유닉시 파일시스템 inode p.582

나) i-node의 개념과 구성요소

(1) i-node 개념

① **i-node란 유닉스(리눅스) 커널이 현재 사용하는 자료구조(파일정보)를 유지하는 구조체이다**.

② 유닉스(리눅스)는 파일에 접근 시 i-node를 통해 파일을 참조한다.

(2) i-node 특징

① 유닉스는 모든 하드웨어 및 소프트웨어를 파일단위로 관리하고 이러한 파일들에 대한 정보가 inode이다

② **모든 파일은 반드시 하나의 inode 값을 가진다**.

(3) inode가 가지고 있는 정보

속성	설명
inode number	파일시스템 내에서 해당 파일을 식별하기 위한 고유한 식별자
파일타입	일반파일, 디렉터리, 장치파일 등 파일 유형
접근권한	파일에 대한 접근권한
link count	해당 inode를 참조하는 링크 갯수(하드링크 카운트)
소유자	파일의 소유자/UID
소유그룹	파일의 소유그룹/GID
파일크기	파일의 크기
MAC Time	**① last Modification Time** • 파일의 내용을 마지막으로 수정한 시간 **② last Access Time** • 파일을 마지막으로 접근한 시간 **③ last Change Time** • 파일의 속성을 마지막으로 변경한 시간 • 파일의 속성은 i-node 정보를 의미한다. 즉 소유자, 접근권한 등의 속성이 변경되면 last Change Time이 변경된다.
Block index	Data blocks에 저장되어 있는 파일 내용에 대한 색인 정보

표 251 inode list 속성

① inode list (아이노드 리스트)는 파일에 대한 속성정보를 관리하기 위한 블록이다.ㅋ

② 침해사고가 발생하게 되면 피해 시스템 파일에 대한 무결성 확인을 위한 타임라인 분석을 수행한다. 이 때 **파일시스템 inode 구조체의 MAC Time을 점검**한다.

2018년 12회
194. UNIX 파일 시스템의 구성 중 아이노드(i-node)가 가지고 있지 않은 정보는?
① 파일의 이름 ② 파일의 링크 수
③ 파일 수정시각 ④ 파일 유형

정답	1

i-node란 유닉스(리눅스) 커널이 현재 사용하는 자료구조(파일정보)를 유지하는 구조체이다.

2018년 12회
195. 다음 중 리눅스 inode 블럭에 포함되지 않는 것은 ?
① 파일 유형
② 파일 이름
③ 파일 수정시간
④ 파일 link 수

정답	2

2015년 06회
196. 다음 중 아이 노드(i-node)에 포함하고 있는 정보가 아닌 것은?
① 파일 유형 ② 파일 이름
③ 링크 수 ④ 수정시각

정답	2

2017년 10회
197. 다음에 설명하는 유닉스 파일시스템의 영역은 무엇인가?

파일시스템 내의 파일이나 디렉터리의 소유자, 소유그룹, 접근 모드(읽기, 쓰기, 실행 권한), 크기, 속성, 시간 및 디스크 블록 내의 포인터 등에 대한 각종 정보를 저장하고 있는 영역으로서 각 파일이나 디렉터리별로 고유한 식별번호를 가지고 있다.

① boot 블록 ② super 블록
③ inode 블록 ④ data 블록

정답	3

리눅스 p.584

리눅스 파일 시스템

	EXT2	EXT3	EXT4
특징	장애발생 시 파일 손상이 발생할 수 있다. fsck명령어로 복구 시 시간이 많이 걸리는 단점이 있다.	저널링 기법으로 안전하고 빠른 복구가 가능하다.	지연된 할당이라고도 알려진, allocate-on-flush라는 파일 시스템 성능 기술을 사용한다.

표 257 리눅스 파일시스템 비교

2018년 11회

198. 다음 중 윈도우 운영체제에서 사용하는 파일 시스템이 아닌 것은?

① FAT16 ② FAT32 ③ EXT3 ④ NTFS

정답 3

2019년 14회

199. 다음은 어떠한 파일시스템에 대한 설명이다. 설명하고 있는 파일 시스템을 고르시오.

> 리눅스 운영체제를 목표로 만들어진 첫 번째 파일 시스템으로, Remy Card가 MFS(MINIX FIle System)의 한계를 극복하기 위해 개발하였다. 최대 용량을 2GB까지 늘렸고 파일이름의 최대 길이는 255자 까지 지원한다. 오래 사용하면 파일 시스템의 단편화가 발생한다는 단점이 있다.

① FAT16 ② MFS ③ NTFS ④ EXT

정답 4

파일시스템이란 파일들이 디스크에서 구성되는 방식으로 디스크 위에 데이터를 어떻게 기록해야 할지에 대한 규칙이다. 리눅스 파일시스템은 EXT2, EXT3, EXT4가 있다.

2016년 07회

200. 파일시스템 점검의 명령어는?

① chgrp ② mount ③ fsck ④ df

정답 3

fsck

- 파일 시스템을 점검하고 복구하는 명령어이다.
- 정전 혹은 예기치 못한 상황 발생으로 시스템 reset 시 컴퓨터를 다시 켜면 자동으로 파일 시스템을 복구하지 못할 경우가 있는데, 이때는 fsck 명령을 사용해서 수동으로 파일 시스템을 복구할 수 있다

2016년 08회

201. 리눅스 서버에서 외부의 모든 Ping of Death 공격을 방어하기 위하여 리눅스의 기본 커널 옵션을 조정하려고 한다. 적절한 명령어는?

① sysctl -w net.ipv4.icmp_echo_ignore_all=0
② sysctl -w net.ipv4.icmp_echo_ignore_all=1
③ sysctl -n net.ipv4.icmp_echo_ignore_broadcasts=1
④ sysctl -n net.ipv4.icmp_echo_ignore_broadcasts=0

정답 2

sysctl : 요약 실시간으로 커널의 파라미터를 설정한다.

2016년 07회

202. 리모트 컴퓨터로부터의 ping 명령에 대한 응답으로 "Destination Unreachable"을 되돌려 주고, 접속을 거절하기 위해 리눅스 방화벽에서 설정하는 타깃 명령어는 무엇인가?

① DROP ② DENY
③ REJECT ④ RETURN

정답 3

리눅스 iptables 주요 정책에는 ACCEPT(허용), DROP(차단), REJECT(차단), LOG(로깅) 등이 올 수 있다. REJECT가 DROP과 다른 점은 DROP시에는 차단과 함께 아무런 응답을 하지 않지만 REJCET의 경우 ICMP에러 응답을 전송한다.

2016년 07회

203. 리눅스 시스템의 커널에 내장된 툴로서 rule 기반의 패킷 필터링 기능, connection tracking 기능 등 다양한 기능을 제공하는 것은?

① TCP - Wrapper ② netcat
③ iptables ④ xinetd

정답 3

2014년 03회

204. 다음은 리눅스 시스템 최적화 모니터링 명령어들이다. 무엇을 모니터링 하는 명령어인가?

FREE, VMSTAT

① CPU문제점 점검 ② 메모리 문제점 점검
③ 디스크I/O문제점 점검 ④ 네트워크 문제점 점검

정답 2

vmstat : 요약 가상 메모리의 정보를 통계 형식으로 출력한다.

리눅스 run level p.587

리눅스 run level 종류

실행레벨	mode	설명
run-level 0	halt	시스템 종료. 런레벨 0은 시스템 종료를 의미한다.
run-level 1	Single user mode	**시스템 복원모드이다. 보통 부팅 시 에러가 발생하여 디버깅을 하러 진입하거나, 관리자가 암호를 변경할 때 사용한다.**
run-level 2	Multiuser mode, without NFS	NFS(Network File System)을 지원하지 않는 다중 사용자 모드로 네트워크를 사용하지 않는 텍스트 유저모드라고 할 수 있다.
run-level 3	Full muliuser mode	**기본적으로 사용하는 rul-level**로 일반적으로 커맨드를 접속하면 rul-level이 3번이이다.
run-level 4	unused	미사용
run-level 5	**X11**	rul-level 3의 GUI버전이다. (X-Window Mode)
run-level 6	reboot	시스템 재부팅을 의미한다.

표 267 Run Level

2018년 12회

205. 리눅스 부팅 레벨(Run Level)중 아래 설명에 맞게 나열한 것을 고르시오.

A: 단일 사용자 모드 B: 재시작 C: 다중 사용자 모드

① A: 레벨1, B:레벨3, C:레벨2
② A: 레벨1, B:레벨3, C:레벨6
③ A: 레벨1, B:레벨6, C:레벨3
④ A: 레벨1, B:레벨6, C:레벨2

정답	3

2017년 09회

206. 실행 레벨을 적절하게 고른 것은?

ㄱ. 단일 사용자 모드 ㄴ. 재부팅 ㄷ. 다중 사용자 모드

① ㉠ 실행레벨 1, ㉡ 실행레벨 6, ㉢ 실행레벨 3
② ㉠ 실행레벨 0, ㉡ 실행레벨 5, ㉢ 실행레벨 3
③ ㉠ 실행레벨 3, ㉡ 실행레벨 6, ㉢ 실행레벨 2
④ ㉠ 실행레벨 0, ㉡ 실행레벨 5, ㉢ 실행레벨 3

정답	1

2019년 14회

207. 리눅스 시스템에서 패스워드 복잡도를 설정하기 위해 /etc/pam.d/system-auth 를 편집하고 있다. 아래와 같은 설정을 위해 사용하는 옵션으로 옳지 않은 것은?

o 숫자를 1자 이상 포함 o 특수문자를 1자 이상 포함 o 영어 대문자를 1자 이상 포함 o 기존 패스워드와의 일치율 50%이상 금지

① ucredit=-1 ② difok=10
③ scredit=-1 ④ dcredit=-1

정답	3

패스워드 규칙을 적용 (vi /etc/login.defs)

- **패스워드의 최소길이 8자**
  pam_cracklib.so minlen=8
- **소문자 최소 1자**
  pam_cracklib.so lcredit=-1
- **대문자 최소 1자**
  pam_cracklib.so ucredit=-1
- **숫자 최소 1자**
  pam_cracklib.so dcredit=-1
- **문자와 숫자이외의 문자 최소 1자(특수문자)**
  pam_cracklib.so ocredit=-1
- **difok : 새 비밀번호와 이전 비밀번호의 문자가 겹치면 안 되는 문자의 수**

2018년 12회
208. 리눅스 PAM의 동작 절차를 바르게 나열한 것은?

(1) 해당 애플리케이션의 PAM 설정 파일을 확인한다. (2) PAM모듈은 성공 또는 실패 상태를 반환(Return)한다. (3) 사용자나 프로세스가 애플리케이션의 접근(Access)을 요청한다. (4) 스택은 계속해서 순서대로 확인되며, 실패 상태를 반환한다해서 중단되지 않는다. (5)스택의 PAM모듈이 리스트상의 순서대로 호출된다. (6) 모든 PAM모듈의 상태 결과가 종합되어 전체 인증 과정의 성공 또는 실패 상태를 반환한다.

① 3 - 2 - 1 - 5 - 4 - 6
② 3 - 2 - 1 - 5 - 6 - 4
③ 3 - 1 - 2 - 5 - 4 - 6
④ 3 - 1 - 5 - 2 - 4 - 6

정답 4

(3) 사용자나 프로세스가 애플리케이션의 접근(Access)을 요청한다.
(1) 해당 애플리케이션의 PAM 설정 파일을 확인한다.
(5) 스택의 PAM모듈이 리스트상의 순서대로 호출된다.
(2) PAM모듈은 성공 또는 실패 상태를 반환(Return)한다.
(4) 스택은 계속해서 순서대로 확인되며, 실패 상태를 반환한다해서 중단되지 않는다.
(6) 모든 PAM모듈의 상태 결과가 종합되어 전체 인증 과정의 성공 또는 실패 상태를 반환한다.

서버 보안 관리 p.588

2016년 07회
209. 서버관리자를 위한 보안 지침 중 옳지 않은 것은?
① 관리자 그룹 사용자의 계정을 최소화한다.
② 정기적으로 파일과 디렉터리의 퍼미션을 점검한다.
③ 관리자로 작업한 후에는 반드시 패스워드를 변경한다.
④ 웹 서버에서 생성되는 프로세스는 관리자 권한으로 실행되지 않도록 한다.

정답 3

2018년 12회

210. 아래 그림은 공격자가 웹 해킹을 시도하는 화면이다. 이래 화면의 URL을 고려할 때, 공격자가 이용하는 웹 취약점으로 가장 적절한 것은?

http://security.com/admin.php

① 관리자 페이지 노출 취약점
② 파일 다운로드 취약점
③ 파일 업로드 취약점
④ 디렉터리 리스팅(Directory Listing) 취약점

정답	1

■ 홈페이지 보안취약점 - 관리자페이지 노출 취약점

취약점 설명 및 사례

⑴ 취약점 설명

① 관리자 페이지 위치를 알지 못할 경우 일반적으로 많이 사용하는 관리자 페이지 명을 입력하여

관리자 페이지가 존재하는지 점검

예) 관리자 페이지 주소

http://admin.test.co.kr
http://www.test.co.kr/admin
http://www.test.co.kr/manager
http://www.test.co.kr/master
http://www.test.co.kr/system
http://www.test.co.kr/adm

② 사용자 인증을 통과하여 페이지에 접속한 후 인증과정 없이 중간 페이지에 접속을 시도하여 접속이 가능한지 점검

③ 웹서버 내부 파일명을 알고 있을 경우 웹서버에서 관리자 페이지로 이용되는 웹페이지(파일) 목록을 확인하여 웹 브라우저를 통해 직접 접속을 시도

버퍼 오버플로우(Buffer Overflow)공격 p.589

2016년 07회

211. 다음 중 네트워크 기반 서비스 거부 공격이 아닌 것은?

① 버퍼 오버플로우(Buffer Overflow)
② 스머프(Smurf)
③ SYN 플러딩(Flooding)
④ 티어드랍(Teardrop)

정답	1

2013년 01회

212. 다음 중에서 버퍼 오버플로우(Buffer Overflow)에 대한 설명으로 옳지 않은 것은?

① 다수의 프로세스간 자원사용에 대한 경쟁을 이용해 관리자 권한 획득

② 메모리에서 스택영역에 복귀주소를 가진다. 스택 오버플로우(Stack Overflow)는 복귀주소에 악성 모듈을 삽입하여 공격할 수 있다.

③ 힙(Heap)영역은 malloc 혹은 new의 동적 함수로 할당된다.

④ 버퍼 오버플로우(Buffer Overflow)는 제한된 메모리를 초과한다.

정답	1

레이스 컨디션(Race Condition) 공격

가) 개념

- Race Condition 상태는 Unix 시스템에서 다수의 프로세스가 서로 동일한 자원을 할당받기 위해 경쟁하는 상태를 나타내는 말이다.
- 다수의 프로세스 간 **자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능**하게 하는 공격 기법이다.
- **두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다**.
- 시스템 프로그램과 공격 프로그램이 서로 자원을 차지하기 위한 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로 파일에 접근을 가능하게 하는 공격방법을 말한다.

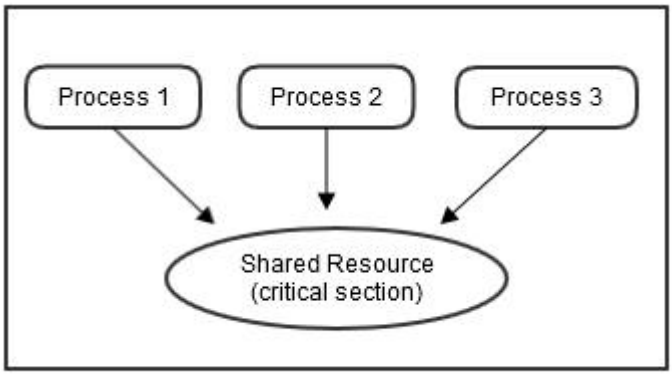

그림 33 Race Condition 상태

- 다중 프로그래밍 시스템이나 다중 처리기 시스템에서 두 명령어가 동시에 같은 기억장소를 액세스할 때 그들 사이의 경쟁에 의해 수행 결과를 예측할 수 없게 되는 것. 이와 같은 현상은 바람직하지 않으므로 운영 체제는 이것을 해소할 수 있어야 한다.

2019년 14회
213. 다음에서 설명하고 있는 공격은?

이 공격은 할당된 메모리 경계에 대한 검사를 하지 않는 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어쓰는 방식이다. 만약 실행 코드가 덮어써진다면 공격자가 원하는 방향으로 프로그램이 동작하게 할 수 있다.

① Buffer overflow 공격
② SQL injection 공격
③ IP spoofing 공격
④ Format String 공격

정답 1

버퍼오버플로우 공격은 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.

2016년 07회
214. 다음 내용은 어느 공격기법에 관한 설명인가?

침해 시스템을 분석하던 중 test라는 계정의 홈 디렉터리에서 C언어로 작성된 Exploit 코드와 컴파일된 바이너리 파일을 발견할 수 있었다. 이 Exploit은 stack에서 할당되어진 변수에 데이터를 초과 입력하여 RET를 덮어 씌워 ShellCode를 실행하는 코드였다.

① Buffer Overflow ② Format String
③ Race condition ④ Brute force

정답 1

2015년 06회
215. 메모리 오류를 이용해 타깃 프로그램의 실행 흐름을 제어하고, 최종적으로는 공격자가 원하는 임의의 코드를 실행하는 것을 무엇이라 하는가?
① 포맷 스트링 ② 버퍼 오버플로우
③ 레이스 컨디셔닝 ④ 메모리 단편화

정답 2