면 5MB의 공간이 파일 시스템의 정보공간으로 필요하므로 플로피에서는 사용할 수 없다. NTFS 파일 시스템으로 포맷을 하면 자체의 보안을 설정 할 수 있다. 로컬시스템에 로그온한 사용자에 대해 같은 폴더에 대한 액세스 권한을 각각 다르게 설정할 수 있다. 파일 시스템 자체가 압축을 지원하기 때문에 별도의 압축 프로그램을 사용하지 않아도 데이터를 압축하여 저장할 수 있다.

(2) 윈도우 운영체제 활용

o 제어판 활용
- 관리도구-로컬보안정책 : 계정정책, 로컬정책 등을 설정 가능
  · 암호정책 : 암호의 사용기간, 길이, 복잡도 등을 설정하여 시스템에 등록되는 암호 정책을 일괄적으로 적용 가능
  · 계정잠금정책 : 로그온 시도에서 다수 입력 값이 잘못 입력되면 계정을 잠금 수 있으며, 계정 크랙도구로부터 시스템을 보호할 수 있다.
- 관리도구-서비스
  · 윈도우의 서비스를 관리하며 불필요한 서비스를 제거하여 시스템 효율성 및 보안을 강화할 수 있다.
- 관리도구-이벤트뷰어
- 관리도구-컴퓨터관리
  · 장치관리, 로컬사용자 및 그룹 관리, 디스크 관리 기능
- 네트워크 및 전화접속 연결
  · TCP/IP 등록정보 이해
  · 윈도우에서 제공하는 네트워크 프로토콜 이해
- 프로그램 추가/삭제
  · 대부분의 프로그램은 프로그램을 설치하면 프로그램 추가/삭제 메뉴에 등록이 되고 삭제도 가능하다.
  · 프로그램을 설치할 때 프로그램 추가/삭제에 등록되지 않는 프로그램 종류
- 기타

o 시스템 도구와 통신 활용
- 시스템도구(보조프로그램) : 디스크정리, 디스크조각모음, 백업 기능 이해
- 통신(보조프로그램) : netmeeting, 전화걸기 기능 이해

2.1.2 공유자료 관리

o 핵심가이드
- NTFS 파일시스템 특징 이해
- 네트워크 드라이브의 개념 및 설정방법
- 공유폴더 사용권한 설정 및 옵션 활용
- 관리적인 목적상의 공유 이해

(1) 파일시스템 이해 : NTFS

o 파일시스템

- 파일 시스템이란 운영제제가 파일을 시스템의 디스크 상에 구성하는 방식을 말한다. 운영체제는 시스템의 디스크 파티션 상에 파일들을 연속적이고 일정한 규칙을 가지고 저장하는데 파일 시스템은 이러한 규칙들의 방식을 제시하는 역할을 한다. 또한 파일 시스템은 시스템 디스크나 파티션 그리고 파일 시스템의 형식을 말할 경우에도 쓰일 수 있다. 윈도우 운영체제 지원 파일시스템은 FAT, NTFS 파일시스템이 있다.

o NTFS 파일시스템

- NTFS는 윈도우 NT에서 지원하는 것으로 NTFS의 클러스터 크기는 512바이트, 1킬로, 2킬로, 4킬로바이트까지 사용자 지정이 가능하다. 파일크기 및 볼륨은 이론상으로 최대 16EB(ExaByte=10의 18승 바이트) 이나 실질적으로는 2테라바이트까지 지원한다. 또한, 이 파일시스템은 안정성, 자세한 사용자 제한, 보안성 등이 FAT32보다 향상된 기능을 가지고 있다.
- NTFS 보안은 NTFS 파일 시스템으로 포맷된 볼륨이나 파티션에 적용된다. 로컬 파일 시스템 보안을 제공하며, 네트워크를 통해 액세스하는 사용자에게도 적용된다.
- NTFS 볼륨의 기본 NTFS 보안은 공유보안과 같이 Everyone 그룹에 대해서 모든 권한이 '허용'이다. NTFS 볼륨이나 파티션의 기본 NTFS 보안을 변경하면 사용자마다 서로 다른 NTFS 보안을 적용시킬 수 있다.(로컬 파일 시스템 보안) 공유 보안에서는 파일 단위까지 보안을 적용시킬 수 없었지만 NTFS 보안에서는 가능하다. 더욱이 파일에 설정한 NTFS 보안이 폴더에 설정한 NTFS 보안보다 우선순위가 높기 때문에 더욱 강력한 보안을 설정할 수 있는 것이다.
- NTFS 시스템에 특정 사용자가 생성한 폴더나 파일에 대해서는 생성한 사용자에게 소유권한이 있다. 이것은 소유권을 가진 폴더나 파일에 대해서 NTFS보안을 설정할 수 있다는 의미이다. 그러나 Windows 2000 Server의 시스템 폴더에 대해서는 일반 사용자가 설정할 수 없다. 이것을 설정할 수 있는 사용자는 Aministrators 그룹과 Power Useers그룹의 구성원만이 가능하다.
- NTFS 폴더 사용 권한 종류는 폴더 또는 파일에 대한 해당 폴더의 [등록정보]의 [보안] 탭에서 확인 가능하다.
- NTFS 주요 기능

· 파일과 폴더 차원의 보안 : NTFS는 파일과 폴더에 대한 접근 제어 가능
· 디스크압축 : NTFS 압축 파일로 더 많은 저장공간 사용 가능
· 디스크 할당 : NTFS는 사용자별 디스크 사용공간을 제어 가능
· 파일 암호화 : NTFS는 파일에 대한 암호화 지원

(2) 네트워크 드라이브의 이해

o 네트워크드라이브는 대상 컴퓨터의 드라이브를 내 컴퓨터에서 네트워크드라이브로 설정하여 내 컴퓨터의 드라이브처럼 사용할 수 있는 기능이다.
o 설정방법
- 바탕화면의 내 컴퓨터에서 마우스 오른쪽버튼을 클릭하여 네트워크드라이브 설정을 클릭하면 기능을 이용할 수 있다.
- 명령프롬프트에서 'net use 드라이브명: \\ip\설정대상드라이브$'를 실행하고 계정 및 패스워드를 입력하면 설정 가능

(3) 공유폴더 보안

o 윈도우 NT 이상에서는 "관리목적을 위한 기본공유"라는 것이 기본적으로 존재한다. 즉, 명령프롬프트에서 net share를 실행하면 기본적으로 ADMIN$, IPC$, C$ 등이 공유가 된다. (컴퓨터의 드라이브가 C 드라이브 1개로 설정되어있는 경우)
- 공유해제 방법
· HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters 디렉토리에 DWORD 값을 추가하고 값을 0으로 설정한다.
o 공유폴더 사용권한 설정
- 폴더를 공유할 경우에는 공유되는 폴더의 등록정보에서 공유-사용권한에서 사용자 및 읽기, 변경, 모든 권한을 선택하여 설정할 수 있다.
o 윈도우탐색기의 도구-폴더옵션에서 보기 탭을 선택하면 '숨김파일 및 폴더 표시 안함'을 선택하여 숨겨진 파일의 공유설정을 방지할 수 있으며, 오파라인파일 탭을 이용하여 오프라인에서 네트워크 공유 파일을 이용할 수 있는 기능을 해제한다.

2.1.3 바이러스와 백신

o 핵심가이드
- 악성코드의 정의 및 범위를 이해하고 악성코드 종류별 특징과 대표적인 도구를 이해
- 컴퓨터 바이러스 명명법
- 안티바이러스 종류 및 자동업데이트, 자동치료, 정기점검 설정 등의 주요 기능 이해

(1) 악성코드에 대한 이해

o 악성코드 : 제작자가 의도적으로 다른 사람에게 피해를 주기 위해 만든 모든 악의적인 프로그램, 매크로, 스크립트 등 컴퓨터상에서 작동하는 모든 실행 가능한 형태

o 컴퓨터바이러스
- 정의 : 이론적인 정의로는 자신 또는 자신의 변형을 컴퓨터 프로그램이나 매크로, 스크립트 등 실행 가능한 부분에 복제하는 명령어들의 조합으로 정의되며, 실제적으로는 사용자 몰래 다른 곳에 자기 자신을 복제하는 프로그램, 악성 프로그램으로 통합되는 추세에 있다.
- 부트 바이러스 : 부트 영역에 감염되는 바이러스(플로피 디스크 / 하드 디스크) 감염 후 윈도우 환경에서는 치료가 어려우므로 도스 부팅 후 치료 필요
  · Brain 바이러스, Michelangelo 바이러스, Monkey 바이러스, Anti-CMOS 바이러스, WYX 바이러스 등
- 파일 바이러스 : 일반적으로 실행 가능한 프로그램 파일에 감염되는 바이러스이며, 윈도우에서는 다양한 형태의 실행 파일 존재, 다양한 형태의 파일에 감염
  · 도스용 파일 바이러스, 윈도우용 파일 바이러스, 매크로 바이러스
- 부트/파일 바이러스 : 부트 영역 및 파일에 모두 감염되는 바이러스
  · 나타스 바이러스, 절반 바이러스, 침입자 바이러스, 테킬라 바이러스 등 소수
- 매크로 바이러스 : 응용 프로그램에서 지원하는 매크로 기능을 이용해서 자신을 복제하는 능력을 가진 바이러스

o 트로이목마 : 백도어 종류도 트로이목마의 한 종류이며 트로이목마 프로그램은 바이러스와 달리 자기 복제 능력이 없으며 유틸리티 프로그램 내에 악의의 기능을 가지는 코드를 내장하여 배포하거나 그 자체를 유틸리티 프로그램으로 위장

하여 배포한다. 트로이목마가 설치되면 특정한 환경이나 조건 혹은 배포자의 의도에 따라 사용자의 정보 유출이나 자료파괴 같은 피해를 입을 수 있다

- 주요기능 : 원격조정, 패스워드 가로채기, 키보드입력 가로채기, 시스템 파일 파괴 등
- Netbus, Back Orifice 등

o 인터넷웜 : 네트워크/전자메일을 통해 자신을 복제하는 악성 프로그램으로 인터넷웜(Internet Worm)이라고도 함

- 전파방법
  · 전자메일 첨부파일
  · 정상적인 전자메일 첨부파일
  · 네트워크 쓰기 권한 악용
  · 서비스의 취약점 이용
- 대표적인 종류
  · I-Worm/Happy99, I-Worm/Hybris, I-Worm/Naked, I-Worm/Navidad, I-Worm/ExploreZip, I-Worm/Wininit 등
  · sql 슬래머

o 메일폭탄 : 메일폭탄(Mail bomb)이란 상대방에게 피해를 줄 목적으로 특정한 사람이나 특정한 시스템을 대상으로 수천, 수만 통의 전자 우편을 일시에 보내거나, 대용량의 전자우편을 지속적으로 보내 결국 해당 사이트의 컴퓨터시스템에 고장을 일으키는 기술이다.

o Joke & Hoax/Myth :

- Joke : 사용자에게 데이터 파괴 등의 구체적인 피해를 입히는 것은 아니지만 바이러스와 유사한 증상으로 사용자들이 놀라게 하는 각종 프로그램
  · Delete_Game, Format_Game, Cokegift, Puzzle 등
- Hoax/Myth : 컴퓨터 바이러스로 잘못 알려진 일종의 스팸(Spam) 메일 부작용 : 보안 의식 저하 -> 양치기 소년 효과
  · GoodTimes virus, Join the crew, Sulfnbk.exe 등

o 악성 스크립트 : 스크립트 기능을 이용해 제작한 악성 프로그램

- 배치파일, mIRC 스크립트, VBS(Visual Basic Script), JS(Java Script)

o 스파이웨어(Spyware) : 개인 정보 일부를 해당 SW 개발자가 알 수 있도록 제작/명시한 정상적인 프로그램

(2) 컴퓨터 바이러스 종류별 명명법과 주요 특징 이해

o 컴퓨터 바이러스 명명법

- 전세계 안티 바이러스 업체에서는 각기 다른 자기들만의 명명법을 가지고 있으며 서로 다른 명명법은 사용자들에게 혼란을 초래할 뿐만 아니라, 동일한 악성 코드라도 다른 이름 때문에 구분이 힘들다는 어려움이 발생하게 되었다. 이러한 문제점을 해결하기 위하여 1993년에는 CARO라는 명명법이 제안되었으나, 그 범위가 MS-DOS 바이러스에 국한되어 있고, 여러 가지 문제들로 인하여 통합되지는 못하였다. 악성코드 이름이 다른 이유는 발견 지역의 차이(주로 미주, 유럽, 아시아 순으로 발견됨), 근무시간대의 차이(시차가 큰 원인), 분석자 혹은 해당 기업간의 명명원칙 차이, 협의를 진행할 충분한 시간적 여유 부족, 시차 및 고객 피해방지를 위한 긴급대응 때문이기도 하다.
- CARO(Computer Anti-virus Research Organization) 명명법
  · 바이러스 이름은 기본적으로 4개 부분으로 나뉘며 각 부분은 점(Point, '.')으로 구분함
  · 각 부분의 이름은 "A-Za-z0-9$%&!'‘#-"등을 사용하여 구분함
  · Non-Alphanumeric 글자도 허용하나 사용은 제한하는 것을 권장함
  · 밑줄(Underscore, '_')은 가독성(readability)을 높이기 위하여 사용-글자수가 20글자 이상이 될 경우는 가급적이면 짧은 이름을 정함
  · 짧은 이름이 사용하기 편리함
- 악성코드 명명 원칙(모 기업의 예시)
  · 플랫폼은 접두어로, 분류명은 접미어로 사용함
  형식 : (접두어/)이름(.접미어)(.변형)
  * ( )는 필요시 생략 가능
  · 접두어는 보통 플랫폼과 형태를 지칭
  · 이름은 분석가 자체적으로 악성코드 명명원칙을 갖고 명명
  · 접미어는 웜(.worm)인지, 트로이목마(.trojan) 인지 표시
  · 바이러스가 아닌 트로이목마나 웜 변종의 경우 크기가 아닌 .B~.Z 사용
  · 변형의 경우 변경된 파일 크기 표시. 단, 동일한 종류에 동일한 크기를 갖고 있을 경우 .B~.Z 사용

[표 1-1] 바이러스 명명법 설명

접두어/	이름	.접미어	.변형
Win32/	Bagle	.worm	.12345 또는 .B~.Z

- 악성코드 명명 원칙(모 기업의 예시)
  · 하우리의 바이러스 명명법은 각각의 항목을 점(.)으로 구분을 하고, 총 3가지 항목으로 나누어져 있다. 각각의 항목은 악성 코드의 종류와 동작 플랫폼, 그리고 악성 코드의 명칭이 나열되어 있다.
  · 하우리의 바이러스 명명법 기본 형태
  형태(TYPE) . 플랫폼(OS).이름(NAME).크기(SIZE).변형정도(A,B…)
  · 형태(TYPE) : 형태는 일반적으로 악성 코드의 종류를 나타내는 항목이다. 그리고 일부 악성 코드의 경우에는 해당 항목을 생략하여 표기한다. (제외항목 - 바이러스, 매크로, 스크립트)
  · 플랫폼(OS) : 예로, DOS, Win32, Win2K, WinXP 등
  · 이름(NAME) : 악성코드 이름은 다음과 같은 내역에서 추출하는 경우가 대부분이며, 최초로 분석한 분석가가 만든 이름을 따라가는 경우가 대부분이다.
  · 크기(SIZE) : 악성 코드의 크기를 나타내는 부분이다. 그러나 악성 코드의 크기가 쉽게 변형될 수 있는 스크립트등은 해당 항목을 생략하여 표기한다.
  · 변형(A, B…) : 동일한 악성 코드가 발견된 순서대로 알파벳으로 표기하며, 원형의 경우에는 생략을 하는 경우가 대부분이다
  · 악성 코드 이름 예제 : I-Worm.Win32.Scold.28160

(3) 안티바이러스의 종류와 활용법

o 안티바이러스 종류
- 안철수연구소 : V3
- 하우리 : Virobot
- 시만텍 : Norton AV
- 기타

o 주요 공통 기능
- 업데이트 주기를 설정하여 자동업데이트 기능
- 바이러스 검사 주기를 설정하여 자동 검사 기능
- 실시간 감지기능의 설정 및 해제 기능

2.1.4 레지스트리 활용 [1급]

(1) 윈도우 레지스트리의 기본 개념과 활용

o 핵심가이드
- 레지스트리의 기본 기능 및 특징, 구조 이해
- 레지스트리의 백업과 복원 방법
- 레지스트리 관련 파일의 주요 특징 및 레지스트리 정보 내용 이해
  · SYSTEM.DAT, USER.DAT, SYSTEM.INI, WIN.INI

o 윈도우 95, 윈도 98, 윈도 NT 시스템에서 사용하는 시스템 구성 정보를 저장한 데이터베이스이며, 윈도우 환경과 프로그램에 관련된 사항 등이 저장된 system.dat, user.dat 파일이 바로 레지스트리이다. 윈도우와 프로그램에 관련된 사항은 레지스트리 외에도 win.ini, system.ini 파일을 비롯한 각종 INI 파일에도 저장되어 있으며 16비트 프로그램을 위한 여러 개의 INI 파일이 존재하긴 하지만 윈도우의 표준을 지키는 32비트 프로그램에 관련된 설정값은 모두 WINDOWS 디렉토리에 있는 레지스트리 파일에 저장된다. 레지스트리는 텍스트가 아닌 16진수로 되어 있어 INI 파일보다 속도가 빠를 뿐 아니라 전용 프로그램(레지스트리 편집기, regedit.exe)을 이용하지 않으면 고칠 수 없다. 그리고 모든 프로그램 설정이 하나의 레지스트리에 저장되기 때문에 관리가 용이하다.
- 윈도우 레지스트리는 총 6개로 구성되어 있다. [시작]-[실행]을 누른 뒤 빈칸에 'regedit'라고 입력하고 엔터를 누르면, 윈도의 레지스트리 내용을 보거나 편집할 수 있는 화면이 나온다. 이 화면이 바로 윈도의 [레지스트리 편집기]이다. 마치 윈도 탐색기를 실행한 것과 같은 화면이므로 쉽게 이해할 수 있을 것이다. 각각의 루트 키의 이름은 HKEY_로 시작된다. 이것은 'Key Handle'의 약자로 고유한 식별표지라고 생각하면 된다.
- 레지스트리 키 설명
  · HKEY_CLASS_ROOT : 파일의 각 확장자에 대한 정보와 파일과 프로그램 간의 연결에 대한 정보가 들어있다.
  · HKEY_CURRENT_USER : 윈도우가 설치된 컴퓨터 환경설정에 대한 정보가 들어있다.
  · HKEY_LOCAL_MACHINE : 설치된 하드웨어와 소프트웨어 설치드라이버 설정에 대한 정보가 들어있다.
  · HKEY_USERS : 데스크탑설정과 네트워크환경에 대한 정보가 들어있다.

· HKEY_CURRENT_CONFIG : 디스플레이와 프린터에 관한 정보가 들어있다.

o 레지스트리 백업 및 복구

- 백업 : 레지스트리 백업은 regedit.exe를 실행하여 활성화된 레지스트리 편집기에서 메뉴에서 백업을 실행하여 백업이 가능
- 복원 : 레지스트리 복원은 regedit.exe를 실행하여 활성화된 레지스트리 편집기에서 메뉴에서 복원을 실행하고 백업된 레지스트리 백업 파일을 선택한다.

o 관련파일

- 윈도우에서 레지스트리 정보는 \windows or \winnt 폴더에 USER.DAT, SYSTEN.DAT 라는 파일로 저장된다.
- 윈도우의 모든 시스템 정보를 백업 및 복구하기 위해서는 USER.DAT, SYSTEN.DAT, SYSTEN.INI, WIN.INI 가 있어야 한다.

(2) 레지스트리의 편집과 활용

o 핵심가이드

- Regedit를 이용한 레지스트리의 검색 및 수정 방법
- 트로이목마 서버 S/W 사례별로 레지스트리를 이용한 발견 방법, 컴퓨터에서 제거하는 방법

o 레지스트리 편집은 regedit.exe 또는 regedt32.exe를 사용하여 레지스트리를 편집할 수 있으며, 시작-실행에서 위의 명령어를 실행하면 윈도우탐색기와 유사한 창이 뜨고 편집하고자 하는 디렉토리를 찾아가서 값을 변경할 수 있다.

o 트로이목마 서버 S/W의 특징

- 트로이목마 서버 S/W가 설치되는 컴퓨터는 공격대상이 되어 중요한 정보가 공격자에게 전달된다. 이때 한가지 중요한 특징은 트로이목마 프로그램은 공격대상 컴퓨터에 설치 시 컴퓨터가 재시작될때도 트로이목마 서버 S/W가 자동으로 실행하도록 설정하는 것이 특징이다. 또한, 자동실행을 설정하기 위해서 주로 레지스트리에 등록하게 된다. 따라서, 이와 유사한 형태로 설치되는 트로이목마 서버 S/W는 레지스트리에서 검색하여 탐지 및 제거할 수 있다.

o 주요 트로이목마 사례

- Netbus 2.0
  · Netbus 2.0 트로이목마는 레지스트리에 자동실행 설정을 하므로 레지스트리 편집기에서 찾기 기능으로 다음과 같은 레지스트리를 검색하여 탐지가

가능하다.

· HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\NetBus Server

- NTRootkit : 레지스트리 자동실행 등록
- BAGLE : 레지스트리 자동실행 등록
- 기타

2.2 인터넷 활용 보안

2.2.1 웹브라우저 보안

o 핵심가이드

- 인터넷 익스플로러의 도구 메뉴의 인터넷 옵션에서 보안 기능, 개인정보 설정 기능, 내용, 연결 기능 및 설정
- 웹브라우저의 보안 취약점 이해 및 업데이트
- HTTP 프로토콜 이해 및 웹브라우저의 오류 메시지 이해

(1) 인터넷 익스플로러의 도구 메뉴의 인터넷 옵션

o 인터넷 익스플로러의 도구-인터넷옵션을 클릭하여 생성된 창에서 기능 이해

- 일반-임시 인터넷 파일
  · 쿠키 삭제 기능의 이해
  · 파일 삭제 기능의 이해 : 인터넷 사용시 웹사이트의 그림파일 등이 내 컴퓨터에 저장되는 원리 및 폴더 이해
- 보안
  · 인터넷 영역에서 기본수준으로 보안수준 설정
  · 인터넷 영역에서 사용자 지정수준 설정을 통하여 ActiveX, Java, 자바애플릿 등의 보안 설정을 통하여 악성스크립트 동작을 제거할 수 있다.
- 개인정보
- 내용
  · 등급관리자 : 등급을 통하여 인터넷 내용 제한 기능
  · 개인정보의 자동완성 기능의 이해 및 자동완성 정보 삭제
  · 인증서 활용

- 연결
  · VPN 설정
  · 프록시 서버 이해 및 프록시 서버 설정 방법
- 고급

(2) 웹브라우저의 보안 취약성 갱신

o 인터넷 익스플로러 보안 설정 방법
- 인터넷 익스플로러에서 java 애플릿 및 active 스크립팅 사용 기능 제거하거나 보안수준을 높이기
- 인터넷 익스플로러의 자동완성 기능 제거 등

(3) 웹브라우저 활용시의 오류 메시지 대처

o http 프로토콜 이해
- HTTP 프로토콜의 특성상 데이터를 요청하고 그리고 데이터를 받고 나면 바로 소켓 연결을 해제하게 된다. 지속적인 연결을 하고 있으면서 데이터를 주고 받는 것이 아니라 필요할 때마다 소켓을 연결하고 데이터를 받자마자 바로 연결을 끊어버리는 방식이 바로 HTTP 프로토콜의 연결 메커니즘이다. HTTP 1.0에서는 하나의 문서 내에 이미지가 존재한다면 문서를 받기위해서 연결설정을 하고 이미지를 받을 때 다시 연결설정을 하게 된다. 하지만 HTTP 1.1에서는 만약 연결설정을 한 후 하나의 문서 내에 포함 되어진 다른 이미지나 Object가 존재한다면 연결설정을 다시 하지 않고 연결되어진 소켓을 통해서 데이터를 이어서 받게 된다. 이렇게 함으로써 HTTP 프로토콜의 수행성능을 향상하게 되는 것이다. HTTP 프로토콜은 연결을 계속 유지하는 것이 아니라 작업을 마치면 바로 연결을 해제하는 방식으로 동작한다. 이러한 Connection의 지속성이 없기 때문에 각각의 클라이언트를 구분할 수 없다는 것은 HTTP 프로토콜의 가장 큰 단점이다. 그러나, 보다 많은 사용자에게 보다 많은 서비스를 할 수 있다는 것이다. HTTP는 한번의 연결로 필요한 작업만을 하고 바로 연결을 해제 해버린다. 이러한 HTTP의 단점을 극복하기 위해서 몇 가지의 방법이 제공되어진다.
  · URL Rewriting
  · Hidden Form Field

· Cookie

· Session

- http 프로토콜 버전

· HTTP 0.9 read only(초기 모델)

· HTTP 1.0 read, input, delete,

· HTTP 1.1 수행성능향상

o http 프로토콜 상태코드 이해

- 트랜잭션이 성공한 경우

· 200 : request가 성공적으로 완료되었음

· 201 : request가 POST method이었으며 성공적으로 완료되었음

· 202 : request가 서버에 전달되었으나 처리 결과를 알 수 없음. 배치 처리를 요한 경우

· 203 : GET request가 실행되었으며 부분적인 정보를 리턴하였음

· 204 : request가 실행되었으나 클라이언트에게 보낼 데이터가 없음

- 트랜잭션의 redirection

· 300 : 요구된 request가 여러 위치에 존재하는 자원을 필요로 하므로 response는 위에 대한 정보를 보낸다. 클라이언트는 가장 적당한 위치를 선택하여야 함

· 301 : request에 의한 요구된 데이터는 영구적으로 새로운 URL로 옮기어졌음

· 302 : request가 요구한 데이터를 발견하였으나 실제 다른 URL에 존재함

· 304 : If-Modified-Since 필드를 포함한 GET method를 받았으나 문서는 수정되지 않았음

- 오류메시지

· 400 : request의 문법이 잘못되었음

· 401 : request가 서버에게 Authorization: 필드를 사용하였으나 값을 지정하지 않았음. 서버는 WWW-Authenticate response header를 통해 가능한 인증 스킴을 보낸다.

· 402 : request가 요구한 일은 비용이 요구되지만 request header의 Chargeto 필드에 아무값도 보내지 않았음. 현재는 구현되지 않았음

· 403 : request는 금지된 자원을 요구하였음

· 404 : 서버는 요구된 URL을 찾을 수 없음

· 405 : 클라이언트는 자원을 액세스하기에 부적합한 method를 이용하였음.

· 406 : 요구된 자원을 발견하였으나 자원을 타입이 request header의 accept: 필드와 일치하지 않아서 전송할 수 없음

· 410 : 요구된 자원은 더 이상 활용가능하지 않음

· 500 : 서버에 내부적으로 오류가 발생하여 더 이상을 진행할 수 없음

· 501 : 요청된 request는 합법적이나 서버는 요구된 method를 지원하지 않음

· 502 : 클라이언트는 다른 서버(보조서버)로부터 자원 액세스를 요구하는 서버에 자원을 요구하였으나 보조 서버가 유효한 응답을 전달해오지 않았음

· 503 : 서버가 바쁘기 때문에 서비스를 할 수 없음

· 504 : 502의 오류와 유사하나 보조 서버의 응답이 너무 오래 지체되어 트랜잭션이 실패하였음

2.2.2 메일 S/W 보안

(1) Outlook 및 Outlook Express 보안

o 핵심가이드
- Outlook의 주요 공격 대상 : 주소록, 메일 폴더, Visual Basic 파일
- 메일 필터링 기법
- 첨부 파일 보안
- PGP 활용

o Outlook의 주요 공격 기술 이해
- 공격자에 의해 운영되는 뉴스그룹을 사용자가 방문했을 때 Outlook Express 이메일 프로그램에 설치되어 사용자 컴퓨터를 컨트롤 할 수 있는 공격기술
- 공격자가 악성스크립트를 메일에 첨부하여 보내면 수신자가 메일을 확인하거나 읽는 순간 악성스크립트에 의해 공격당할 수 있음.

o 메일 필터링 기법
- 도구-메시지 규칙 기능을 이용하여 메일, 뉴스, 차단할 보낸사람목록의 기능을 이용하여 제목, 내용, 첨부파일 등에 대한 메시지 규칙을 설정하여 메일 필터링이 가능하고 메일주소 또는 도메인으로 메일을 차단 가능

o 첨부 파일 보안
- 메일의 첨부파일을 이용한 웜 및 악성스크립트를 이용한 공격이 가능하므로 송신자 메일주소 및 메일제목을 확인하여 불필요한 메일을 삭제하는 것이 우선

o PGP 활용

- PGP는 사용자가 작성한 이메일의 내용과 첨부되는 파일을 암호화하여 이메일 수신자만이 그 내용을 볼 수 있도록 하는 기밀성을 제공해 주며, 전자서명 기능을 제공하여 송신자라고 주장하는 사용자와 이메일을 실제로 보낸 송신자가 동일인 인가를 확인해준다.
- 특징
  - 인증 받은 메시지와 파일에 대한 전자 서명 생성과 확인 작업
  - 키 관리를 Graphic Interface로 지원
  - 공개키를 4096 비트까지 생성할 수 있으며, RSA와 DSS/Diffie-Hellman 등 두 가지 형태의 공개키 생성 가능
  - 공개키 서버와 직접 연결되어 있어 공개키 분배 및 취득이 간편
- 활용방법
  - Setup 프로그램을 이용하여 설치하면 최초 사용자는 개인키/공개키 쌍을 생성하게 하고 개인키는 안전하게 자신의 컴퓨터에 패스워드로 암호화하여 저장하고 공개키는 다른 사용자들이 사용할 수 있도록 분배해 주어야 한다. 이때, PGP는 다른 사용자들이 여러분의 공개키를 가지고 있어야 여러분에게 암호문을 전송할 수 있고, 여러분이 생성한 전자서명을 확인할 수 있다. 공개키를 분배하는 방법은 크게 다음의 3가지로 나눌 수 있는 데, 공개키 서버에 등록하는 방법, 이메일의 내용에 공개키를 포함시키는 방법, 별도의 텍스트 파일에 복사하는 방법이 있다. 공개키를 분배하는 방법들 중에서 가장 좋은 방법은 공개키 서버에 등록시켜 놓는 방법이다. 세계적으로 다수의 공개키 서버가 존재한다. 이중에는 PGP 사에서 제공하는 공개키 서버도 포함된다.
  - 공개키를 등록하고 이후에 송신자가 암호화해서 메일을 송신하면 나의 컴퓨터에 저장되어있는 개인키를 선택하여 복호화하고 메일내용을 볼 수 있다.

(2) 웹기반 메일 서비스 보안

o 핵심가이드

- 웹기반 메일 서비스의 보안 취약성 및 공격기술 개념 이해
- 코드 기반 공격
- SSL 활용
- PGP 활용

o 웹기반 메일 서비스의 보안 취약성 이해

- XSS 공격 개념 및 대처방법
- 계정 크랙 공격 개념
- 클라이언트 측에서 동작하는 스크립트 공격
- 스니핑 도구에 의한 전송되는 정보 유출(ID/패스워드 및 메일내용 등)
- 기타

o 코드 기반 공격

- 악성코드를 전파 및 공격대상에 설치하기 위해서 웹메일을 이용하는 사례가 증가하고 있다. 인터넷익스플로우를 이용하여 웹메일 사용 시에 메일을 읽거나 메일보기를 선택하는 경우 사용자 컴퓨터에 악성코드가 실행되면서 다양한 공격이 가능하게 된다.
  · Active X를 이용한 공격
  · 자바스크립트를 이용한 공격
  · 기타
- 공격의 유형
  · 해킹프로그램 설치 및 레지스트리에 자동실행 설정
  · 인터넷익스플로우 초기화면 변경
  · 특정 사이트 팝업창 지속적인 디스플레이
  · 기타

o SSL 활용

- SSL은 넷스케이프에서 개발된 프로토콜로서 네트워크 통신 및 인터넷 사용자에게 안전한 정보를 교환하기 위한 보안 프로토콜로써 전자상거래 및 은행 거래시에 많이 활용되고 있다.
- 특징
  · TCP/IP 프로토콜에서 트랜스포트 레이어 바로 위에서 보안기능을 수행한다.
  · SSL v3.0 이후 IETF에서 표준화되어 TLS로 명명
  · SSL 구성은 핸드쉐이크 프로토콜, change cipher spec, alert 프로토콜, record 프로토콜로 각기 기능을 수행한다.
- 보안기능
  · 사용자 상호 인증-웹사이트 이용시 사이트 인증
  · 데이터 기밀성
  · 메시지 무결성
- 구성요소 이해

· handshake protocol : 서버와 클라이언트간에 인증을 허용, 암호 및 MAC 알고리즘을 교환, 암호화 키들을 SSL 레코드에서 보내진 데이터를 보호하기 위해 사용

· Record protocol : 모든 상위 프로토콜 메시지의 Encapsulation 수행하고 SSL 연결을 위해 보안 서비스 제공(기밀성, 무결성한다. 레코드 프로토콜은 단편화, 압축, MAC 값 삽입, 암호화, SSL 헤더삽입의 과정으로 데이터를 캡슐화한다.

· Change cipher spec : hand shake 과정에서 end-to-end 간의 Cipher-Suite 이 설정되었음을 의미한다.

· alert protocol : hand shake 과정에서 end-to-end 간의 error 발생시

o PGP 활용

- PGP를 가장 편리하게 사용할 수 있는 방법은 현재 널리 사용되고 있는 이메일 어플리케이션과 PGP를 연계하여 사용하는 plug-in을 이용하는 것이다. 이러한 방법을 사용하면 사용자들은 이메일을 작성하거나 읽을 때 단지 마우스를 클릭하는 것만으로도 암호화/서명, 복호화/서명확인 등의 작업을 수행할 수 있다

2.2.3 기타 인터넷 S/W 보안

o 핵심가이드

- ICQ, IRC의 보안 취약성 및 대처 방안
- Procmail, Sanitizer, Inflex의 기능 및 동작원리 이해

(1) ICQ, IRC의 보안 취약성과 대처방법

o ICQ, IRC의 보안 취약성

- 인스턴트 메시징 시스템은 암호화되지 않은 상태에서 다른 사람과의 파일 교환이 가능하다. 그러나 이러한 파일 전송은 혼합 보안위협뿐 아니라 바이러스, 웜, 트로이목마 프로그램 등의 확산을 위해 악용
- 인스턴트 메시징은 Visual Basic, JavaScript, 특정 스크립트 코드 또는 메시징 클라이언트에서 다양한 기능들을 제어하기 위한 기본 윈도우 프로그램 등 스크립트를 작성할 수 있는 스크립팅 기능을 제공한다. 그와 같은 스크립트들은 다른 유저와의 자동 연결, 파일 전송, 프로그램 설정 변경 및 잠재된 악의적

활동 개시 등을 IM 클라이언트에 명령할 수 있다

(2) 메일 서버 스캐너의 주요 기능과 사례

o Procmail과 Sanitizer

- Procmail"은 강력한 메일 프로세서로 메일 메시지의 헤더와 본문에서 특정 정보를 찾아 정의된 규칙에 따라 적절한 조치를 수행하는 프로그램이며, sanitizer라는 procmail ruleset은 앞서 설명한 E-mail을 이용한 모든 공격에 효과적으로 대응할 수 있도록 해준다.

o Inflex 등

- Inplex는 메일서버에서 로컬이나 외부로 나가는 E-Mail을 검사하여 E-mail에 대한 In-Outbound 정책을 새울 수 있게 해주는 도구이다. 이러한 In-Outbound 정책기능을 통하여 관리자는 최근의 바이러스나 인터넷 웜이 첨부된 메일을 필터링할 수 있도록 해준다. 또한 임의 파일 이름과 파일 유형에 대하여 검색하고 필터링하는 기능을 제공하여 Anti-virus 패키지에 의해 탐지되지 않는 바이러스로부터의 공격에 대응할 수 있도록 해준다. Procmail을 이용한 필터링보다는 설치 및 운영이 쉬운 반면, Inflex는 첨부파일만을 필터링할 수 있다

2.3 공개 해킹도구에 대한 이해와 대응

2.3.1 트로이목마 S/W

o 핵심가이드

- 트로이목마 프로그램의 기능 이해
- 트로이목마 프로그램의 공격 유형 및 탐지/제거 방법 이해
- 최신 트로이목마 S/W의 동작원리 및 특징, 종류별 대표적인 도구

(1) 트로이목마의 개요

o 트로이목마 프로그램은 바이러스와 달리 자기 복제 능력이 없으며 유틸리티 프로그램 내에 악의의 기능을 가지는 코드를 내장하여 배포하거나 그 자체를 유틸리티 프로그램으로 위장하여 배포한다. 트로이목마가 설치되면 특정한 환경이

나 조건 혹은 배포자의 의도에 따라 사용자의 정보 유출(Backdoor)이나 자료파괴 같은 피해를 입을 수 있다.

o 트로이목마 기능(일반적인 기능)

- 원격 조정 : 원격 조정은 해커가 트로이목마에 감염된 시스템을 통해서 악의적인 행위를 할 수 있다. 해커는 감염된 시스템의 파일, 데이터 등 시스템에 관한 모든 것을 완벽하게 조정할 수 있다.
- 패스워드 가로채기 : 트로이목마에 감염된 시스템에 존재하는 캐시된 패스워드를 찾아내는 것이다. 주로 메신저, 인터넷에 존재하는 웹사이트, 기타 응용프로그램 사용시에 요구되는 사용자 계정과 패스워드를 사용자 모르게 공격자의 이메일 주소로 전송한다.
- 키보드 입력 가로채기 : 시스템에서 사용자가 입력하는 키보드 입력을 임의의 로그파일에 복사한 후 해커가 설정해 놓은 특정한 이메일 주소로 전송하거나 실시간으로 전송한다.
- 시스템 파일 파괴 형태 : 감염된 시스템에 있는 파일이나 데이터들을 삭제하는 기능을 가지고 있다.

o 트로이목마 활용

- 대부분의 트로이목마 프로그램은 서버프로그램과 클라이언트 프로그램이 있으며, 서버프로그램은 공격대상 컴퓨터에 설치가 되며, 클라이언트 프로그램은 서버프로그램에 접속하여 공격을 수행할 때 활용하는 것으로 공격자가 이용하는 프로그램이다.

o 트로이목마 탐지 방법

- 안티바이러스 프로그램에 의한 탐지
- 레지스트리를 검사하여 자동실행 설정된 내용 검사
- 사용자의 컴퓨터에서 사용하지 않는 포트가 열려져 있는지 검사
- 사용자의 컴퓨터에 설치하지 않은 프로그램이나 파일이 설치되었는지 검사
- 기타

(2) 트로이목마 S/W 사례별 이해

o NetBus

- 넷버스는 file manager, registry manager, Application Redirect, 화면 캡쳐, 키보드입력정보 보기 등의 기능
- 서버프로그램의 접속패스워드 설정 기능

- 서버프로그램의 포트변경 기능

o Back Orifice

- 백오리피스는 CDC라는 해킹그룹에서 만든 해킹도구로 파일시스템의 모든 파일에 대한 접근, 프로세스 생성/삭제, 시스템 패스워드 유출, 키보드 모니터링, 네트워크 자원의 공유지정, 파일조작, 레지스트리조작 등의 기능
- 서버프로그램의 접속패스워드 설정 기능

o School Bus 등

- 패스워드 유출, 캐쉬영역의 패스워드 추출, 파일관리, 키보드 입력 모니터링 등의 기능
- 서버프로그램의 접속패스워드 설정 기능

o ackcmd

- 윈도우 2000을 위한 특수한 원격 명령 프롬프트. TCP ACK 세그먼트만 사용해서 통신을 하므로 어떤 경우 방화벽을 통과하는 연결이 가능하다.
- 즉, netstat -an 명령어로 연결세션정보를 얻기 어렵다.

o 루트킷

- 루트킷의 목적은 자신과 다른 소프트웨어를 보이지 않게 숨기고 사용자가 공격자의 소프트웨어를 인지하고 제거할 가능성을 피하는 것이다. 루트킷은 파일 서버, 키로거(keylogger), 봇넷(botnet) 및 재전송 메일(remailer)을 포함하여 거의 모든 소프트웨어를 숨길 수 있다. 따라서, 대개 감지할 수 없으며 제거하기도 거의 불가능합니다.
- 루트킷 기능
  - ·트래픽이나 키스트로크를 감시
  - ·시스템에 트로이목마 프로그램 설치
  - ·로그파일 수정
  - ·프로세스나 파일 숨김 기능
  - ·자동실행 설정
  - ·기타
- 루트킷 종류
  - ·윈도우용 : FU-Rootkit, Hxdef100, NTRootkit 등등
  - ·리눅스용 : Suckit, lrk4, lrk5, adore 등
- 루트킷 탐지 : 안티바이러스 프로그램이나 전용도구를 이용하여 탐지 및 제거
  - ·안티바이러스 프로그램에 의한 탐지
  - ·일반적인 행동 기반의 루트킷 감지 소프트웨어 : Rootkit Revealer 등

2.3.2 크래킹 S/W

o 핵심가이드

- 크래킹 개념 및 대응 기술
- 크래킹 S/W의 공격 방법 및 특징

(1) 크래킹의 개요

o 크래킹은 해킹과 비교하여 악의적인 목적을 가지고 시스템에 침입하는 행위를 말하며, 다른 의미로 쉐어웨어 프로그램을 정식버젼으로 변환하는 행위를 의미하기도 한다.

o 해킹도구로써의 크래킹 기술은 사용자의 ID, 패스워드를 찾는 도구로써 활용되고 있는데 이때의 공격원리는 ID, 패스워드를 대입하여 맞는지, 틀리는지 지속적으로 수행해보는 방법이다.

(2) 크래킹 S/W 사례별 이해

o WWWhack

- 웹서버의 로그인 ID와 패스워드, 접속계정의 ID와 패스워드, FTP의 ID와 패스워드 그리고 POP의 ID와 패스워드를 크랙하는 도구

o Golden Eye, Webcrack 등

2.3.3 포트 스캐닝 S/W

o 핵심가이드

- 포트스캐닝의 목적 및 원리
- 포트스캐닝 S/W의 종류 및 기능

(1) 포트스캐닝의 개요

o 포크스캐닝은 공격자가 공격대상 시스템의 열려진 포트를 스캐닝하는 것으로써 OS 판별, 공격경로 선택 등을 위해서 수행하는 절차이다.

- 포트번호는 인터넷이나 기타 다른 네트워크 메시지가 서버에 도착하였을 때, 전달되어야 할 특정 프로세스를 인식하기 위한 방법이다. TCP와 UDP에서, 포트번호는 단위 메시지에 추가되는 헤더 내에 넣어지는 16 비트 정수의 형태를 갖는다. 이 포트번호는 논리적으로는 클라이언트와 서버의 전달계층 사이를, 그리고 물리적으로는 전달계층과 인터넷계층 사이를 통과하여, 계속 전달된다. 포트번호는 0-65535번 까지가 있으며, 애플리케이션용으로 지정되어있는 포트번호(well-known)는 0-1023, 그 외 포트는 연결시 일시적으로 부여되는 포트번호이다. 예를 들면, 클라이언트가 인터넷 서버에 하는 요청은, 호스트의 FTP 서버에 의해 제공되는 파일을 요청하는 것일 수 있다. 원격지의 서버 내에 있는 FTP 프로세스에 사용자의 요청을 전달하기 위해, 사용자 컴퓨터에 있는 TCP 소프트웨어 계층은 요청에 부가되는 16 비트 정수의 포트번호 내에 21 (FTP 요청과 관련하여 통상 사용되는 번호이다) 이라는 포트번호를 확인한다. 서버에서, TCP 계층은 21이라는 포트번호를 읽고, 사용자의 요청을 서버에 있는 FTP 프로그램에 전달할 것이다.
- Port scanner에 의한 목적지 시스템에 대하여 Listen 되어 있는 port(접속 가능한 port)를 찾기 위한 행위이다. 공격자들은 Target 시스템이 alive 되어 있는지 확인(주로 ping을 이용하며, 네트워크 단위에서는 ping sweep을 한다)하고, 열려진 port를 탐색한 후 취약점 scanner(Nessus, Internet Scanner 등)를 이용하여 취약점 분석을 한다. 그 후에 시스템의 취약점을 이용하여 공격을 하게된다.
- 포트스캐닝은 특정 포트에 대해서 3Way hand-shaking가 확립되면 포트가 열려진 것을 확인할 수 있다.

(2) 포트 스캐닝 S/W 사례별 이해

o NMap
- 다양한 방식을 이용한 포크스캐너
  · TCP connect() scan : 3Way hand-shaking을 이용한 scanning 이다. 완전한 TCP 연결을 하여 Port의 open/close 상태를 확인하기 때문에 시스템에서 쉽게 탐지가 될 수 있다.
  · TCP SYN scan : Half-open scan 또는 Stealth scan으로 불리기도 하며 완전한 TCP 연결을 맺지 않고, 대상 포트로 SYN 패킷을 전송하여 SYN/ACK을 받으면 open 상태, RST/ACK를 받으면 close 상태이다. SYN scan은

half-open 연결을 통하여 포트의 open/close 상태를 확인하기 때문에 TCP connect() scan에 비하여 비밀스러운 연결로 시스템에 로그가 기록되지 않는다. TCP를 이용한 scanning 중 scan 속도가 TCP connect() scan 보다 빠르기 때문에 가장 많이 사용하는 방법이다.

· TCP FIN, Xmas Tree, NULL scan : 이 세가지 scan기법은 Stealth scan이라고 불리기도 하며 UNIX 계열 시스템에 대해서만 사용할 수 있다. 만약, TCP FIN, Xmas Tree, NULL scan으로 scanning을 하여 결과가 없다면 해당 시스템은 Windows 계열의 시스템이라고 판단할 수 있다. TCP FIN scan은 TCP flag의 FIN을 활성화 하여 대상 포트로 패킷을 전송하고, Xmas Tree scan은 TCP flag의 FIN, URG, PUSH을 활성화 하여 대상 포트로 패킷을 전송한다. NULL scan은 TCP flag를 모두 비활성화 하여 대상 포트로 패킷을 전송한다. 세 scan 모두 포트가 close 상태이면 RST 패킷을 되돌려 보낸다(RFC 793). Open 상태이면 패킷을 무시한다.

· UDP scan : UDP scan은 UDP를 사용하는 열린 포트를 찾기 위한 scanning 이다. 대상 포트로 UDP 패킷을 전송하고 대상 포트로부터 "ICMP Port Unreachable" 메시지를 받으면 close 상태이며 메시지가 오지 않으면 open 상태이다. UDP scan은 정확도가 떨어지기 때문에 결과에 대해서 신뢰를 할 수 없는 scan이다. Close상태는 명확하게 포트가 닫혀 있다는 것을 알 수 있지만 Open 상태는 UDP protocol의 특성(비연결형 protocol)상 네트워크의 상태나 Router, Switch등에 의한 Filtering에 의해서 응답이 없을 수 있기 때문에 특히, open상태는 정확도가 떨어진다고 할 수 있다.

o Superscan, Aat4xx 등

2.3.4 키로그 S/W

o 핵심가이드
- 키로그 S/W의 기능 및 대처 방법
- 주요 키로그 프로그램 종류 및 특징

(1) 키로그의 개요

o 키로그 프로그램은 설치된 컴퓨터에서 키보드로 입력한 정보를 로그로 남기는 프로그램이며, 기능이 업데이트된 키로그 프로그램은 키보드 입력 뿐만 아니라

윈도우를 이용한 프로그램 사용, 인터넷 익스플로러를 이용한 인터넷접속 정보 등도 로그로 남기며, 로그파일을 실시간으로 공격자에게 전송하거나, 설정된 메일 및 메신저로 지정된 시간에 로그파일을 자동 전송하는 기능도 있다.

o 키로그 프로그램 탐지 방법
  - 안티바이러스 프로그램에 의한 탐지
  - 키로그 전용탐지도구에 의한 탐지
  - 특정 문자열을 타이핑한 후 파일의 내용에서 타이핑한 문자열 검색

(2) 키로그 S/W 사례별 이해

o Keylog25은 설치된 컴퓨터에서 자판을 입력한 정보를 파일에 로그로 남김.

o SK-Keylog
  - 키보드 입력을 로그로 남김
  - 지정된 시간에 로그파일을 설정된 공격자 메일로 자동 전송 기능 포함.

o Winhawk 등

2.3.5 기타 S/W

o 핵심가이드
  - 누킹의 기능
  - 폭탄메일 종류 및 기능

(1) 누킹 S/W : Vconnect, Cgsioob 등

o 누킹(nuking)이란 레지스트리, 키 파일, 파일 시스템 등을 훼손하여 시스템을 사용 불능상태로 빠뜨리는 프로그램으로 ‘blue bomb’ 혹은 ’WinNuke’이라고도 알려져 있다.

(2) 폭탄 메일 S/W

o 특정 사람에게 한꺼번에 많은 양의 메일을 전송하는 것. 주로 상대방의 메일 용량을 초과시켜 많은 피해를 줌

o Anonymail은 익명으로 메일을 보낼 수 있는 프로그램이다. 일반적으로 메일을

작성해서 전송하면 자신의 메일 주소도 같이 전송되지만, anonymail 프로그램은 자신의 메일 주소를 임의로 작성해서 보낼 수 있도록 제공한다.

o QuickFyre, Avalanche, eremove 등

2.4 도구활용 보안관리

2.4.1 PC용 보안도구 활용

o 핵심가이드
- BlackICE, BO2K Server Sniper, BO Remover, NoBo, NoNuke, Visual Route 등의 기능 이해

(1) 공개해킹도구에 대한 대응 S/W

o BlackICE(PC 프로텍션 버전)
- 외부에서 자신의 컴퓨터에 접근하는 것을 감시, 제어(차단, 허용)하는 프로그램
- 기능
  - ㆍ침입차단 기능 : IP 및 포트 기반으로 접근 허용, 차단 등으로 필터링
  - ㆍ애플리케이션 보호 기능 : 애플리케이션 실행을 모니터링하여 실행 허가/거부를 선택할 수 있으므로 악의적인 사용을 모니터링할 수 있다. 설치 시 전체 애플리케이션 파일에 대한 베이스라인(baseline) 설정을 함으로써 설치 시간이 길고, 주로 쓰는 애플리케이션에 대해서도 일일이 허용 여부를 물어보는 등 불편함을 발생
  - ㆍ침입탐지 패턴을 보유한 IDS(침입 탐지) 기능 : 침입탐지를 기반으로 한 자동 차단 기능이 특징이다. 보통의 방화벽이 갖고 있는inbound(유입)/outbound(유출) 트래픽에 대한 차단 위주의 기본 정책 보호 기능 외에 일반 상용 IDS에 맞먹을 정도의 강력한 침입탐지 엔진을 장착하고 이를 침입 차단 기능과 연동한다.

o BO2K Server Sniper
- Back Orifice 탐지 도구

o BO Remover, NoBo
- Back Orifice 탐지 도구 및 제거도구

o NoNuke

- Nuke 방지 도구

o Visual Route

- IP나 도메인을 이용하여 대상 컴퓨터까지의 라우팅 경로 및 네트워크 상태를 확인하는 도구로써 공격자를 추적시에 활용 가능

o 기타

2.4.2 PC용 방화벽 운영 [1급]

o 핵심가이드

- PC용 방화벽 기능의 주요 기술 개념 이해
  - ㆍ블로킹(포트, IP 주소), 접근 제어 목록(ACL), 실행 제어 목록(ECL), 침입 탐지 기능, False Positive
- PC용 방화벽의 기본 활용법 이해

(1) PC용 방화벽의 기본 개념과 용어

o 블로킹(blocking) : 포트, IP 주소

- 나의 컴퓨터를 기준으로 들어오고 나가는 패킷을 확인하여 IP 헤더의 소스 IP/목적지 IP와 TCP 헤더의 송신자 포트/수신자 포트 등을 기반으로 패킷을 필터링할 수 있다.

o 접근 제어 목록(ACL)

- ACL은 접근제어 정책을 설정하여 접근을 제어하는 것으로 시스템에서는 파일이나 폴더에 대해서 ACL을 설정하여 보안을 수행할 수 있으며, 네트워크 보안 시스템에서는 서비스에 대한 액세스나 거부를 제어하는 수단으로 자주 사용되는 방법이다. 이것은 이용 가능한 서비스 리스트이므로 각 서비스에 대해서 이용할 수 있는 호스트의 리스트가 기술된다.

o 실행 제어 목록(ECL)

- 애플리케이션에 대해서 사용자도 모르게 악의적인 사용이 될 수 있으므로 애플리케이션 실행 정책을 설정하여 악의적인 사용을 모니터링할 수 있다.

(2) PC용 방화벽의 종류와 활용법

o ZoneAlarm 활용

- 존알람 프로그램은 설치된 pc에서 입출력되는 모든 데이터통신에 대해 허용 여부를 설정할 수 있으며 실행되는 프로그램별 혹은 내부, 외부 네트워크별로 구분하여 통신가능여부를 설정할 수 있는 등의 다양한 기능을 제공한다. 존알람의 단점이라면 이러한 세세한 설정이 가능한 만큼 설치 후 최초 설정이 번거롭다는 것이다. 존알람의 기능은 크게 다섯가지로 제공된다.
- Alerts
  - Alerts 에서는 사용자의 컴퓨터에 외부로부터의 접근을 금지하거나 미리 상대방에게 경고성 메시지를 보내는 창이 있고, 이 내용들을 기록할 것인가 하는 옵션 선택과 함께 접속된 현재 자신의 포트를 방어하고 있는 상황을 체크할 수 있다.
- Lock
  - Lock 기능은 모든 인터넷에 접근이 가능하지만, STOP을 누르면 모든 인터넷 접속 자체가 완전히 차단된다.
- 보안기능
  - Security 설정은 인터넷 사용에 있어 보안의 범위를 설정하는 것으로 크게 로컬과 인터넷으로 나눌 수 있다. 기본적으로 로컬은 미디엄(medium), 인터넷은 하이(high)로 설정되어 있다.
- 프로그램 보호 기능
  - 존알람에서 가장 유용하면서도 번거로운 기능중의 하나이다. 존알람을 사용해본 사용자는 설치 후 pc외부와의 통신에 대한 설정을 하도록 존알람에서 보여주는 경고문 을 보게 되며 외부와의 통신을 취하는 프로그램은 모두 통신허용여부를 설정해야 하기 때문이다.
- 설정 기능
  - Configure 메뉴에서는 인터넷 사용 중에 존알람의 상태를 설정하는 것으로 항상 모든 창의 위치하거나 시스템 시동 시 자동으로 실행되도록 할 수 있다. 또한 프로그램 업데이트가 됐다면 자동으로 업그레이드 된다.

2.4.3 PC실 관리 및 보안 [1급]

o 핵심가이드

- PC 실습실 관리 기능
- PC 실습실 관리를 위한 S/W, H/W 사례별 이해

(1) PC 실습실 관리 기능 이해

o 시스템 장비 관리
- 실습실의 장비의 노후 및 결함 등에 대한 관리 및 전체적인 시스템 사양 등에 대한 지속적인 관리
- OS 및 필수적인 소프트웨어를 지속적으로 관리 및 정기적으로 다시 설치할 수도 있다.

o 불법 소프트웨어 제거
- 실습실은 동일한 환경에서 다수의 사용자가 사용할 수 있으므로 사용자들이 불법적인 소프트웨어를 자유롭게 설치할 수 있으므로 불법 소프트웨어 검사 및 제거를 수행행야 한다.

o 바이러스 및 해킹 등의 방지
- 실습실은 OS와 안티바이러스 프로그램 등의 정기적인 업데이트 및 보안프로그램 설치 및 유지

o 기타

(2) PC 실습실 관리용 S/W 사례별 활용 이해

o PC 프로그램 정기적인 재설치
- Norton ghost를 이용하여 동일한 시스템 환경을 다수의 컴퓨터에 동시에 설치 가능

o PC 원격 중앙 관리 프로그램
- OS 및 안티바이러스 프로그램 등의 정기적인 업데이트 및 불법적인 소프트웨어 관리 등을 위해서 원격 중앙 관리 프로그램 사용 가능

(3) PC 실습실 관리용 H/W 사례별 활용 이해

o 하드디스크 보안관
- 지정된 프로그램을 제외하고는 프로그램을 설치하여도 컴퓨터 재부팅시에 원상태로 복원되는 제품

o 리본카드

3. 서버보안

3.1 인증과 접근 통제

3.1.1 계정과 패스워드 보호

(1) 시스템에서 사용하는 기본적인 접근 통제 방법

o 핵심가이드
- 사용자 계정은 하나의 시스템을 여러 사람이 이용할 때 그들을 구분하는 역할
- 패스워드는 각 계정 사용자를 확인하기 위하여 사용
- 그룹은 목적을 같이하는 사용자들을 묶은 것으로써 그룹에 대한 권한 및 허가를 설정하고 관리

o 사용자 계정 생성 및 활용
- 사용자 계정별로 실행할 수 있는 프로그램 및 접근할 수 있는 폴더 및 파일이 구분할 수 있다.
- 사용자 계정으로 로그인하여 사용하면 관리자 또는 root 계정이 아니면 프로그램 설치가 안되거나 설정파일 변경이 제한되기 때문에 악성코드 설치를 제한할 수 있다.

o 그룹은 여러 사용자를 동일한 작업권한을 가질 수 있는 하나의 그룹으로 묶는 것으로 해당 디렉토리별로 사용자 계정별로 권한을 부여하는 것은 어려운 일이므로 그룹으로 소유권을 부여하게 되면 그룹에 소속된 사용자들에게 해당 디렉토리에 대한 사용 권한을 가지도록 설정 가능
- 윈도우즈에서는 사용자 계정을 추가하면 일반 사용자 그룹인 Users 그룹에 자동으로 포함되는데 Users 그룹은 프로그램을 실행할 가장 보안이 강한 환경을 제공한다. NTFS로 포맷된 볼륨에서는 이 그룹의 구성원이 운영 체제 및 설치된 프로그램의 무결성을 해칠 수 없도록 새로 설치된 시스템(업그레이드한 시스템은 포함되지 않음)의 기본 보안 설정이 지정되어 있다.
  - · Users는 시스템 크기의 레지스트리 설정, 운영 체제 파일 또는 프로그램 파일을 수정할 수 없다.
  - · Users는 워크스테이션을 종료할 수는 있지만 서버는 종료할 수 없다.
  - · Users가 로컬 그룹을 만들 수는 있지만 자신이 만든 로컬 그룹만 관리할 수 있습니다.

· 관리자가 설치하거나 배포한 인증된 Windows 2000 프로그램을 실행할 수 있다.
· Users 그룹의 구성원은 자신의 모든 데이터 파일(%userprofile%) 및 레지스트리에서 자신의 부분(HKEY_CURRENT_USER)을 완전하게 제어할 수 있습니다.
· Users 그룹의 구성원은 다른 Users 그룹에서 실행할 수 있는 프로그램은 설치할 수 없습니다. 이렇게 하면 트로이 목마 프로그램을 방지할 수 있습니다. 시스템 관리자가 다른 Users 그룹의 개인 데이터나 데스크톱 설정에 액세스할 수도 없습니다.

(2) 계정 및 패스워드 보호 정책

o 핵심가이드
- 효과적인 계정 관리 기법 사용
  · 사용자별 권한 그룹을 지정하여 관리
  · root 권한에 대한 사용을 제한
  · guest, anonymity 등의 특정 공개용 계정의 사용을 제한
- 안전한 패스워드 관리 기법 사용
  · 예측하기 쉬운 패스워드를 사용하지 않음
  · 패스워드 파일을 암호화하여 보관하고 무결성을 위해 이미지 파일 보관
- 여러 운영체제에 따라 적용하는 패스워드 방식
  · 윈도우즈 NT에서 사용하는 계정과 패스워드 관리 기법
  · 유닉스 계열에서 사용하는 계정과 패스워드 관리 기법
- 여러 가지 패스워드 방식
  · OTP(One Time Password) 방식,
  · PAM(Pluggable Authentication Modules)을 통한 인증 방법, SSH를 사용한 암호화 통신 등
o 계정관리
- 계정을 그룹별로 설정
  · 유닉스 계열 : 그룹생성 및 그룹사용자 생성 명령어(groupadd)로 계정 생성 후 chmod 명령어를 이용하여 허가권 설정
- set user id 또는 set group id의 사용을 제한하여 root 권한의 사용을 제한
- 사용하지 않는 계정을 제거

o 패스워드 관리기법

- 윈도우즈 NT에서 사용하는 계정과 패스워드 관리 기법
  · 유추 가능한 단어를 피하고 조합형 문자열 또는 특수문자를 포함한 문자열로 패스워드 생성
  · 윈도우즈 NT 및 2000 계열은 계정 데이터베이스 보호를 위해 syskey 명령으로 128 bit 암호화 DB를 사용할 수 있다.
- 유닉스 계열의 계정과 패스워드 관리 기법
  · 유추 가능한 단어를 피하고 조합형 문자열 또는 특수문자를 포함한 문자열로 패스워드 생성
  · /etc/passwd는 일반 사용자들도 접근하여 파일 내용을 볼 수 있기 때문에 패스워드가 암호화되어 있더라도 안심할 수 없으므로 새도우(shadow) 패스워드 시스템을 사용하는데 /etc/passwd의 패스워드 필드를 /etc/shadow라는 파일에 암호화하여 저장하고 root 만이 읽을 수 있는 권한설정으로 패스워드를 보호

o PAM 방식

- PAM은 시스템 관리자가 응용프로그램들이 사용자를 인증하는 방법을 선택할 수 있도록 해주는 공유 라이브러리 묶음으로 PAM을 사용하는 응용프로그램을 재컴파일(재작성)하지 않고, 인증 방법을 변경할 수 있다는 것이다. 일반적으로 계정과 패스워드 만을 이용한 인증 방식을 이용하고 있지만 다양한 형태의 인증방식을 부가적으로 사용할 수 있고, 새로운 프로그램에 적절한 인증방식을 부가하여 사용할 수도 있게 하는데 이는 응용프로그램이 사용자 인증을 처리하기 위해 사용될 함수의 라이브러리를 제공함으로써 가능하다. PAM 라이브러리는 /etc/pam.conf(또는 /etc/pam.d/에 있는 여러 파일들)에서 각 시스템에 맞게 설정을 하여, 각 시스템에서 사용가능한 인증 모듈을 통해 사용자의 인증 요구를 처리한다.

3.1.2 파일 시스템 보호

(1) 유닉스에서의 파일 시스템 구성 내용

o 핵심가이드

- 유닉스 시스템에서는 각 파일마다 한 명의 소유자가 존재함
- 유닉스에서 파일은 그 파일의 소유자와 root만 변경 가능

- mount 명령을 통하여 여러 파일 시스템을 연결하여 사용함
- root로 동작하여야 하는 파일 이해
- SUID와 SGID를 이용하여 권한 밖의 자원에 대한 접근을 허용함
- umask 설정 개념 및 특징

o root로 접근 및 변경 권한을 설정해야 하는 파일
- ~/.login, ~/.profole, crontab, NFS 파티션의 파일, /etc/rc* 파일 등등
- 사용자 계정에서 실행권한이 필요없는 파일은 실행권한을 제거

o SUID와 SGID는 권한이 없는 프로그램을 실행할 수 있으며, SUID는 소유자 권한으로 실행하는 것이며, SGID는 소유그룹 권한으로 실행하는 것이므로 불필요한 파일에 설정된 SUID와 SGID의 비트를 제거

o umask는 시스템 파일이 만들어질 때의 허가권 기본값을 정하기 위해서 사용한다.

(2) 윈도우즈 NT에서의 파일 시스템 구성 내용

o 핵심가이드
- 윈도우즈 NT의 파일 시스템 형식 : NTFS, FAT 등의 이해
- administrator 계정의 사용 권한 관리 방법
- 목적에 따른 계정 그룹의 사용 방법

o 윈도우즈 NT에서는 보안 기능이 강화된 NTFS 파일시스템을 사용하는 것을 권장

o administrator 계정의 사용 권한 관리 방법
- 최소 권한의 규칙
  · 규칙에 따르면 모든 사용자는 현재 작업을 완료하는 데 필요한 최소한의 권한만 가진 사용자 계정으로 로그온해야 하며 그 이상의 권한을 부여하면 안된다. 이렇게 하면 다른 위협보다도 악성 코드로부터 보호할 수 있다.
  · 불필요한

o 목적에 따른 계정 그룹의 사용 방법
- 목적에 따라서 계정 그룹을 만들어서 일괄적인 권한 설정이 가능하게 되며, 그룹별로 권한 설정 방법 이해
- 윈도우 NT는 기본적으로 네 기본 그룹(Administrators, Power Users, Users 및 Backup Operators)과 세 특수그룹(Interactive, Network, Terminal Server User)이 존재하며 새로운 계정 및 그룹을 생성하여 권한을 임의로 부여할 수

도 있으며, 새로 생성한 계정에 대해서는 권한을 임의로 부여할 수도 있다.

(3) 파일 시스템 보호 정책

o 핵심가이드
- 파일 시스템 백업(backup) 및 복구 방법
- 무결성 도구를 이용한 파일 시스템의 무결성 검사
- 파일 및 디렉토리 관리 기법

o 파일 시스템 백업(backup) 및 복구 방법
- 윈도우시스템
  · 시스템도구-백업 이용 방법
  · 기타 솔루션 및 도구
- 유닉스시스템
  · tar를 이용하여 파일 백업 방법
  · 기타 솔루션 및 도구

o 무결성 도구를 이용한 파일 시스템의 무결성 검사
- 유닉스용 tripwire 등의 무결성 점검 도구를 이용한 무결성 점검 방법
- md5 도구를 이용한 무결성 점검 방법

3.1.3 시스템 파일 설정과 관리

(1) 유닉스에서의 시스템 파일 설정

o 핵심가이드
- mount 테이블을 이용한 파일 시스템 관리
- 호스트에 대한 접근통제 내용의 설정 방법
- 네트워크 서비스에 대한 내용의 설정 방법
- X 윈도우 사용을 위한 환경 설정 및 관리 기법
- 시스템 로그 파일의 기록을 위한 환경 설정 및 관리 기법

o mount 테이블을 이용한 파일 시스템 관리
- /etc/fstab 파일 보기

o 호스트에 대한 접근통제는 TCP-wrapper 및 xinetd를 활용하여 접근통제 가능

o 네트워크 서비스의 주요 설정 내용 : ftp, telnet, http, rlogin, ssh, scp, samba 등

- telnet
  - ・원격 시스템에 접속할 때 사용하는 서비스로써 텔넷 데몬을 실행하고 사용자 계정을 등록하여 사용한다.
- rlogin :
  - ・원격 시스템에 접속할 때 사용하는 서비스로 사전에 서버에 /etc/hosts.equiv 파일에 호스트를 등록한 후에 클라이언트는 패스워드를 입력할 필요없이 로그인이 가능한 서비스이다.
- ssh : 원격 시스템에 접속할 때 사용하는 서비스로써 telnet, rlogin, rcp 등은 암호화하지 않은 상태의 평문으로 데이터가 전송되므로 보안에 취약할 수 있으므로 이를 보완하기 위한 서비스로써 전송되는 데이터를 개인 열쇠 암호 기법으로 암호화한다.
  - ・주요 설정 내용 : 개인키/공개키 설정, 설정파일 설정
- scp : 네트워크상에서 안전하게 파일을 복사할 수 있도록 해주는 유틸리티로 데이터 전송과 사용자 인증을 위하여 ssh를 사용한다.
- samba : 운영체제 간에 서로 자료 및 하드웨어 공유를 위한 프로토콜로써 주로 윈도우와 리눅스간에 자료 및 프린터 공유를 위해서 사용된다. 삼바의 주된 기능은 IBM OS/2, 마이크로소프트 윈도우 98/NT,에서 LanManager 또는 NetBIOS와 호환되는 SMB 프로토콜을 사용하여 파일 및 프린터를 공유할 수 있도록 한다.

o X 윈도우 사용을 위한 환경 설정 및 관리 기법
- X 윈도우를 설정하기 위해서는 비디오 그래픽카드와 모니터를 정확하게 알고 설정
- X 윈도우를 초기화면으로 부팅하기 위해서는 실행 레벨값을 확인하고 지정
- X 윈도우는 클라이언트가 X서버에 접속하여 윈도우를 띄우는 서비스를 제공하므로 공격자에게 이용당할 수 있으므로 ‘xhost -’명령어를 이용하여 서비스를 중지한다.

(2) 윈도우즈 NT에서의 시스템 파일 설정

o 핵심가이드
- NTFS에 대한 접근통제 수행 방법
- SAM을 통한 인증 서비스 수행 방법
- 관리용 공유 폴더의 유지 및 관리 기법

- 윈도우즈 환경의 레지스터리에 대한 보존 및 관리 기법

o NTFS에 대한 사용권한 설정 방법

- 원하는 위치에서 마우스 오른쪽 버튼을 클릭한 후 등록정보 선택
- 등록정보 대화상자에서 보안탭 선택
- 사용자나 그룹에 사용 권한을 할당하기 위해 추가/제거를 선택
- 대화상자에서 원하는 사용자나 그룹 선택한 후 추가/제거를 설정
- 사용권한 메뉴에서 적절한 사용권한 설정

o 윈도우즈 환경의 레지스터리에 대한 보존 및 관리 기법

- 익명 엑세스로부터 레지스트리 보호
  · 윈도우 2000 레지스트리 편집 도구에서 기본적으로 원격 액세스를 지원하므로, 레지스트리 원격 액세스 권한은 관리자에게만 부여해야 한다. 레지스트리에 대한 네트워크 액세스를 제한하려면 레지스트리를 수정한다.
  · HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg를 선택, 보안 메뉴를 선택한 후 사용권한을 클릭하여 Administrators 사용권한을 모든 권한으로 설정하고 기타 계정 설정은 제거한다.
- 레지스트리에 적절한 ACL을 적용
- 레지스트리 백업 보관

3.1.4 시스템 접근통제 기술

o 핵심가이드

- 접근통제 리스트 및 여러 가지 접근통제 관리 기법
- 강제적 접근통제 정책(MAC), 임의적 접근통제 정책(DAC), 역할기반 접근통제 정책(RBAC)등
- 접근통제 도구 및 유닉스 계열의 접근통제 방법

(1) 주체와 객체간의 관계를 지정하고 접근을 제한하는 방법

o 접근통제 리스트는 시스템의 서비스 및 사용자 등의 특성을 고려하여 접근통제 리스트를 설정한다.

(2) 접근통제 기술 분류 방법

o 임의적 접근통제(DAC) : 주체나 또는 그들이 소속되어 있는 그룹들의 ID에 근거하여 객체에 대한 접근을 제한하는 방법을 DAC라고 한다. 즉, 접근통제는 객체의 소유자에 의하여 임의적으로 이루어진다. 그러므로 어떠한 접근 허가를 가지고 있는 한 주체는 임의의 다른 주체에게 자신의 허가를 넘겨줄 수 있다.

o 강제적 접근통제(MAC) : 객체에 포함된 정보의 비밀성과 이러한 비밀 정보에 대하여 주체가 갖는 정형화된 권한에 근거하여 객체에 대한 접근을 제한하는 방법을 MAC라고 한다. 시스템 내에서 주체와 객체간에 성립하는 MAC 관계에는 다음과 같은 조건이 존재한다.

- 한 주체는 하나의 객체를 주체의 비밀 등급에서의 계층적 분류가 객체의 비밀 등급에서의 계층적 분류보다 크거나 같고 주체의 비밀 등급에서의 비계층적 범주들이 객체의 비밀 등급에서의 모든 비계층적 범주들을 포함하는 경우에 판단할 수 있다.
- 한 주체는 하나의 객체를 주체의 비밀 등급에서의 계층적 분류가 객체의 비밀 등급에서의 계층적 분류보다 작거나 같고 주체의 비밀등급에서의 비계층적 범주들이 객체의 비밀등급에서의 비계층적 범주들에게로 포함되는 경우에 기록할 수 있다.

o 다단계 보안 정책(MLS) : MLS 보안 정책은 최초 1960년대 후반 미국의 국방성에서 시작되었다. 국방성에서 사용하는 문서에는 보안등급이 있었으며, 문서를 읽기 위해서는 문서의 보안등급과 같거나 높은 보안등급이 필요했다. 컴퓨터의 발전으로 종이 형태로 보관되던 정보는 컴퓨터로 옮겨지게 되었으며, 종이 문서의 보안 등급이 컴퓨터에 저장된 정보에도 적용되어야 했다. MLS 보안 정책은 컴퓨터에서의 정보와 사용자간의 보안 정책을 명시하고 있다. MLS의 기본 보안 정책만을 본다면 매우 간단하지만 보안등급이 낮은 프로세스/파일과 보안등급이 높은 프로세스/파일이 있는 경우 기본 보안 정책만으로는 보안등급이 낮은 프로세스가 높은 파일에 쓰기가 제한되는데 이것이 문제가 될 수 있다. 따라서, 기본 보안정책 외의 제한 속성을 정의하고 있다.

- 단순 보안 : 주체는 보안등급이 같거나 낮은 객체에 읽기를 할 수 있으나 높은 보안등급의 객체에는 읽기를 할 수 없다.
- 제한 속성 : 주체는 보안등급이 같거나 큰 객체에 쓰기를 할 수 있으나 낮은 보안등급의 객체에는 쓰기를 할 수 없다.

o 역할기반 접근제어(RBAC) : RBAC의 주요한 목적은 보안 관리와 감사(review)

를 용이하게 하자는 것이다. 메인프레임에 관련된 상업적으로 성공한 많은 접근통제 시스템들은 보안 관리를 위해 역할들을 정의한다. 예로, 운영자 역할은 모든 자원들에 접근할 수 있지만 접근 권한을 바꾸지는 못한다는 등이 있을 수 있는데 이 역할들에 대한 관리는 NetWare나 Windows NT와 같은 현대 네트워크 운영체제에서도 볼 수 있다.

- RBAC은 정책 중립적이지만 세 가지 기본 보안 정책을 제공
  · 특권의 최소화는 RBAC이 역할에 할당된 사용자들에 의해 수행되는 작업들이 단지 설정된 것에 의해 허가된 것만 가능하므로 지원
  · 직무의 분리는 재정관리와 같은 민감한 작업을 수행하기 위해 상호 배타적인 역할을 보장했을 때 가능
  · 데이터 추상화는 운영체제에서 제공되는 읽고 쓰기 권한이라기보다 계정에 대한 credit와 debit 같은 추상화 허가의 방법에 의해 제공

(3) 접근통제 도구

o 프로토콜 기반의 접근통제 도구
- 패킷필터 : ipfwadm, ipchain, iptable, tcp wrapper 등
- 프록시 서비스 : TIS FWTK

(4) 유닉스 계열의 접근통제

o 파일 및 폴더의 허가권 설정
- 파일과 디렉토리에 접근 권한 변경 : chmod
- 파일과 디렉토리에 소유자 및 소유그룹을 변경 : chown

3.2 보안 측면의 관리

3.2.1 시스템 보안 등급 [1급]

o 핵심가이드
- 정보 시스템 보안 평가 종류 및 등급 기준
  · 국가별 정보보호 시스템 평가 기준 : TCSEC, ITSEC, CTCPEC 등
  · 국제 공통 평가 기준 표준 : CC

    · 국내 평가 기준 : CC와 유사한 기준 제시(침입차단 시스템, 침입탐지 시스템)
  - 각 등급별 보안 요구사항

(1) 시스템 보안 평가 기준

o 정보보호시스템 평가인증제도는 정보보호시스템에 대한 안전성과 신뢰성을 보증하기 위하여 공신력있는 제 3자로부터 객관적이고 공정한 평가를 통하여 검증된 정보보호시스템 사용을 권장함으로써 정보의 불법적 유출이나 해킹, 바이러스와 같은 정보화 역기능으로부터 안전한 정보화 사회 확보를 구축하는데 목적이 있다. 평가인증제도는 미국의TCSEC(Trusted Computer System Evaluation Criteria)과 캐나다의 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria), 영국을 비롯한 유럽국가에서 사용하는 ITSEC(Information Technology Security Evaluation Criteria) 등이 있으며, 국제적으로는CC (Common Criteria)가 국제표준으로 제정되어 평가에 활용되고 있으며 우리나라에서는 1996년 정보화촉진기본법에 의하여 한국정보보호센터가 설립되었으며, 정보통신망 침입차단시스템 평가 기준을 개발하여 1998년 정보통신부에서 고시됨으로써 정보보호시스템 평가가 시작되었고 2000년에는 정보통신망 침입탐지시스템 평가기준이 고시되었다.

o TCSEC
  - 보안요구사항
    · 보안정책 : 임의적 접근통제, 객체의 재사용, 레이블, 강제적 접근통제
    · 책임성 : 식별 및 인증, 감사
    · 보증 : 운영상의 보증, 생명주기 보증
    · 문서화 : 사용자 설명서, 보안기능 설명서, 시험문서, 설계문서

o ITSEC
  - ITSEC은 TCSEC과 달리 단일 기준으로 모든 정보보호제품을 평가하고자 하였기 때문에 보안기능은 제품이 사용될 환경을 고려하여 개발자가 보안기능을 설정하거나, TCSEC 혹은 독일의 ZSIEC에서 미리 정의한 보안기능을 사용토록 하였으며 제품에 대한 평가는 보증부분만으로 수행된다. 이러한 ITSEC의 특징은 시스템과 제품을 동일한 평가기준으로 평가하도록 되어있으며 새로운 보안기능의 정의가 용이하고 등급의 평가는 보증 평가만으로 이루어진다.
  - 효용성 기준

· 적절성 분석 : 보안기능이 보안위협을 잘 대처하는지를 분석
· 바인딩 분석 : 보안기능과 메카니즘이 상호 연동하여 통합적이고 효과적으로 잘 동작하는지를 분석
· 메카니즘의 강도 분석 : 보안위협을 방지하기 위한 보안 메카니즘의 강도를 분석
· 개발시의 취약성 분석 : 개발 중의 취약성을 분석하고 이에 대한 대처가 적절한지를 분석
· 사용의 용이성 : 시스템의 관리자 혹은 사용자가 시스템이 안전하다고 믿을지라도 시스템이 안전하지 않게 구성되거나 사용될 수 있는지의 여부를 조사
· 운영중의 취약성 분석 : 운영 중에 발견된 취약성이 시스템의 보안을 얼마나 위협하는지를 평가

- 정확성 기준
  · 요구사항, 구조설계, 상세설계, 구현, 형상관리, 프로그래밍 언어 및 컴파일러, 개발자 보안, 운영문서, 배달절차 및 구성 그리고 시동 및 운영에 대한 요구사항과 같은 구현된 보안기능의 신뢰성을 소프트웨어 공학적인 측면에서 평가하고자 하는 것이다.
- ITSEC의 등급은 E1(최저), E2, E3, E4, E5 및 E6(최고)의 6등급으로 구분

o CTCPEC

- 개발 목적은 보증 기준을 제시하고 보안제품 개발자에게 제공되어야 할 서비스에 대한 지침을 제시하며, 구매자에게는 필요한 서비스 지침을 제공하는 것이다. ctcpec는 기능성과 보증성에 대한 요구사항으로 이루어진다. 기능은 크게 비밀성, 무결성, 가용성, 책임성의 4가지 분류로 구분되며 각 기능에 대한 세부 보안요구사항을 기술하고 있다. 여기서, 비밀성은 암호화를 의미한다기보다는 접근통제를 의미한다. 보증은 ITSEC 등과 같이 전체에 적용이 되며 구현된 보안기능에 대한 신뢰정도를 나타낸다. 보증의 평가등급은 T1, T2, T3, T4, T5, T6, T7의 7등급으로 구성된다.
- 비밀성 기준
  · 비밀채널(CC-0 ~ CC-3), 임의적 비밀성(CD-0 ~ CD-4), 강제적 비밀성(CM-0 ~ CM-4), 객체 재사용(CR-0 ~ CR-1)
- 무결성
  · TCB 무결성(IB-0 ~ IB-2), 임의적 무결성(ID-0 ~ ID4), 강제적 무결성(IM-0 ~ IM-4), 물리적 무결성(IP-0 ~ IP-4), 복귀(Rollback, IR-0 ~ IR-2), 의무분리

(Seperation of Duties, IS-0 ~ IS-3), 자체검사(IT-0 ~ IT-3)

- 가용성 기준
  - ㆍ억제(Containment, AC-0 ~ AC-3), 고장허용(AF-0 ~ AF-2), 지속성(Robustness, AR-0 ~ AR-3), 복구(Recovery, AY-0 ~ AY-3)
- 책임성 기준
  - ㆍ감사(WA-0 ~ WA-5), 식별 및 인증(WI-0 ~ WI-3), 안전한 경로(WT-0 ~ WT-3)

o 국내 평가기준

- 등급은 7등급(K1, K2, K3, K4, K5, K6, K7) 체계를 지니고 있으며 보안기능 요구사항과 보증요구사항으로 이루어진다.
- 보안기능 요구사항
  - ㆍ신분확인, 임의적 접근통제, 강제적 접근통제, 보안레이블, 데이터무결성, 전송데이터 무결성, 비밀성, 감사기록 및 추적, 보안관리

o CC

- 보안기능 요구사항은 11개 클래스로 구성
  - ㆍFAU(보안감사), FCO(통신), FCS(암호지원), FDP(사용자 데이터 보호), FIA(식별 및 인증), FMT(보안관리), FPR(프라이버시), FPT(TOE 보안기능의 보호), FRU(자원활용), FTA(TOE 접근), FTP(안전한 경로/채널)
- 공통평가기준 평가보증등급은 7등급(EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7)으로 구분되며 등급이 높아질수록 보증요구사항이 강화된다.

3.2.2 운영체제 설치 [1급]

o 핵심가이드

- 작업 용도에 따른 시스템의 파티션 분리 방법
- 유닉스 계열의 운영체제 커널 설치 방법 이해
- 윈도우즈 계열의 운영체제 설치 특징 이해

(1) 시스템 파티션과 마운트

o 작업 용도에 따른 시스템의 파티션 분리는 루트영역과 사용자 파일 시스템이 같은 파티션에 존재하면 공격자가 SUID를 사용할 수 있는 기회가 늘어나게 되어 보안상 취약하게 되며 백업이 용이하지 못하고 몇몇 파일 손상 등으로 인해

전체 시스템을 재설치하는 일이 발생할 수 있기 때문에 분리하여 사용하는 것이 보안상 유리하다. 예로, /server에 웹서버 관련 프로그램을 설치하여 웹서버를 운용하고 /DB에 DB 파일들이 저장되는 디렉토리를 만들어 관리할 수 있다.

(2) 운영체제 커널과 소프트웨어 설치

o 유닉스 계열
- 리눅스의 커널은 기본적으로 사용자가 작동시키는 응용프로그램과 하드웨어간의 조정자 역할을 맡는다. 동시에 수행되는 여러 응용프로그램들을 위해 메모리관리를 해 주며 컴퓨터 자원을 배분하는 역할을 해 준다. 리눅스는 커널의 소스를 완전 공개한 운영체제여서 커널의 소스를 사용자가 직접 컴파일 할 수 있다. 이 여러 옵션을 잘 조정해서 커널을 자신이 원하는 환경 및 구성으로 구축할 수 있으며 이를 커널 컴파일이라고 한다.
- 불필요한 서비스 중지 및 프로그램 제거 필요

o 윈도우즈 계열
- 운영체제는 소스코드가 공개되어있지 않기 때문에 인위적인 조작이 불가능
- 불필요한 서비스 중지 및 프로그램 제거 필요

3.2.3 시스템 최적화 [1급]

(1) 자원 관리의 최적화

o 핵심가이드
- 메모리 관리 개념 및 명령어 이해
  · 동적 메모리 관리, 스택/힙 영역 관리
- 프로세스 및 CPU 관리 개념 및 명령어 이해
  · 좀비 프로세스 관리, 프로세스 우선순위 관리 등

o 메모리 관리
- free를 이용한 swap 상태 확인
- top 명령어를 이용한 프로세스별 메모리 사용량 확인

o 프로세스 및 CPU 관리
- 좀비 프로세스는 실행이 종료되었지만 아직 삭제되지 않은 프로세스를 의미하며, ps 명령어 실행 후 stat 값이 Z로 표시되는 프로세스가 좀비 프로세스 이

며, 프로세스 중지를 위해서는 kill 명령어를 사용한다.

- 프로세스 우선 순위 관리가 필요한 경우가 발생하는데 프로세스마다 두 개의 우선순위 번호를 갖는다. ps -l 이라는 명령어를 실행시키면 PRI와 NI라는 항목을 볼 수 있다. 프로세스 우선순위 PRI 항목은 운영체제에 의해 동적으로 계산되는 실제적인 우선순위이다. 다른 기준인 NI는 Nice 값이라는 것으로 PRI로 계산하고 업데이트하는 근거가 되는 번호이다. NI는 Nice 넘버 혹은 요청된 프로세스 실행 우선순위 번호라고 하며 nice 명령어를 이용해서 우선순위를 설정할 수 있다.

(2) 사용자 및 파일 관리

o 핵심가이드
- 사용자별 사용 제한 설정 방법
- 사용자별 홈 디렉토리 설정 및 접근 제어 기능

o 사용자별 홈 디렉토리 설정 및 접근 제어 기능
- 사용자별로 홈디렉토리를 설정하기 위해서는 /etc/passwd 파일에 사용자별로 설정되어있는 홈 디렉토리를 변경하여야 하지만 변경된 디렉토리에서 파일을 쓰고 읽기 등의 권한은 다시 권한 설정을 한다.

(3) 최소권한(least privilege)

o 핵심가이드
- 보안에 대한 취약요소를 줄이기 위한 최소 권한의 프로세스 수행

o 스크립트나 바이너리는 루트 계정만이 주로 사용하므로 기타 계정에는 권한을 제거하여야 하며, 리눅스의 경우 웹서버를 실행하는 apache 계정은 웹서버를 실행하는 권한을 주고 원격 로그인이 필요가 없으므로 쉘 사용권한을 제거하는 등의 권한 설정 필요

3.2.4 시스템 로그 설정과 관리 [1급]

o 핵심가이드
- 유닉스 계열과 윈도우즈 계열 로그관리 방법 및 시스템 관련 중요 이벤트에 대한 로그 개념 및 특징

- 트렌젝션 로그 설정 및 관리 이해
  · 응용 트랜잭션 로그, 데이터베이스 로그, 운영 체제 로그, 접근통제 로그, 통신 로그, 메일 로그, 웹 서버 로그 등

(1) 시스템 로그(syslog)

o 운영체제 제어 하에 시스템 관련 중요 이벤트에 대한 로그
  - syslog, klog : 유닉스 시스템에 대한 로그 설정 및 로그 디렉토리, 로그보기 방법
  - 윈도우즈 이벤트 로그 : 윈도우즈에서는 시스템, 애플리케이션, 보안로그가 기본적으로 설정되어 남게되는데 보안로그는 디폴트로 설정이 되어있지 않게 때문에 설정이 필요하다.

(2) 응용프로그램 로그

o 데이터베이스 로그
  - My-SQL, MS-SQL, Oracle 로그 설정 및 관리
o 웹서버 로그
  - IIS, Apache 로그 설정 및 관리
o 메일서버
  - Sendmail, SMTP 메일서버 관리
o 접근통제로그
  - TCP-wrapper 로그
o 기타

3.2.5 서버 해킹 원리 이해 [1급]

(1) 시스템 해킹은 정보 시스템의 결함으로 생기는 보안 허점을 활용

o 핵심가이드
  - 시스템 해킹의 유형 및 개념 이해
o 시스템 해킹 유형
  - 계정 크랙 공격

- 시스템 취약점을 이용한 해킹
  · 버퍼오버플로우 공격
  · 포맷스트링 공격
- 네트워크 공격
  · 패킷스니핑 공격
  · DoS 공격
  · 스푸핑 공격
- 애플리케이션 취약점을 이용한 해킹
- 웹서버 취약점을 이용한 해킹
- 사회공학적인 공격

(2) 직접 대입 공격

o 핵심가이드
  - 무차별 공격(brute force) 개념 및 대응 방법
  - 사전 공격(dictionary attack) 개념 및 대응 방법
o 무차별 공격(brute force)
  - 시스템 또는 서비스의 ID, 패스워드에 대해서 도구를 이용하여 ID, 패스워드를 자동 조합하여 크랙하는 공격
o 사전 공격(dictionary attack)
  - 시스템 또는 서비스의 ID, 패스워드에 대해서 도구를 이용하여 ID, 패스워드를 크랙하기 위해서 ID와 패스워드가 될 가능성이 있는 단어를 사전파일로 만들어놓고 사전파일의 단어를 대입하여 크랙하는 공격

(3) 네트워크 공격

o 핵심가이드
  - 스푸핑(Spoofing) 공격기술 개념 및 원리
  - 스니핑(Sniffing) 개념 및 원리
  - 서비스 거부 공격(Denial of Service) 개념 및 원리
o 스푸핑
  - 스푸핑 공격은 IP 주소, 하드웨어 주소(MAC address) 등의 정보를 속임으로써 권한을 획득하고 중요 정보를 가로채고 서비스 방해까지 행하는 공격을

말한다.

- IP 스푸핑
  - IP 스푸핑은 다양한 원리를 이용하여 공격을 수행할 는 기술이며, 간단한 예로 리눅스의 rlogin 서비스는 서버에 클라이언트의 IP 및 계정을 등록하여 등록된 클라이언트만이 서버에 접속을 허용하는 서비스로써 공격자는 정상적인 클라이언트 패킷을 스니핑하여 IP 및 계정 정보를 획득하고 계정생성과 IP 변경을 통하여 서버에 비정상적인 접속을 할 수 있다.
- ARP 스푸핑
  - ARP 프로토콜은 32bit IP 주소를 48bit의 네트워크 카드 주소(Mac Address)로 대응시켜 주는 프로토콜이고 실제로 IP 주소를 통해 네트워크 연결을 시도하면 TCP/IP에서는 해당 IP에 해당하는 네트워크 카드 주소를 찾아 연결하게 된다. 이러한 IP 주소와 네트워크 카드 주소의 대응 테이블은 사용자 컴퓨터에서 arp cache 테이블이라는 곳에 위치하게 된다. 이더넷 환경에서 공격대상자의 arp cache 테이블에 공격자가 원하는 IP에 대한 하드웨어주소(MAC address) 쌍을 업데이트하여 공격대상자의 패킷 흐름을 공격자가 원하는 방향으로 조절하여 공격하는 기술이다.
- DNS 스푸핑
  - DNS 프로토콜은 인터넷 연결 시 도메인 주소를 실제 IP 주소로 대응시켜 주는 프로토콜로써 인터넷 연결 시 사용하는 DNS 서버가 IP 주소를 찾아달라는 요청을 받았을 때 계층적인 DNS 서버의 상위계층부터 확인하여 IP를 찾아서 전달해주는 기능을 수행한다. 공격자가 클라이언트가 사용하려는 DNS 서버를 이용하여 클라이언트에게 비정상적인 응답을 보내면 클라이언트는 비정상적인 응답으로 받은 IP 주소로 접속이 될 것이다. 이 공격을 이용하여 피싱(Phishing) 공격을 추가적으로 수행할 수 있다.
- 이메일 스푸핑
  - 이메일 발송 시 송신자의 주소를 위조하는 것으로 이메일 송신자 From 필드에 별칭(alias) 필드를 사용하여 간단하게 송신자 주소를 위조할 수 있으며 폼메일 및 다양한 방법이 있다.

o 스니핑(Sniffing)

- 네트워크 패킷이나 버스를 통해 전달되는 중요 정보를 엿보고 가로채는 공격 행위로 스니퍼(sniffer)는 "컴퓨터 네트워크 상에 흘러다니는 트래픽을 엿듣는 도청장치"라고 말할 수 있다. 그리고 "스니핑"이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말하며 암호화하지 않고 랜 라인을

통해서 전송되는 대화 내용, 계정정보, 카드번호, 주민등록번호 등의 모든 내용을 도청할 수 있다.

- 허브로 연결된 네트워크에서는 스니핑 프로그램만을 설치하여 간단하게 패킷을 스니핑하여 중요한 정보를 탈취할 수 있으나 스위칭 허브로 네트워크가 연결된 환경에서는 Switch Jamming, ARP Redirct나 ICMP Redirct 등의 기법을 이용하여 다른 네트워크 세그먼트의 데이터를 스니핑할 수 있다.

o 서비스 거부 공격(Denial of Service)

- DoS 공격은 대량의 패킷을 이용하여 네트워크를 마비시키거나 특정 서비스의 수행을 방해하는 공격으로 시스템의 한 프로세스가 자원을 모두 독점하거나 소비하여 시스템이 다른 프로세스의 서비스를 제공하지 못하도록 하는 것과 같이 다양한 공격이 가능하다.
- DoS 공격의 특징
  · DoS 공격은 다른 해킹처럼 시스템의 관리자 권한 획득, 시스템에 있는 데이터의 파괴 등을 행하지 않으며 서비스를 사용할 수 없게 만든다. DoS 공격은 문제가 발생했을 때 추적하기 어려우며, 이를 해결하기가 어렵다는 문제점이 있다.
- DoS 공격의 유형
  · 내부에서의 공격 : 시스템의 /tmp와 같이 시스템이 프로세스를 생성하거나, 작업을 처리하는데 사용하는 폴더의 디스크 공간을 채우는 방법이 있다. 이와 같은 방법을 미연에 방지하려면 사용자에게 디스크 용량 사용 제한(쿼터: quota)을 두는 방법이 있다. 다른 내부 공격 유형으로는 프로세스를 생성하여 메모리와 CPU 클럭을 고갈시키는 방법이다. 이러한 공격은 프로세스를 생성하고 메모리를 할당하는 루프를 무한히 돌리거나 단순히 프로세스를 무한히 복제하는 것으로 이루어질 수 있다.
  · 외부에서의 공격 : SYN Flooding은 SYN을 대량으로 보내서 시스템의 특정 서비스를 마비시키는 방법이다. TCP/IP는 Three Way Handshaking 이라는 전송 방법을 이용하는데 클라이언트가 서버에게 SYN 신호를 보내고 서버가 클라이언트에게 연결을 허용한다는 ACK 신호를 보낸다. 이렇게 연결이 설정된 이후에는 일련의 연속번호를 증가시켜가면서 데이터를 주고 받게 된다. 만약 클라이언트가 이 연결 과정에서 ACK 신호를 보내지 않게 되면 서버는 해당 연결을 half-open 상태로 두게 된다. 그리고 일정시간 동안 half-open 상태가 유지되면 연결을 버리고 다시 정상상태로 돌아오게 된다. 만약 공격자가 고의적으로 ACK 신호를 보내지 않게 되어 큐를 모두 채워

버리게 되면 서버의 해당 서비스는 마비될 것이다. 또한, 메일 폭풍과 같이 동시에 대량의 메일을 전송하여 메일 시스템을 마비시키는 방법, 패킷의 순서번호 바꾸어 보내기, 비정상적인 패킷 프래그먼트를 하여 보내기 등 다양한 공격이 있다.

(4) 시스템 오류를 이용한 공격

o 핵심가이드
- 버퍼 오버플로우(buffer overflow) 공격의 원리 이해 및 대표적인 공격 프로그램(스텍 오버플로우, 힙 오버플로우)
- 경쟁 상태(race condition) 공격의 원리 이해 및 대표적인 공격 프로그램

o 버퍼오버플로우는 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소(return address)를 조작하여 해커가 원하는 코드를 실행하는 것이다. 여기서, 버퍼(buffer)는 프로그램 처리 과정에 필요한 데이터가 일시적으로 저장되는 공간으로 메모리의 스택(stack) 영역과 힙(heap) 영역이 여기에 속하며, 버퍼 오버플로우 공격은 스택 오버플로우와 힙 오버플로우 공격이 있다.
- 스택 오버플로우 공격 원리 : 하나의 프로그램은 수많은 서브루틴들로 구성되는데 이런 서브루틴이 프로그램에 의해 호출될 때, 함수 변수와 서브루틴의 복귀 주소(return address) 포인터를 스택(stack)이라는 논리적 데이터 구조에 저장하게 되며 서브루틴이 종료될 때 운영체제는 그것을 호출한 프로그램에 제어권을 반환해야 하기 위하여 복귀 포인터를 통해서 프로그램이 서브루틴의 실행을 마치고 나서 되돌아갈 주소를 가리키게 된다. 공격은 프로그램이 변수의 할당된 공간에 저장될 데이터의 크기를 검사하지 않고 크기에 제한을 두지 않는다면, 데이터의 길이와 내용을 적절히 조정하여 변수 공간을 넘치게 할 수 있으며 버퍼에 오버플로우가 발생하면 저장된 데이터는 인접한 변수 영역까지 침범하여 포인터 영역까지 침범하므로 해커가 원하는 특정 코드가 실행되게 할 수 있다.
- 힙 오버플로우 공격 : 힙은 프로그램이 실행하면서 동적을 할당해서 사용하는 영역을 말하는데 프로그래머가 malloc 같은 메모리 할당 함수를 이용하여 프로그램을 사용할 때 할당하며 힙 영역을 오버플로우 시켜서 특정 코드를 실행하여 공격하는 기술이다.

o 레이스컨디션 공격

- 레이스컨디션 공격은 두 프로세스 간에 자원을 사용하기 위해서 경쟁하는 것을 이용한 공격으로 시스템 프로그램과 공격 프로그램이 경쟁 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로(set user id가 붙은 경우 Root 권한) 파일에 접근을 가능하게 하는 방법을 말한다.

o 기본 설정 오류를 이용한 공격

- 시스템을 활용하기 위한 다양한 설정에서 잘못된 설정에 의해서 공격을 당할 수 있다. 공유폴더 및 관리자 암호를 취약한 암호로 설정하여 사용하는 경우나 IIS 웹서버 설정에서 쓰기 권한을 부여하는 등의 경우에 공격을 당할 수 있다.

(5) 사회공학적 방법

o 핵심가이드

- 사회공학적 방법 이해

o 사회공학(social engineering)은 사람을 속여서 민감한 정보를 유출하게 하는 기술로써 설득과 회유를 통해 자신의 신분을 속이거나 사람들을 교묘히 조종하는 것을 말한다. 예로, 내부자의 결탁으로 인한 정보유출, 내부자의 부주의로 인한 외부에서의 정보습득, 피쉉(Phishing) 및 파밍(Pharming) 등이 있다.

- Phishing은 금융기관 등 신뢰할 수 있는 기관으로부터 보내지는 메일로 위장하여 개인의 인증번호 및 계정정보 등을 빼내는 해킹기술이다.

- Pharming은 피싱의 진화된 형태이며 파밍은 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 중간에서 탈취하는 수법이다. 피싱의 경우에는 사용자가 주의 깊게 살펴보면 알아차릴 수 있지만, 파밍의 경우에는 사용자가 아무리 도메인 주소나 URL 주소를 주의 깊게 살펴본다 하더라도 쉽게 속을 수 밖에 없다

3.2.6 서버 관리자의 의무 [1급]

o 핵심가이드

- 시스템의 시작, 종료 방법 및 재시작해야하는 상황 이해
- 패스워드 파일, 그룹 파일 관리를 위한 파일내용 이해 및 관리 방법
- 프로세스 및 메일, 디스크, 메모리 등의 관리를 위한 명령어와 활용법
- 네트워크 연결 관리 및 상태 관리 방법 및 명령어 이해

(1) 시스템 시작과 종료

o 리눅스 시스템은 도스나 윈도우 운영체제와 달리 시스템을 종료될 때까지 커널 메모리상에 프로세스들이 작동하고 있으므로 시스템을 종료하기 위해서 파워를 끄는 등의 행위로 인하여 리눅스 시스템의 파일시스템에 결함을 발생시킬 수 있다.
- shutdown
  · shutdown -r now : 지금 바로(now 옵션) 시스템 리부팅(-r 옵션)
  · shutdown -h now : 지금 바로 종료
- halt : 강제종료 명령어로 주로 shutdown을 사용하는 것이 안전하며 시스템의 조정을 할 수 없을 경우에 주로 사용된다.
- reboot : 시스템 재부팅 명령어로 shutdown과 유사하지만 shutdown는 프로세스를 종료할 때 kill -15를 사용하여 파일 시스템의 무결성을 보장할 수 있고 reboot는 현재 실행중인 프로세스를 즉시 종료하는 kill -9를 사용하므로 안전한 종료를 보장할 수 없다.

(2) 사용자 계정 관리

o 리눅스는 멀티태스킹의 특징을 가지고 있으므로 다중 사용자를 수용하여 작업을 수행할 수 있다. 이때 사용자마다 계정을 생성하면 /etc/passwd 파일에 계정 및 패스워드 사용자 및 그룹 ID, 그리고 쉘이 정의된다.
- /etc/passwd는 일반 사용자들도 접근하여 파일 내용을 볼 수 있기 때문에 안전한 관리를 위해서 섀도우 패스워드 시스템을 사용하여 /etc/shadow에 암호문으로 저장된다.
- /etc/shadow 파일은 계정명, 암호화된 패스워드 등 9개의 필드로 되어있으며 일반사용자에게는 접근 권한이 없으므로 더욱더 안전하다.
- chage 유틸리티를 이용하여 계정 패스워드 관리

o 계정 사용 제한
- 원격 접근권한 제거 : /etc/passwd 파일에서 /bin/bash과 같은 쉘을 삭제
- 계정 사용기간 설정 : /etc/shadow 파일에서 사용기간 또는 만료일 설정

(3) 자원 관리

o 프로세스 관리
  - ps, kill, wait, su 등을 사용한 프로세스 관리
    · wait : 프로세스가 마치기를 기다리는 명령어. 옵션에 따라서 전체 또는 특정 프로세서 id의 백그라운드 프로세서를 기다리고 있다가 종료 상태를 보고
    · nice : 프로세스의 우선순위를 변경할 수 있는 nice 값을 설정하는 명령어로 프로세스의 실행우선순위가 높다는 것은 더 많은 시스템 자원을 할당하게 되어 속도가 빨라지는 것으로 이해할 수 있으며 범위는 -20 ~ +20까지 값을 설정할 수 있다.
o 메모리 관리
  - free : 시스템의 실제 메모리와 스왑 메모리에 대한 사용 현황을 확인할 수 있는 명령어로 실제메모리 전체용량, 실제메모리 중 유휴메모리의 량, 실제메모리 중 사용중인 메모리 량, 스왑 메모리의 량, 커널에서 사용되는 공유메모리와 버퍼량, 캐시된 메모리의 량 등을 확인할 수 있다.
o 메일, 디스크 등의 자원 관리
  - 리눅스 시스템의 경우 디스크 사용량을 사용자 및 그룹별로 설정하기 위해서는 quota를 사용하며 전체적인 메일 용량 크기의 제한은 메일 스풀 디렉터리를 별도의 파티션을 주고 그 파티션에 쿼터를 설정
  - du : 디스크의 파일 사용량을 재귀적으로 보여줍니다. 특별히 지정하지 않으면 현재 디렉토리에 대해서 동작합니다

(4) 네트워크 관리

o 네트워크 연결 관리를 위한 명령어
  - ifconfig, route, netstat, nslookup, ping, traceroute 등
o 네트워크 상태 관리를 위한 명령어
  - fuser : 지정된 파일이 사용하고 있는 프로세스 ID를 출력하는 명령
  - tty : 시스템에 연결되어 사용하고 있는 시스템 이름 확인

3.3 서버 보안용 S/W 설치 및 운영

3.3.1 시스템 취약점 점검 도구

o 핵심가이드
  - 보안 취약성의 개념 및 종류
  - 보안 위협의 개념 및 종류
  - 주요 취약성 점검 도구의 동작원리 및 특징 이해 : SAINT, SATAN, COPS, ISS, K-COPS, nessus, gabriel 등

(1) 보안 취약성 및 위협

o 위협(Threat)
  - 시스템 또는 조직에 피해를 초래할 수 있는 원치 않는 사건의 잠재적인 원인으로 자산에 피해를 줄 수 있는 위험의 원천이다. 위협은 자산이 지니고 있는 취약성을 이용하여 자산에 손상을 입힌다.
  - 위협 종류 : 자연에 의한 위협, 인간에 의한 비의도적 위협, 인간에 의한 의도적 위협 등으로 구분
    · 인위적인 위협 : 고의적(도청, 정보수정, 시스템해킹), 우발적(자료입력 실수, 정원 변동)
    · 자연적인 위협 : 지진, 벼락, 홍수
o 취약성(Vulnerability)
  - 위협에 의해 이용될 수 있는 자산의 약점으로 달리 말하면 자산이 잠재적으로 갖고 있는 약점을 말합니다. 취약성 자체가 손상을 초래하지는 않는다. 취약성은 단순히 위협이 자산에 영향을 줄 수 있는 조건을 제공할 뿐이다.
  - 취약성 종류 : 물리적 취약성, 자연적 취약성, 환경적 취약성, 하드웨어 취약성, 소프트웨어 취약성, 매체 취약성, 전자파 취약성, 통신 취약성, 인적 취약성 등으로 구분
    · 파일업로드 취약성, 버퍼 오버플로우 취약성 등

(2) 취약점 점검 도구

o 취약점 점검도구
  - SATAN/SARA
    · SARA는 SATAN이 업데이트가 되지 않는 상황에서 SATAN을 기반으로 개

발된 취약점 분석도구로써 네트워크 기반의 컴퓨터, 서버, 라우터 IDS에 대해서 취약점 분석, 유닉스 플래폼에서 동작, HTML 형식의 보고서 기능이 있다.

- SAINT
  - ･유닉스 플래폼에서 동작하는 네트워크 취약점 분석도구로써 HTML 형식의 보고서 기능이 있다.
  - ･원격으로 취약점 점검도구하는 기능
- COPS
  - ･유닉스 플래폼에서 동작하며 시스템 내부에 존재하는 취약성을 점검하는 도구하는 도구로써 취약한 패스워드 체크,
  - ･시스템에서 취약점 점검하는 기능
- Nessus
  - ･유닉스 플래폼에서 동작하는 네트워크 취약점 점검도구
  - ･클라이언트-서버 구조로 클라이언트를 취약점 점검하는 기능
  - ･기타
- nmap
  - ･포트스캐닝 도구로써 TCP connect 방식 뿐만 아니라 stealth 모드로 포트 스캐닝 하는 기능 포함

3.3.2 시스템 침입 탐지 시스템

(1) 침입탐지 시스템의 특징

o 핵심가이드

- 침입탐지 시스템의 특징 및 원리 이해

o 침입탐지 시스템 정의

- 허가받지 않은 접근이나 해킹시도를 감지하여 시스템 또는 망관리자에게 통보해 주고, 필요한 대응을 취하도록 하는 시스템
  - ･암호화 패킷에 대해서는 침입탐지 불가능
  - ･패킷의 데이터 부분까지 분석

o 침입탐지 시스템은 정보 수집, 가공, 침입탐지 처리, 보고 등으로 구성 이해

- 정보 수집 : 감사 로그나 네트워크 패킷 정보를 수집
- 정보 가공 : 침입탐지 시스템이나 침입대응 시스템에서 이용하기 편리하도록

정보를 가공하여 보관

- 침입탐지 처리 : 이벤트 정보와 프로파일이나 공격관련 규칙을 비교하여 침입탐지 수행
- 침입 보고 : 탐지된 행위에 대하여 보안 관리자 등에게 침입행위를 알림

o 침입탐지 시스템의 원리 이해

- 오용 기반 침입탐지 : 알려진 취약점을 기반으로 탐지 규칙을 작성하여 침입행위를 판단
- 비정상행위 탐지 : 사용자나 시스템의 정상행위에 대하여 프로파일링을 수행한 후에 실제 발생한 이벤트의 정상유무를 판단

o 구현기술

- 사후 감사추적에 의한 분석기술 : 미리 수행된 의심스러운 행위에 대하여 발생한 자료를 토대로 감사, 분석이 이루어진다.
- 실시간 패킷 분석기술 : 단일 네트워크 세그먼트(link)에 흐르는 패킷을 가로채는 기술, 실시간 탐지 기술
- 실시간 행위 감시 및 분석 기능 : 인가되지 않은 파일접근, Log-in 프로그램의 변경과 같은 시도를 탐지 가능

(2) 네트워크 모니터링

o 핵심가이드

- 네트워크 모니터링 및 침입탐지 도구의 주요 특징 및 설정, 로그분석 방법 이해
  · Snort, Shadow 등
- 방화벽 프로그램의 주요 특징 및 설정, 로그분석 방법 이해
  · TCP-Wrapper, IPCHAIN 등

o 네트워크 모니터링 및 침입탐지 도구

- Snort : snort는 실시간 트래픽 분석과 IP 네트워크 상에서 패킷 로깅이 가능한 가벼운(lightweight) 네트워크 침입탐지시스템이다. snort는 프로토콜 분석, 내용 검색/매칭을 수행할 수 있으며 오버플로우, Stealth 포트스캔, CGI 공격, SMB 탐색, OS 확인 시도 등의 다양한 공격과 스캔을 탐지할 수 있다
- Shadow 등
- 예로, smurf 공격은 DoS 공격의 일종으로 공격대상자는 스푸핑된 소스 IP로부터 ICMP reply를 동시에 다시를 수신하는 현상을 나타내게 된다. 네트워크

모니터링 도구를 이용하여 패킷을 캡쳐하여 확인할 수 있다.

```
yyy.yyy.86.170 -> xxx.xxx.36.12 ICMP Echo reply
yyy.yyy.179.166 -> xxx.xxx.36.12 ICMP Echo reply
yyy.yyy.179.8 -> xxx.xxx.36.12 ICMP Echo reply
yyy.yyy.179.50 -> xxx.xxx.36.12 ICMP Echo reply
yyy.yyy.179.6 -> xxx.xxx.36.12 ICMP Echo reply
yyy.yyy.179.11 -> xxx.xxx.36.12 ICMP Echo reply
yyy.yyy.179.165 -> xxx.xxx.36.12 ICMP Echo reply
yyy.yyy.179.200 -> xxx.xxx.36.12 ICMP Echo reply
yyy.yyy.179.160 -> xxx.xxx.36.12 ICMP Echo reply
```

o 방화벽

- TCP-Wrapper
  - · TCP-Wrapper는 네트워크 서비스에 관련한 트래픽을 제어하고 모니터링 할 수 있는 UNIX 기반의 방화벽 툴로써 임의의 호스트가 서비스를 요청해 오면 실제 데몬을 구동하기 전에 접속을 허용한 시스템인지 여부를 확인하여 호스트명 및 서비스명을 로그에 남긴다음, 허가된 시스템은 서비스를 제공하고 허가되지 않은 경우에는 접속을 차단해 주는 도구로 동작원리 이해
  - · 특정 서비스를 TCP-Wrapper로 접근제어를 하려면 외부의 연결로부터 보호할 네트워크 서비스들을 선택하여 tcpd가 보호하도록 inetd.conf 파일을 수정해 주어야하는데 이를 위한 서비스별 설정 방법 이해
  - · /etc/hosts.deny, /etc/hosts.allow 파일 설정 이해
- IPchain/IPtable
  - · IPtable은 패킷필터링 방화벽으로 패킷 필터란 네트워크를 통하는 모든 것은 패킷의 형태를 가지며, 패킷의 앞부분에 는 패킷이 어디서 왔는지 어디로 향하는지, 어떤 프로토콜을 이용하는지 등과 같은 정보를 가지고 있다. 패킷 필터는 이렇게 지나가는 패킷의 헤더를 보고 패킷을 'DROP'하거나 'ACCEPT'하는 등의 작업을 하는 프로그램을 말한다. iptable은 이런 패킷 필터링 기능을 설정하는데 사용할 수 있는 프로그램 이며 다음과 같이 패킷 검사를 수행한다.
    1. 패킷이 커널에 도착하면 그 패킷의 목적지를 확인한다. 이것을 '라우팅' 이라고 한다.
    2. 패킷의 목적지가 이곳이면, 패킷은 전달돼 입력체인에 도달한다. 패킷이

입력체인을 통과하면 패킷을 기다리고 있던 프로세서가 받게 된다.

3. 그렇지 않고 커널이 포워딩 불능이나, 패킷을 어떻게 포워딩해야 하는가를 알지 못하면, 그 패킷은 'DROP' 된다. 포워딩이 가능하게 돼있고 다른 곳이 목적지이면 패킷은 포워딩 체인으로 간다. 이 체인이 ACCEPT' 하게 되면 이것은 포워딩할 네트워크로 보내진다.
4. 마지막으로, 로컬에서 수행하던 프로그램은 네트워크 패킷을 전송할 수 있다. 이 패킷은 즉시 출력 체인에 보내지며 이 체인이 'ACCEPT'되면 이 패킷은 그 목적지가 어디든지 보내진다.

· 특정 서비스에 대한 IPtable 정책설정 방법 이해

iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP

(3) 침입대응 방법

o 핵심가이드
- 침입대응의 종류 및 방법 이해

o 침입탐지시스템의 자동 경고메시지 및 로그분석 등을 이용하여 침입을 탐지할 수 있으며 침입에 대한 대응방법은 침입의 종류 및 시스템의 환경 및 서비스에 따라서 달라질 수 있다. 침입대응으로는 세션 끊기, 네트워크 분리, 프로세스 제거, 공격자 추적, 등의 다양한 방법이 있을 수 있다.

3.3.3 무결성 점검 도구 [1급]

(1) 시스템 무결성 검증

o 핵심가이드
- 시스템 커널의 이미지를 복사하고 백업 보관하여 시스템 자체의 무결성을 검증하는 방법
- 컴퓨터 포렌식스 용도로 사용하기 위한 시스템의 이미지 사본 저장하는 방법

o 리눅스/유닉스 백업
- tar를 이용하여 백업
  · tar -zcvpf /archive/full-backup-'date '+%d-%B-%Y''.tar.gz \ --directory /

o 컴퓨터 포렌식스 용도의 이미지 백업
- 이미지 백업은 시스템이 설치된 논리디스크를 비트단위를 복사하는 것으로 일

반적인 복사의 개념과 다르며, 만일 하드디스크를 1개의 드라이브로 설정하여 사용하는 경우에는 이미지로 백업할 때 저장할 공간이 필요하므로 원격 PC의 저장장치에 nc를 이용하여 실시간으로 이미지를 백업하여 저장할 수 있다.

- dd를 이용하는 경우
  - 리눅스/유닉스 백업 : dd if=/dev/hda2 bs=1024 | nc ip 포트(/dev/hda2를 백업)
- Norton ghost를 이용
- 컴퓨터포렌식 전용툴을 이용한 이미지 백업
  - Encase, FTK 등

(2) 파일 무결성 점검

o 핵심가이드
- 시스템 전체보다 중요한 파일이나 디렉토리에 관련된 정보를 보관한 후 불법적인 변조나 삭제가 있었는지를 점검
  - tripwire, MD5, Fcheck, AIDE 등

o 파일무결성 점검도구는 정상적인 상태의 디렉토리 및 파일 정보를 백업하고 있다가 점검 수행 시점에서의 정보와 백업한 정보를 비교하여 변경된 사항을 점검하는 도구
- tripwire
  - MD5, SHA, CRC-32등의 다양한 해쉬 함수를 제공하고, 파일들에 대한 데이터베이스를 만들어 이를 통해 공격자들에 의한 파일들의 변조여부를 판별

3.3.4 접근통제 및 로깅 도구 [1급]

(1) 유닉스 환경의 접근통제

o 핵심가이드
- 그룹 영역을 설정하여 사용자별 그룹 관리 방법
  - 객체에 대한 소유권을 부여하여 소유자 이외 에는 접근이 어렵게 함
  - 비슷한 일을 수행하는 사용자에 대한 그룹을 부여하여 그룹별 접근통제 수행
- 파일이나 디렉토리에 대한 퍼미션 적용 방법

· 읽기/쓰기/실행 퍼미션을 적용하여 파일에 대한 접근통제 관리
· sticky bit, set user id(SetUID) bit, set group id(SetGID) bit의 설정으로 융통성있는 접근통제 관리

- 접근통제 관련 로깅 도구 활용
  · 유닉스 환경에서는 syslogd를 통하여 여러가지 접근통제 위반 내용 및 허가권 변경 사항을 메시지로 기록할 수 있게 함

o 그룹 영역을 설정하여 사용자별 그룹 관리 방법
- groupadd/groupdel 명령어를 이용하여 그룹 계정을 관리하고 chown을 이용하여 모든 파일이나 디렉토리에 액세스할 수 있는 소유자와 그룹 소유권을 설정할 수 있다.

o 파일이나 디렉토리에 대한 퍼미션 적용 방법
- 모든 파일과 디렉토리에 액세스할 수 있는 허가권을 설정할 수 있으며, 허가권은 파일이나 디렉토리별로 소유자, 그룹, 타인에 대해 각각 읽기, 쓰기, 실행 권한을 설정할 수 있으며, chmod 명령어를 활용한다.
- sticky bit는 모든 사용자가 쓰고 삭제할 수 있는 디렉토리에 적용하는데 리눅스에서는 /tmp 폴더가 설정되어있으며, 이 비트를 적용한 디렉토리에서는 누구든지 파일을 쓰고 삭제할 수 있지만 파일 삭제는 오직 소유자만이 삭제할 수 있다.
- SetUID나 SetGID는 파일을 실행할 때 그 파일의 소유자 또는 그룹의 권한으로 실행되도록 하는 것으로 사용자가 시스템 작업을 할 때 루트 권한이 필요한 경우나 어떠한 시스템 자원을 이용하기 위한 경우에 필요하다.

o 접근통제 관련 로깅 도구 활용
- syslogd : syslog.conf 설정파일에 설정에 따라서 동작하는 로그 데몬으로써 커널로그, 메시지(messages) 로그, secure 로그, 크론로그, 부팅로그 및 메일로그, 네임서버 로그, ftp 로그 등의 로그를 관리할 수 있다.

(2) 윈도우즈 환경의 접근통제

o 핵심가이드
- administrator 권한의 수행
- 사용자 및 그룹별 접근 통제 수행 방법
- 윈도우즈 NT 이상 시스템에서는 시스템 이벤트 로그 정보 기록 방법

o administrator 권한을 수행하여 접근 통제를 수행할 수 있으며 응용 프로그램,

디렉토리 및 폴더 별로 사용자와 그룹별로 접근 통제를 수행할 수 있다.

o 윈도우즈 NT 이상 시스템에서는 시스템 이벤트 로그 정보 기록 방법

- 시스템 이벤트에는 시스템, 애플리케이션, 보안 이벤트가 있는데 보안 이벤트는 디폴트로 설정이 되어있지 않으므로 설정을 해야 로그가 기록된다. 보안 로그는 제어판-관리도구-로컬보안설정-감사정책에서 성공/실패 로그를 각각 설정할 수 있다.

3.3.5 스캔 탐지 도구 [1급]

(1) 스캔 공격

o 핵심가이드

- 알려진 취약점 점검 도구를 통한 공격이 수행될 수 있으며 알려진 취약점 점검 도구의 종류 및 특징 이해
- 취약점을 찾기 위한 공격용 도구 종류 및 특징 이해

o 취약점 점검도구 종류

- SATAN, SAINT, COPS, nessus, nmap 등

o 취약점을 찾기 위한 공격용 도구

- mscan
  · 메인 전체를 스캔하여 그 도메인 내에 있는 wingate, test-cgi, NFS exports, statd, named, ipopd, imapd 등 최근 많이 이용되는 주요 취약점을 한번에 스캔할 수 있는 해킹 도구
- sscan
  · mscan을 업데이트하여 개발한 유닉스/윈도우 시스템에 대해서 네트워크를 통하여 취약점 점검을 수행할 수 있는 도구로써 공격용으로도 많이 활용되고 있다.
- 최신 취약점 점검도구 : nikto, x-scan, N-stealth 등

(2) 스캔 탐지 방법

o 핵심가이드

- 네트워크 스캔 공격은 일반적으로 여러 포트의 존재 여부를 검사하게 되므로 실시간 스캔 탐지 도구의 종류 및 활용 이해

o 실시간 스캔 탐지 도구의 활용

- 포트스캔 탐지
  - portsentry : 실시간으로 포트 스캔을 탐지하고 대응하기 위한 프로그램으로 정상적인 스캔과 stealth 스캔을 탐지할 수 있으며, 스캔로그 남기기, 공격호스트를 /etc/hosts.deny 파일에 기록하여 자동 방어, 공격 호스트를 경유하여 오는 모든 트래픽을 자동 재구성하는 기능이 있다.
  - scanlogd, scandetd 등
- 특정 스캐너 탐지도구
  - SATAN, ISS 탐지도구 : Courtney, Gabriel, Natas 등
- 네트워크 패킷 모니터링 도구 및 침입탐지시스템 활용
  - Ethereal, Snort 등

3.3.6 로깅 및 로그 분석 도구 [1급]

(1) 로깅정보

o 핵심가이드
- 감사 증적(audit trail), 감사(auditing), 감사로그(audit log)에 대한 이해
  - 감사 정보는 그 정보의 변조가 없다는 가정 하에 법적 증거로써 사용 가능하므로 감사로그의 보호 및 백업 방법 이해
- 감사로그 분석 방법 이해 및 로그 분석을 통한 사고 파악
  - 사후 감사로그 분석 : 일반적으로 많이 사용되었던 방식으로 사건 발생 후에 감사로그를 모아 놓고 집중적으로 분석 수행
  - 주기적 감사로그 분석 : 주기적으로 감사로그를 분석하여 시스템 침해가 있었는지를 검사·
  - 실시간 감사로그 분석 : 감사로그 파일을 실시간 탐지 시스템에 연결하여 시스템 침해가 발생하는 것을 실시간으로 탐지하고 대응함

o 감사증적, 감사, 감사로그
- 감사증적이란 기록된 특정 내용에 대해서 원시문서까지 추적해 갈 수 있는 연결고리를 말하는 데 정보시스템의 경우 원시문서가 없거나 중간의 처리 과정을 밝힐 수 없는 경우처럼 감사증적이 소멸해 버리는 수가 많다.

o 감사로그 분석 방법
- 윈도우시스템 로그분석
  - 윈도우시스템 로그분석은 이벤트뷰어를 이용해서 로그분석을 수행할 수 있으나 다

량의 로그에 대해서 분석을 위해서는 이벤트 ID를 기반으로 로그분석을 수행할 수 있다.

· Windows 2000에서는 보안 이벤트에 사용할 수 있는 몇 가지 감사 범주를 제공한다. 기업의 감사 전략을 설계할 때 다음과 같은 보안 감사 이벤트 범주를 포함시킬 것인지 결정해야 한다.(로그온 이벤트, 계정 로그온 이벤트, 개체 액세스, 디렉터리 서비스 액세스, 권한 사용, 프로세스 추적, 시스템 이벤트, 정책 변경으로 구분)

· 로그온 이벤트 : 로그온 이벤트를 감사하는 경우 사용자가 컴퓨터에 로그온 하거나 로그오프할 때마다 로그온이 시도된 컴퓨터의 보안 로그에 이벤트가 생성된다. 사용자가 원격 서버에 연결할 때에도 원격 서버의 보안 로그에 로그온 이벤트가 생성된다. 로그온 이벤트는 로그온 세션 및 토큰이 작성되거나 삭제될 때 각각 만들어진다.

528 : 컴퓨터에 성공적으로 로그온했다.

529 : 알 수 없는 사용자 이름을 사용하거나 사용자 이름은 알 수 있지만 잘못된 암호를 사용하여 로그온을 시도했다

- 리눅스/유닉스 시스템 로그분석

· wtmp : 사용자들의 로그인 및 로그아웃한 정보 정보를 가지고 있으며, utmp와 같은 데이터 스트럭쳐를 사용. 텔넷을 통한 로그인뿐만 아니라, FTP를 통한 로그인 등 실질적으로 로그인 프로세스를 거친 정보 및 라부트와 같이 시스템과 관련된 정보 취득. last 명령어를 사용하여 정보를 확인할 수 있다.

· utmp : 시스템에 현재 로그인한 사용자들에 대한 상태 정보 수집. 상태정보는 사용자이름, 터미널 장치이름, 원격 로그인시 원격 호스트 이름, 사용자가 로그인한 시간 등을 기록. who, w, whodo, users, finger 등의 명령어

· pacct : 사용자가 로그인한 후부터 로그아웃할 때 까지 입력한 명령과 시간, 작동된 tty 등에 대한 정보를 수집. lastcomm 명령어를 이용하여 분석

· history : history 로그는 사용자별로 실행한 명령을 기록하는 로그. bash, sh, tcsh, csh 등 사용자들이 사용하는 쉘에 따라서 각각 .bash_history, .sh_history, .history 등의 파일로 기록을 남기며, 명령어뿐만 아니라 파일위치 및 파일명까지 기록. vi 편집기, history 명령어로 로그분석

· sulog : su 명령어를 사용한 결과를 저장하는 로그. vi 에디터 활용

· lastlog : 서버에 접속한 사용자의 IP 별로 가장 최근에 로그인 한 시간이 기록. lastlog 명령어

· btmp : 5번 이상 로그인 실패를 했을 경우에 로그인 실패 정보를 기록. lastb 명령어
· syslog : syslog 데몬에서 일괄적인 방법으로 생성된 로그들에는 authlog, messages, syslog, secure 등 /var/log 디렉토리에 대한 로그가 있다.
· messages : syslog 계열의 로그로써 콘솔 상의 화면에 출력되는 메시지들을 저장하고 시스템의 장애에 대한 기록뿐만 아니라 보안측면에서 취약점에 의한 공격 흔적을 기록으로 남기게 된다. vi 명령어로 로그분석
· secure로그 : secure 로그는 보안과 관련된 주요한 로그를 남기는 파일로 사용자 인증에 관련된 로그를 기록한다. vi 에디터
· 웹관련 로그 : vi 명령어로 분석

o 로그분석을 통한 침입탐지
- 시스템 및 네트워크 공격, 웹공격 등에 대한 로그 분석

(2) 로그 분석 도구

o 핵심가이드
- 감사로그는 그 크기가 엄청날 수 있기 때문에 감사로그에 대한 축약 방법 및 백업 방법
- 감사로그의 불법적인 변조나 삭제가 발생하였을 경우 감사로그의 증거로써 활용 가능성이 떨어지기 때문에 감사로그에 대한 변화를 탐지하는 방법
- 감사로그를 이용하여 공격이 있었는지를 탐지하는 도구가 필요함

o 감사로그는 그 크기가 크기 때문에 감사로그에 대한 축약 방법 및 백업 방법
- 유닉스계열
· logrotate를 이용한 로그 관리 방법 이해
· 스크립트를 crontab에 설정하여 기간별로 로그를 분리하여 관리 및 백업하는 방법 이해
- 윈도우계열
· 시스템로그의 경우에 기본 설정은 지정된 일자보다 오래된 이벤트를 자동 덮어쓰기, 수종으로 로그지우기 등의 기능으로 설정할 수 있으며 필요한 경우 수동으로 로그백업 또는 스크립트를 이용한 백업을 수행할 수 있다.
· 웹서버 로그의 경우에 특히 로그의 양이 크게 증가하므로 웹서버 설정 메뉴에서 지정된 일자별로 로그를 분리하여 기록하게 설정할 수 있다.

o 감사로그를 이용하여 공격이 있었는지를 탐지하는 도구

- 윈도우계열 : 윈도우의 보안 문제를 다룰 때 가장 중요한 리소스 중의 하나는 윈도우 보안 로그이며 로그에 포함되어 있는 모든 정보를 살펴보는 것은 쉽지 않을 일이므로 이벤트 ID를 이용한 로그 검색을 통하여 로그분석하는 것이 효과적일 수 있다.
  - ㆍEventCombMT 유틸리티 활용 : 마이크로소프트에서 제공하는 로그분석 도구
  - ㆍlogparser 활용 : 로그 파일에 대해서 쿼리를 보내서 로그의 이벤트 ID 또는 로그 문자열 검색 등의 방법으로 의심스러운 로그를 검색하여 로그 분석하는 도구
- 리눅스/유닉스 계열
  - ㆍlogcheck

o 로그변조 탐지 도구
- chklastlog, chkwtmp 등

참고문헌

[1] 운영체제, 상조사, 2002

[2] 리눅스 서버보안 관리 실무, (주)슈퍼유저코리아, 2005.4

[3] Microsoft 홈페이지, http://www.microsoft.com/korea/technet/

[4] 인터넷침해사고대응지원센터, www.krcret.or.kr

[5] 국가정보원, 정보통신부, 2005 국가정보보호백서, 2005.6

[6] 정보보안 개론과 실습:네트워크 해킹과 보안, 한빛미디어, 2003

[7] 정보보안 개론과 실습:시스템해킹과 보안, 한빛미디어, 2004