계정 관리

계정/그룹 관리 파일

1) 파일 /etc/passwd

- 사용자들의 기본 정보를 저장하는 파일
- 시스템에 로그인하여 자원을 이용할 수 있는 사용자의 목록을 저장하고 있는 정보파일
- /etc/passwd에는 콜론(:)을 구분자로 7개의 기본적인 정보를 담고 있음

username : password : uid : gid : comment : homedirectory : shell

① ② ③ ④ ⑤ ⑥ ⑦

①	**사용자 이름(계정명)**	
②	**암호화된 비밀번호**	
③	**사용자의 UID**	사용자에게 부여한 번호 (계정명은 중복이 안되지만, UID는 중복 가능)
④	**사용자의 GID**	해당 사용자가 속해 있는 주그룹 ID
⑤	**설명(주석)**	
⑥	**사용자 홈 디렉토리**	
⑦	**실행 프로그램**	일반적으로 사용자가 로그인 시 실행되는 shell 지정

❶ 계정명

- 사용자 역할에 따라 root, 일반 사용자, 시스템 계정으로 분류

root	• 시스템운영에 있어서 모든 권한을 행사(Privileged User 또는 Super User) • Root UID(User Identity)는 0 할당 (UID 0번 사용자를 슈퍼유저로 인식)
일반 사용자	• 로그인이 가능한 사용자(Normal user 또는 Unprivileged user라 부름) • 시스템에 대해 제한적인 권한을 행사
시스템 계정	• 로그인은 되지 않고 시스템의 필요에 의해 생성된 계정 - /etc/passwd 파일에 bin, daemon, adm, game 등 관리자가 생성하지 않는 계정들이 존재 • 시스템 필요에 의해 생성된 계정 • 시스템 계정이 없다면 모든 파일 생성과 프로세스 생성 시에 root 권한이 부여되어야 함

<<시스템 계정>>

root	시스템에서 모든 권한을 가지고 있는 최고 권한 사용자 시스템 내의 보호되는 파일이나 권한 등의 제한 사항에 대해 영향을 받지 않음
bin	시스템의 구동중인 실행 파일을 관리하기 위한 계정
daemon	백그라운드 프로세스에 대한 작업을 제어하기 위한 시스템 계정
adm	시스템 로깅이나 특정 작업을 관리하는 시스템 계정
lp	프린터 관리를 위한 계정
gdm	Gnome display를 관리 계정

❷ UID(User ID)

- 시스템이 사용자를 식별하는 번호
- 리눅스에서는 사용자를 숫자값 형태의 UID(User Identity)로 관리
- 계정명은 중복이 불가능하지만, UID는 중복이 가능
- UID로 root 권한을 가질 수 있음

<<버전 별 UID 범위 비교>>

계정자	CentOS 6 이전	CentOS 7
root	0	0
시스템 계정	1~499	1~999
일반 사용자	500번부터 할당	1000번부터 할당

[중요] root 이외 UID ‘0’ 금지

- root(UID=0)와 동일한 UID를 가진 계정 존재 시 root 권한 으로 시스템 접근이 가능
- 사용자간 UID 중복시에 권한 중복으로 사용자 감사 추적이 어려움

2) 파일 /etc/shadow

- 사용자 패스워드 저장
- /etc/passwd의 두 번째 필드인 패스워드 부분을 암호화하여 관리
- root 사용자만 접근할 수 있고, 총 9개 필드로 구성
- 패스워드 만기일, 계정 만기일 등을 설정

username : password : lastchange : mindays : maxdays : warndays : inactive :expire : flag

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

①	사용자명
②	암호화된 비밀번호(역으로 풀수 없다)
③	최근 비밀번호 변경일(1970년 1월 1일 기준의 날짜 수 : timestamp)
④	패스워드 최소 사용 일 수
⑤	패스워드 최대 사용 일 수 (예) 15일 경우, 15일이 지나면 패스워드 변경 유도가 진행
⑥	패스워드 만료 전(또는 계정만료 전⑧) 해당 사항을 경고 메시지로 알려줌
⑦	inactive(휴면계정, 지정기간동안 로그인이 안된 경우 잠금 계정으로 지정) 유효 기간 (10일이면, 10일에 한번도 로그인을 되지 않으면 휴면계정으로 전환) 계정자가 로그인을 시도하면 다시 활성화가 됨
⑧	패스워드 만료일 또는 계정 만료일, 비밀번호 만료 기간 이후 해당 계정을 더 이상 사용할 수 없게 되는 날
⑨	나중에 사용하기 위해 예약으로 설정되어 있고, 현재는 사용되지 않으며, 0으로 지정

❶ 패스워드

- 암호화된 패스워드 필드 구성

$ID $Salt $Encrypted_password

(ex) 6LL489S99$PyhPazr/uKuAkuFT0

Hash(password) ➔ 암호문1
Crypt(암호문1 + Salt) ➔ 암호문2

ID	해시알고리즘 명시 1 : MD5 , 2 : BlowFish , 5 : SHA-256 , 6 : SHA-512
Salt	패스워드 암호화 강도를 높이기 위한 임의 값 운영체제에서 Random하게 만들어내는 값 **동일한 패스워드에 서로 다른 패스워드 값 산출 (같은 암호를 사용시 혼락막음)**
Encrypted_password	사용자 패스워드에 Salt를 조합해서 해시한 해시값 * : 패스워드가 잠긴 상태로 로그인 불가(SSH 인증로그인 가능) !! : 패스워드가 잠긴 상태로 모든 로그인 불가 공백 : 패스워드가 설정되지 않은 상태

명령어 pwconv

#pwconv ➔ shadow 패스워드 정잭 적용

#pwunconv ➔ 일반 패스워드 정책 적용

#pwck ➔ password check약자 (예) pwck –r 또는 pwck /etc/passwd

* /etc/passwd와 /etc/shadow 점검
* 각 사용자의 필드 개수 검사, 아이디중복 유무 검사, 유효한 사용자 여부검사, 유효한 UID및 GUI 여부 검사
* 사용자의 primary 그룹 존재 유무검사
* 홈 디렉터리 존재 유무검사, 로그인 셀 검사 등을 함

❷ lastchange/warndays/expire

username : password : lastchange : mindays : maxdays : warndays : inactive :expire : flag

root : 6LL489S99PyhPa0 : 18198 : 2 : 9 : **2** : **10** : **18261** :

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

3) /etc/group

- 그룹 정보 저장
- 그룹 목록이 들어 있는 파일로 4개의 필드로 구성

필드	설명
GroupName	그룹이름, 보통 groupadd 명령으로 생성한 그룹명
Password	그룹 패스워드를 나타내는 부분 리눅스 배포판에서는 그룹패스워드도 /etc/gshadow에서 별도로 관리 별도로 관리되는 경우에는 'x'라고만 나타남
GID	리눅스에서 그룹에 부여한 숫자값
Member_List	해당 그룹에 속한 사용자의 아이디가 기록 주 그룹(Primary Group)이 아닌 2차 그룹(Secondary Group) 멤버들이 기록

그룹(Group) 개요

- 서버에 존재하는 많은 사용자 중에 특정 사용자끼리 파일 공유할 때 유용
- 사용자들을 같은 그룹으로 묶어서 Permission 설정을 통해 파일/디렉터리를 공유
- 모든 사용자는 하나 이상의 그룹에 반드시 속하도록 설정
- 레드햇 계열에서는 사용자간의 불필요한 공유를 막기 위해 사용자의 아이디와 동일한 그룹을 생성해서 단독으로 그룹에 포함

4) /etc/gshadow

- 그룹 암호를 관리하는 파일로 4개의 필드로 구성

필드	설명
GroupName	그룹이름
Password	그룹 패스워드가 기록 그룹의 패스워들 설정하지 않으면 '!'로 표시 gpasswd 명령으로 설정하면 암호화된 패스워드가 기록 SHA-512 알고리즘을 사용해서 $6으로 시작하는 패스워드가 기록 다른 그룹에 속한 사용자가 newgrp명령을 이용해서 해당 그룹으로 변경 가능
Admin	그룹관리자가 기록
Member_List	그룹의 멤버를 나타냄 보통 2차 그룹으로 속한 사용자의 아이디가 기록되며 여러 명이 존재할 수도 있음 여기에 등록된 사용자는 newgrp명령으로 주 그룹(Primayr Group)으로 전환 할 때 패스워드를 묻지 않음

3.2 계정/그룹 관리 명령어

❶ 명령어 useradd (또는 adduser)

[사용법] # useradd [option] **사용자계정이름**

옵션	설명
-p	사용자의 암호를 추가 시에 지정
-d	홈디렉터리 지정
-g	그룹 지정
-e	사용자 계정 만기일 지정

옵션	설명
-u	사용자 계정의 UID 지정
-g	사용자 계정의 GID 지정
-s	기본 쉘 지정
-f	계정 유효일 지정

[사용예]

 # useradd user01 → user01이라는 계정을 생성

 # useradd user02 -d /home/TEST → user02이라는 사용자를 생성하면서 홈 디렉터리의 경로 지정

date : 오늘의 날짜 확인
useradd -e 2023-10-31 user03 : 계정만료일 2023년 10월 31일로 설정하고 계정 생성
useradd –e 2023-11-01 user04 : 계정만료일 2023년 11월 01일로 설정하고 계정 생성

```
[root@localhost ~]# date
2023. 10. 01. (일) 09:14:00 KST
[root@localhost ~]# useradd -e 2023-10-31 user03
[root@localhost ~]# useradd -e 2023-11-01 user04
[root@localhost ~]#
[root@localhost ~]# tail -4 /etc/passwd
user01:x:1001:1001::/home/user01:/bin/bash
user02:x:1002:1002::/home/TEST:/bin/bash
user03:x:1003:1003::/home/user03:/bin/bash
user04:x:1004:1004::/home/user04:/bin/bash
[root@localhost ~]#
[root@localhost ~]# tail -4 /etc/shadow
user01:!!:19631:0:99999:7:::
user02:!!:19631:0:99999:7:::
user03:!!:19631:0:99999:7::19661:
user04:!!:19631:0:99999:7::19662:
[root@localhost ~]#
```

사용자 계정 만료일
(1970년 1월1일부터 설정한 날까지의 시간(단위, 일))

useradd -f 3 –e 2023-10-31 user05

- 계정만료일 2023년 10월 31일로 설정하여 계정 생성
- 3일동안 로그인을 하지 않을 경우 locking

```
[root@localhost ~]# useradd  -f 3  -e 2023-10-31 user05
[root@localhost ~]# tail -1 /etc/passwd
user05:x:1005:1005::/home/user05:/bin/bash
[root@localhost ~]# tail -1 /etc/shadow
user05:!!:19631:0:99999:7:3:19661:
[root@localhost ~]#
```

설정된 날짜까지 로그인하지 않을 경우
사용자 계정은 잠김(locking)

```
[root@localhost ~]# cat -n /etc/shells
     1  /bin/sh
     2  /bin/bash
     3  /sbin/nologin
     4  /usr/bin/sh
     5  /usr/bin/bash
     6  /usr/sbin/nologin
     7  /bin/tcsh
     8  /bin/csh
[root@localhost ~]#
```

시스템에서 사용할 수 있는 쉘 종류 확인

❷ 명령어 usermod

[사용법] # usermod [option] **사용자계정이름**

옵션	설명
-d	사용자의 홈디렉터리 변경
-m	홈디렉터리변경 시 기존 사용 했던 파일 및 디렉터리를 이동
-g	사용자 그룹 변경
-s	사용자 shell qusrud

옵션	설명
-u	사용자 UID 변경
-e	계정 만료일 변경
-f	계정 유효일(inactive) 변경
-l	사용자 계정명 변경

[사용예]

 # usermod –d /home/TEST –m user01 // 사용자 홈 디렉터리를 변경, 이동된 디렉터리로 파일 변경

 # usermod –g terran drone //drone이란 사용자 그룹을 terran으로 변경

#usermod –s /bin/sh user01 //user01의 사용자 쉘을 /bin/sh로 변경

❸ 명령어 passwd

- useradd로 계정을 생성한 후에 암호를 지정하지 않으면 로그인이 되지 않음
- passwd만 입력하면 현재 로그인 사용자의 암호 변경
- root만 다른 사용자의 암호를 변경

[사용법] **# passwd** [사용자명]

[사용 예] $ passwd

→ 현재 로그인한 사용자 본인의 암호를 변경

passwd gildong

→ gildong 사용자의 암호를 변경

[사용법] **# passwd [option] 사용자명**

#passwd –l gildong	패스워드 잠금 설정, 로그인을 막음 /etc/shadow의 두번째 필드 '!!'을 넣어서 막음
#passwd –u gildong	패스워드 잠금 해제
#passwd –d gildong	패스워드 제거
#passwd –e gildong	사용자가 다음 로그인 시 패스워드를 변경하도록 설정

❹ 명령어 chage

- 사용자의 패스워드에 대한 정보를 출력하고 설정하는 명령어
- /etc/shadow의 날짜관련 필드 설정

#chage –l gildong • 사용자 패스워드 정보를 보여줌
#chage –m 10 –M 100 –W 5 gildong • 최소 사용 날짜 : 10일(-m) • 최대 사용 가능한 날 : 100일(-M) • 패스워드만기일 5일전에 경고메세지 보냄 (-W 5)

/etc/shadow와 날짜관련 명령어 옵션비교

username : password : last : may : must : warn : expire : disable : reserved

chage	-d	-m	-M	-W	-I	-E
passwd		-n	-x	-w	-i	
usermod					-f	-e

❺ 명령어 userdel

- 옵션 –r : 사용자의 홈 디렉터리와 메일 관련 파일까지 삭제

❻ 명령어 groupadd

- 새로운 그룹을 생성하는 명령으로 root만 사용 가능한 명령어

[사용법] # groupadd [option] 그룹명

[사용 예] # groupadd test → test이라는 그룹을 생성

❼ 명령어 groupmod

- 그룹명이나 GID를 변경할 때 사용하는 명령

[사용법] # groupmod [option] 그룹명

[사용 예] # groupmod –n TEST test

→ test 그룹의 이름을 TEST 으로 변경

groupmod –g 555 TEST

→ TEST 그룹의 GID를 555로 변경

❽ 그룹 환경 설정 변경 : gpasswd

- 그룹의 패스워드를 설정하거나 그룹관리자를 지정하는 명령어
- 그룹관리자는 해당 그룹에 속하지 않아도 지정 가능
- 지정된 그룹관리자는 다른 사용자들을 해당 그룹에 2차 그룹으로 속하게 하거나 그룹 패스워드를 설정
- 그룹 패스워드가 설정되면, 해당 그룹에 속하지 않은 사용자들이 newgrp 명령을 이용하여 그룹 패스워드 입력 후에 일시적으로 1차 그룹을 변경 할 수 있음

[사용법] $ gpasswd [options] group

[사용 예] #gpasswd -A posein TEST

→ terran 그룹의 관리자로 posein을 지정

posein이라는 사용자는 실제적으로 terran그룹의 일원이 아니어도 가능

→ 관리자등록은 /etc/gshadow에 3번째 필드에 기록

gpasswd –a user01 TEST → user01 사용자를 test 그룹에 포함

gpasswd -d user01 TEST → user01 사용자를 test 그룹에서 제외

❾ 명령어 groupdel

- 생성된 그룹을 삭제하는 명령
- 삭제할 그룹에 속한 사용자가 없어야 하는데, 2차 그룹(Secondary Group)으로 속한 사용자들은 존재해도 상관없음

[사용법] # groupdel 그룹명

[사용예] # groupdel TEST → hong 그룹을 삭제

Password Cracking

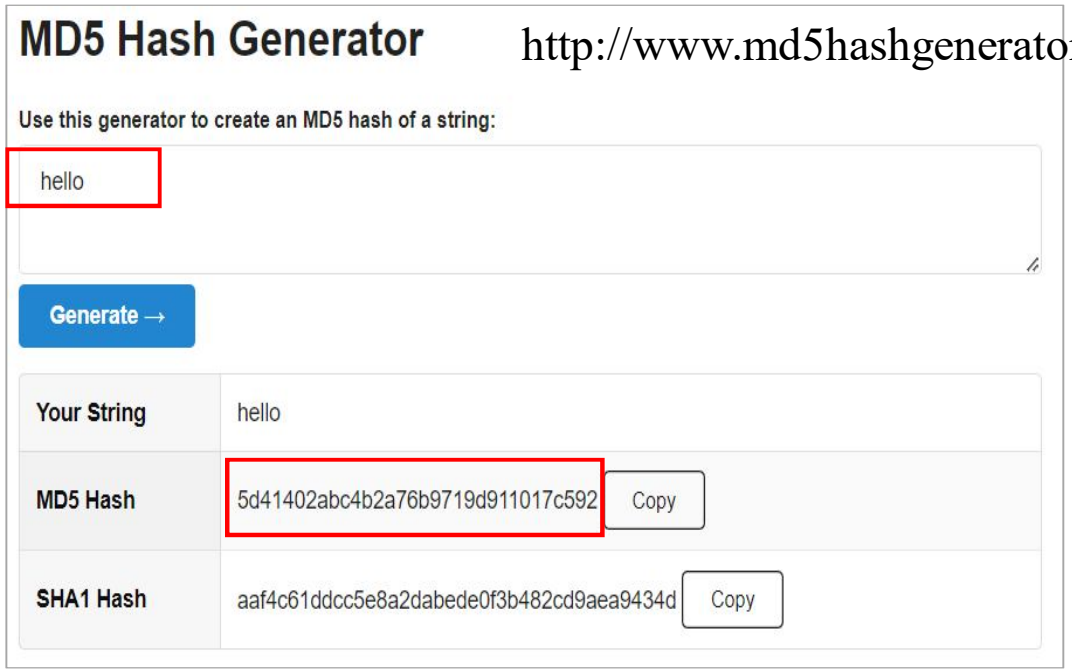
Password Cracking

- 공격대상의 ID를 알고 있다는 전제 하에 비밀번호를 알아내는 공격 기법

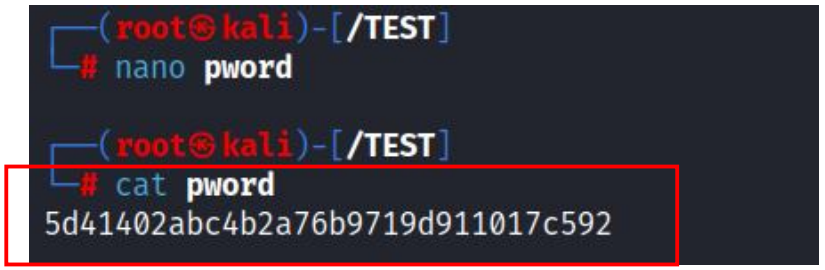
사전 대입 공격 (Dictionary attack)	패스워드로 사용할 만한 사전 파일을 미리 만들어 놓고 하나씩 대입하여 패스워드 일치 여부를 확인
무차별 대입 공격 (Brute-force attack)	가능한 모든 경우의 수를 모두 대입
레인보우 테이블 공격 (Rainbow table attack)	패스워드와 해시로 이루어진 체인을 무수히 만들어 테이블에 저장한 다음, 암화화 값을 데이블에서 찾는 방법
사회공학 기법 (Social Engineering)	개인 정보가 들어 있는 비밀번호 사용 자신의 이름을 사용 또는 생년월일, 전화번호 등 상대방을 속여 비밀번호 획득 또는 카페나 도서관에서 대화내용을 수집

Lab 1. 해쉬 값 기반의 패스워드 크래킹

❶ 해쉬 값 생성



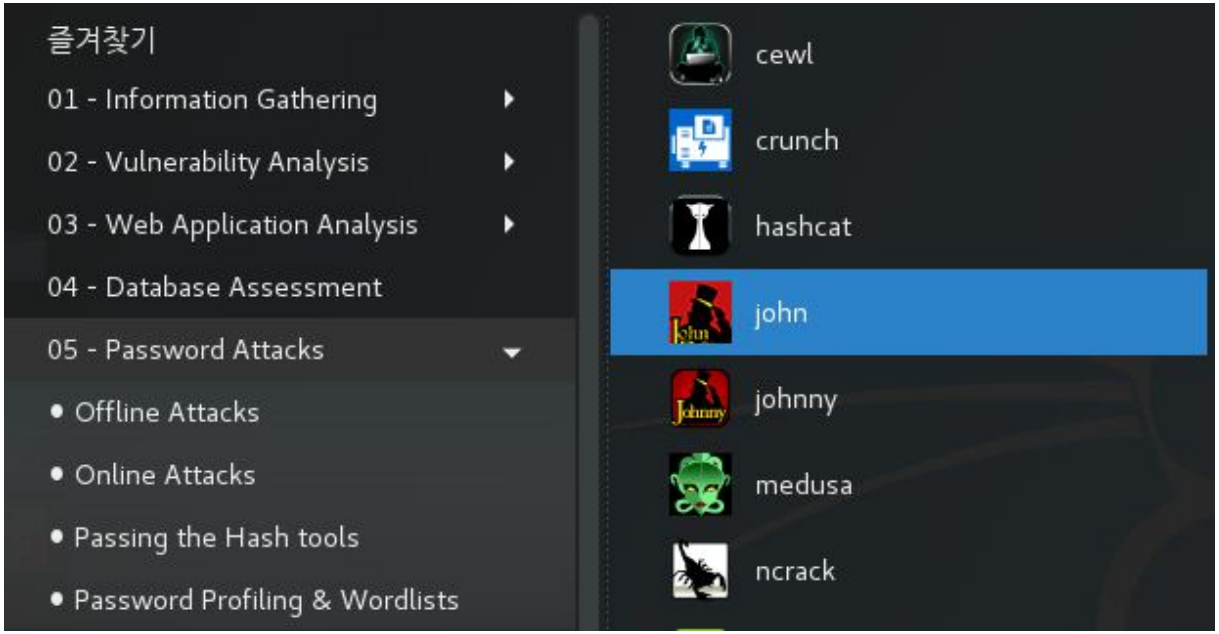
❷ 해쉬 파일 생성



#nano /TEST/pword

❸ John The Ripper 실행

즐겨찾기 > 05. Password Attacks > john



❹ John The Ripper를 이용한 해쉬 값 복원

#john --format=raw-md5 /usr/share/wordlists/rockyou.txt.gz /TEST/pword

```
┌──(kali㉿kali)-[~]
└─$ ls -l /usr/share/wordlists/rockyou.txt.gz

-rw-r--r-- 1 root root 53357329 May 31  2022 /usr/share/wordlists/rockyou.txt.gz

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 /usr/share/wordlists/rockyou.txt.gz /TEST/pword
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt.gz
Warning: UTF-16 BOM seen in password hash file. File may not be read properly unless you re-encode it
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
hello            (?)
1g 0:00:00:00 DONE 2/3 (2023-10-01 21:22) 100.0g/s 19200p/s 19200c/s 19200C/s 123456..knight
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Lab 2. 패스워드 파일의 패스워드 크래킹

❶ Crack 파일 만들기

#cd /TEST

#cp /etc/passwd passwd

#cp /etc/shadow shadow

#unshadow passwd shadow | grep '\$y' | tee passcrack

❷ Password Cracking

#john passcrack --wordlist /usr/share/wordlists/fasttrack.txt --format=crypt

❸ 결과 확인

#john –show passcrack

```
┌──(root㉿kali)-[/TEST]
└─# unshadow passwd shadow | grep '\$y' | tee passcrack
kali:$y$j9T$lR7REZ4XgU56yXNl9PFiN/$oI3B/OeQGXOoTb7opQ.azBMOgG2IM0neRj4MN3HCqQ.:1000:1000:,,,:/home/kali:/usr/bin/zsh
gildong:$y$j9T$6lVdyOfzeXObyp8nMdWr30$UJ8DOvSh11DHnwkQLEypo3Jz9fyfmBwmNleRJyRueC1:1001:1001:,,,:/home/gildong:/bin/ba
hong:$y$j9T$icu6Yki9TxcTBmcRNjldr0$xaXrYzTwmhUHeaLuZAuDlMrKOdpkAPtMkWdksCK3DaC:1002:1002:,,,:/home/hong:/bin/bash

┌──(root㉿kali)-[/TEST]
└─# john passcrack --wordlist /usr/share/wordlists/fasttrack.txt --format=crypt
Warning: hash encoding string length 15, type id #0
appears to be unsupported on this system; will not load such hashes.
Using default input encoding: UTF-8
Loaded 5 password hashes with 4 different salts (1.3x same-salt boost) (crypt, generic crypt(3) [?/64])
Remaining 2 password hashes with no different salts
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 1 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2023-10-01 23:16) 0g/s 354600p/s 354600c/s 709200C/s !@#$%..sss
Session completed.

┌──(root㉿kali)-[/TEST]
└─# john --show passcrack
kali:kali:1000:1000:,,,:/home/kali:/usr/bin/zsh
gildong:1234:1001:1001:,,,:/home/gildong:/bin/bash
hong:1234:1002:1002:,,,:/home/hong:/bin/bash

3 password hashes cracked, 0 left
```

[참고] #john –list=formats

패스워드 관리 정책

1) 패스워드 정책

- 대/소문자, 숫자, 특수문자를 혼용하여 8개 글자 이상의 패스워드를 사용
- 동일 문자를 연속 4회 이상 사용 금지
- 패스워드 히스토리를 관리하여 2~3개 이상의 동일 패스워드 사용금지
- 패스워드 변경주기를 설정(패스워드 유효기간을 90일 이하로 설정)
- 사전에 나오는 쉬운 단어나 이름은 패스워드로 사용하지 못하도록 설정
- 기본 설정된 패스워드는 사용하지 못하도록 설정
- 초기 부여된 패스워드는 사용자 최초 접속 시 변경하도록 설정

2) 패스워드 정책 설정 파일 /etc/security/pwquality.conf

difok = N	기존 패스워드와 비교. 기본값 10(50%)
minlen = 8	최소 패스워드 길이 설정
dcredit = -1	최소 필요한 숫자 수
ucredit = -1	최소 필요한 대문자 수
lcredit = -1	최소 필요한 소문자 수
ocredit = -1	최소 필요한 특수문자 수
maxrepeat = 3	최대 연속된 동일한 반복 수 (예 aaa,111 형태를 사용 못함)
maxclassrepeat = 3	최대 연속 문자 반복 수 [최소 3 이상 권장] (예 abc,123 형태를 사용 못함)
usercheck = 1	패스워드에 유저 ID가 포함되어 있는지 점검 [1 권장/0 체크 안 함] (예 ID:gildong PASS:gildong123 형태를 사용 못함)
retry = 3	패스워드 입력 실패 시 재시도 횟수

3) 패스워드 기본값 설정 파일 /etc/login.defs

- 사용자 추가할 때 참고하는 메일 디렉터리
- 패스워드 관련 설정(최대 사용기한, 최소 사용기한, 최소 길이, 만기 이전 경고 주는 날짜)
- UID의 최소값 및 최대값
- GID의 최소값 및 최대값
- 홈 디렉터리 생성 여부
- 기본 umask 값
- 패스워드에 적용되는 암호화 알고리즘 등이 정의되어 있는 파일

4) 패스워드 관련 명령어 passwd

- 패스워드를 부여하거나 변경
- 사용자명을 입력하지 않으면 현재 사용자의 패스워드로 변경
- 계정을 사용하지 못하게 하거나 패스워드 만기일 및 유효기간을 설정

[사용법] **# passwd [option] [사용자명]**

-n	패스워드 변경 후 최소 사용 기간
-x	패스워드 변경 후 최대 사용 기간
-w	패스워드 만기일 이전에 사용자에게 경고 메시지를 전달할 날짜 지정
-e	최초 로그인 시에 강제로 패스워드를 변경하도록 설정
-d	passwd 입력 없이 로그인 가능 (shadow 파일의 패스워드 필드 값 제거)
-l	해당 사용자의 상태를 locking으로 변경
-S	해당 사용자의 현재 패스워드 설정 조회