4주차 3차시. 리눅스/유닉스 인증과 패스워드

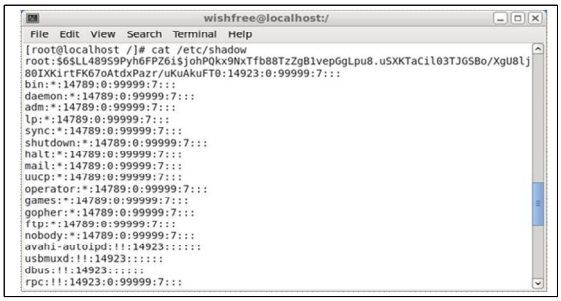
【학습목표】

1. 리눅스/유닉스 인증 및 패스워드 관리에 대해 설명할 수 있다.

학습내용1 : 리눅스/유닉스 인증

1. 리눅스/유닉스의 인증 방식

윈도우의 인증 방식보다 단순하지만 윈도우 인증 방식보다 취약하지는 않음
리눅스에서 인증 필수 요소
패스워드 파일 : 패스워드는 shadow 파일에 암호화되어 저장
shadow 파일: shadow 파일에서 root 계정에 대한 정보 확인
cat /etc/shadow



root : 6LL489S99Pyh6~중략~Pazr/uKuAkuFT0/ : 14923 : 0 : 99999 : 7 : : :
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

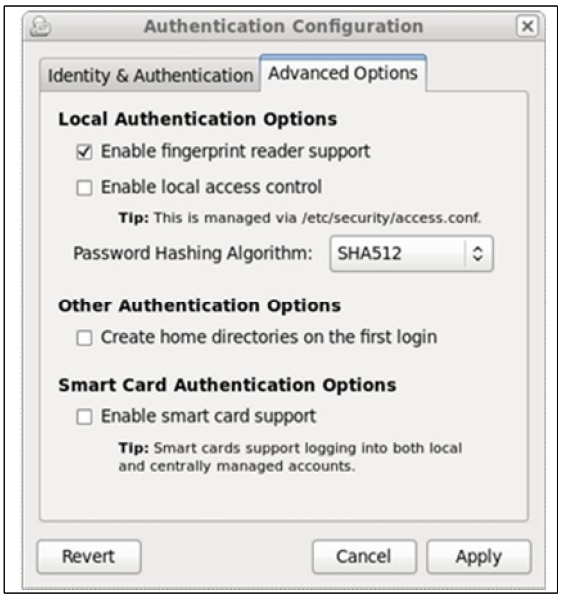
① 사용자 계정
② 암호화된 사용자의 패스워드 저장
1로 시작하면 MD5
5로 시작하면 SHA256
6로 시작하면 SHA512를 나타냄
③ 1970년 1월 1일부터 마지막으로 패스워드 변경한 날까지 계산 값
14923일은 약 41년
④ 패스워드 변경하기 전 패스워드 사용한 기간
최초 설정 후 바꾸지 않았으므로 0
⑤ 패스워드 바꾸지 않고 최대한 사용할 수 있는 기간
이 값은 보안 정책에 따라 변경 됨
보통 패스워드의 최대 사용 기간을 60일로 권고
⑥ 패스워드 최대 사용 기간에 가까워질 경우 사용자에게 미리 통지
패스워드 사용 기한 며칠 전에 경고를 보낼지 지정

⑦ 계정에 대한 사용 제한을 설정
며칠 후에 완전히 사용 정지할지 설정
⑧ 1970년 1월 1일부터 계정이 완전 사용 정지된 기간 계산 값 기록
⑨ 관리자 임의 사용 부분

· 로직이 정형화되어 있지 않음
· 운영체별로 다르며 기본적으로 대부분 Salt와 해시를 이용

2. 페도라 14의 인증 방식

· 기본값으로 SHA512 해시 알고리즘 사용
· [System]-[Administration]-[Authentication] 메뉴 선택 하면 'Advanced option'에서 추가적으로 MD5, SHA256 등의 알고리즘 선택 가능



3. 전형적인 리눅스의 인증 방식

passwd 파일과 shadow 파일을 이용
· /etc/passwd: passwd 파일은 대부분 /etc/passwd 파일로 동일
· /etc/shadow: shadow 파일은 운영체제별로 고유한 경로와 파일명을 사용하는 경우도 많음

4. 운영체제별 passwd와 shadow 파일 위치

운영체제	Shadow 파일 위치
IBM AIX	/etc/security/passwd
IBM A/ux 3.0.3 (RS-6000)	/tcb/file/auth/?/*
BSD 4.3 - Reno	/etc/master.passwd
DEC DG/ux (Digital Unix)	/etc/tcb/aa/user
DEC EP/ux	/etc/shadow
HP/ux	./secure/etc/passwd
IRIX 5	/etc/shadow
Free BSD	/etc/shadow
SunOS 4.1 + C2	/etc/security/passwd.adjunct
SunOS 5.x	/etc/shadow, passwd
System V Release 4.0	/etc/shadow, passwd

학습내용2 : 리눅스 패스워드 크래킹

1. 주제

리눅스 패스워드 크래킹

2. 참고

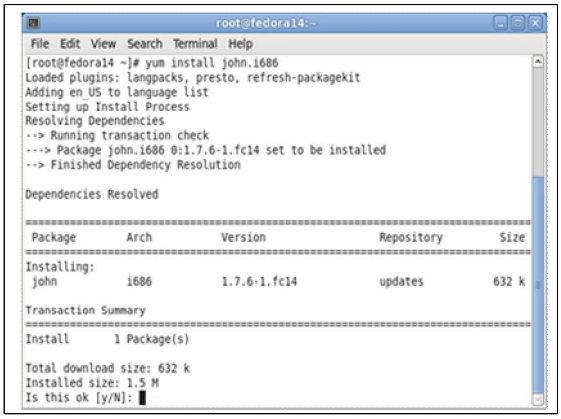
· 한빛미디어
· 정보 보안 개론과 실습 : 시스템 해킹과 보안
· 199페이지
· 실습 4-2. 리눅스 패스워드 크래킹하기

3. 실습 환경 및 내용

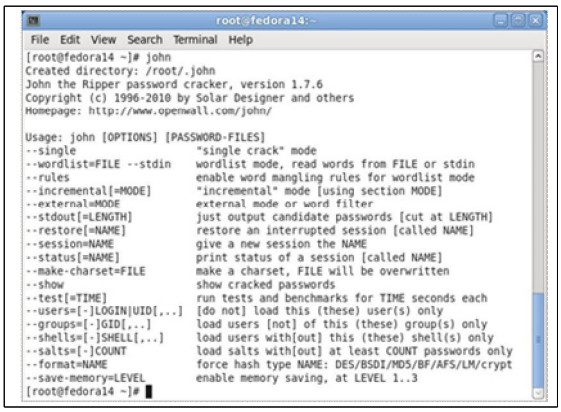
· 페도라 14
· John-the-ripper를 이용한 무작위 대입 공격

4. John-the-ripper 설치

Yum(Yellow dog Updater, Modified)을 이용한 설치
Yum이란?
RPM 기반의 시스템을 위한 자동 업데이터 및 패키지 설치/제거 도구
패키지 설치 : yum install 패키지명
패키지 삭제 : yum remove 패키지명
패키지 업그레이드 : yum update 패키지명



5. John-the-ripper 명령어



6. 테스트 계정 생성

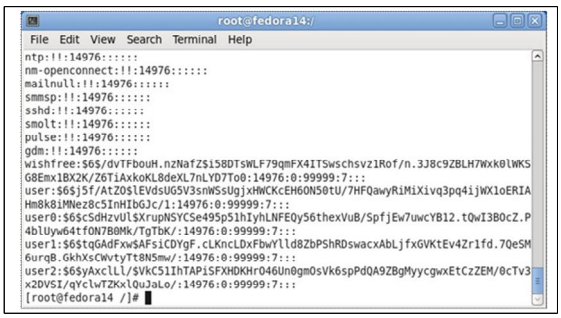
useradd user

7. 테스트 계정 패스워드 설정

passwd user

8. 테스트 계정의 패스워드 정보 확인

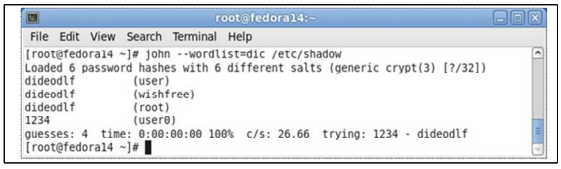
cat /etc/shadow



9. 사전 대입법을 이용한 패스워드 크래킹

John-the-ripper를 이용
'dideodlf' 이라는 단어를 입력해둔 사전파일을 이용

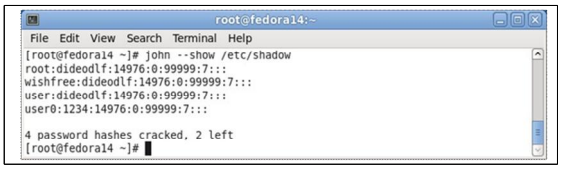
john --wordlist=dic /etc/shadow



10. 무작위 대입법을 이용한 패스워드 크래킹

사전 대입 공격이 실패할 경우 사용
--wordlist 옵션 없이 실행

john --show /etc/shadow



학습내용3 : 리눅스 패스워드 복구

1. 주제

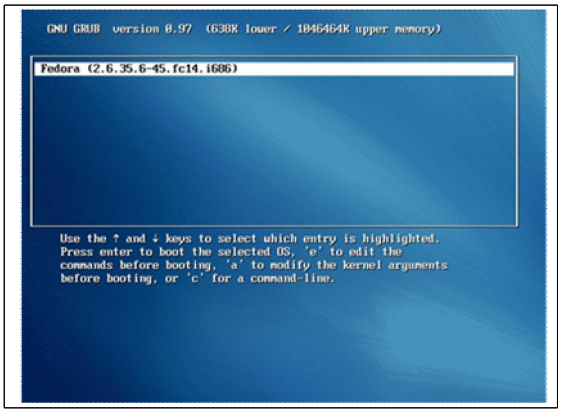
리눅스 패스워드 복구

2. 참고

· 한빛미디어
· 정보 보안 개론과 실습: 시스템 해킹과 보안
· 212페이지
· 실습 4-5. 리눅스 패스워드 복구하기

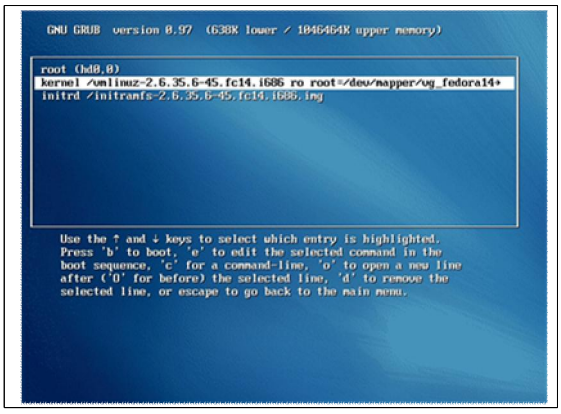
3. GRUB을 이용한 싱글 모드 부팅

GRUM 화면에서 e를 누름



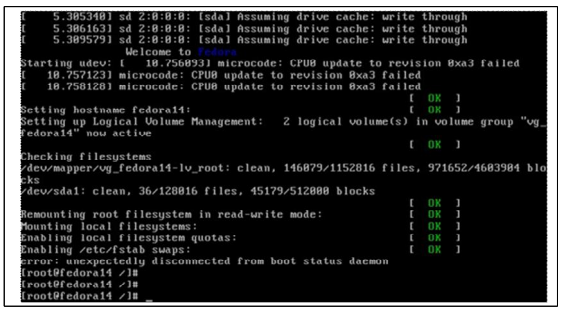
5. 싱글 모드 부팅 설정

Kernel 선택 후 e를 누름



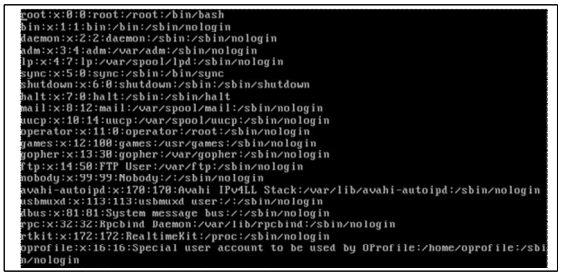
6. 싱글 모드 부팅

패스워드 입력 없이 셸을 획득할 수 있음

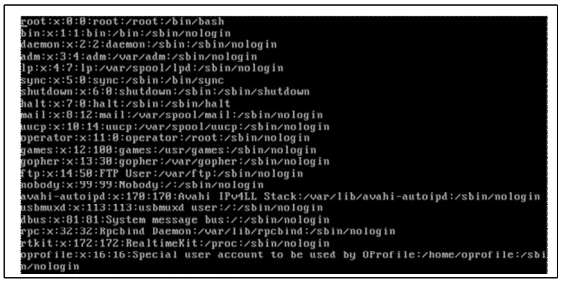


7. 패스워드 파일 수정

편집기를 이용하여 /etc/shadow 내용 중 패스워드를 새로 설정할 계정의 x를 지우고 저장 후 부팅
이후 로그인할 때 패스워드를 물어보지 않음



편집기를 이용하여 /etc/shadow 내용 중 패스워드를 새로 설정할 계정의 x를 지우고 저장 후 부팅
이후 로그인할 때 패스워드를 물어보지 않음



【학습정리】

1. 윈도우의 패스워드를 분실한 경우 복구용 CD를 이용하여 패스워드를 초기화하는 방법을 사용한다.

2. 리눅스/유닉스 시스템에서 패스워드를 분실한 경우 싱글모드 부팅을 통해 비밀번호를 삭제하는 방법이 있다.