Password Cracking

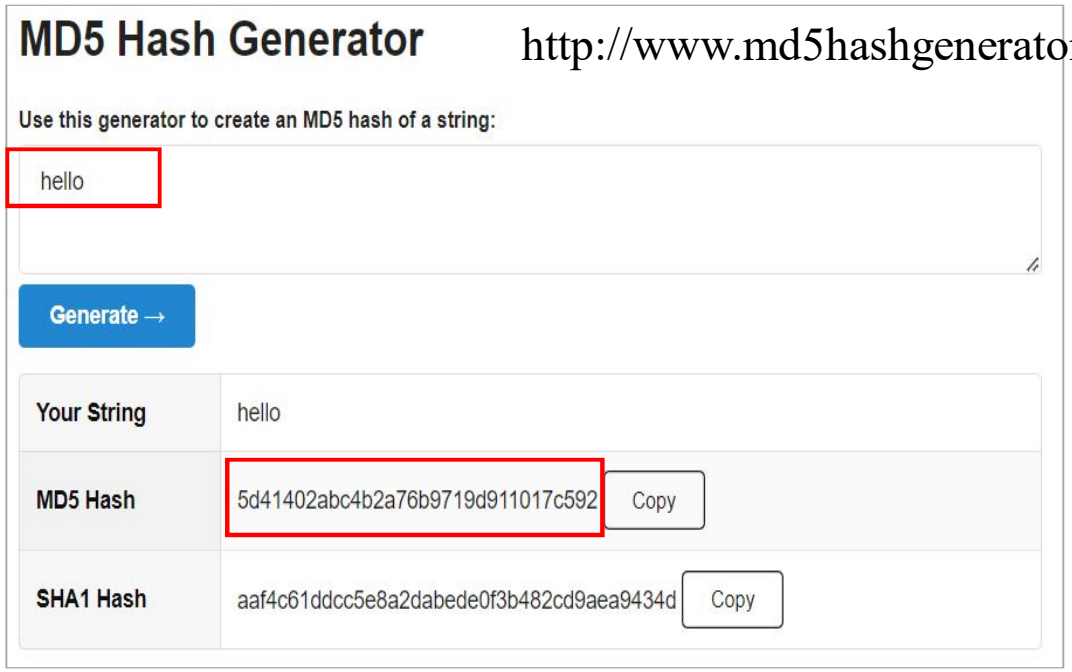
Password Cracking

- 공격대상의 ID를 알고 있다는 전제 하에 비밀번호를 알아내는 공격 기법

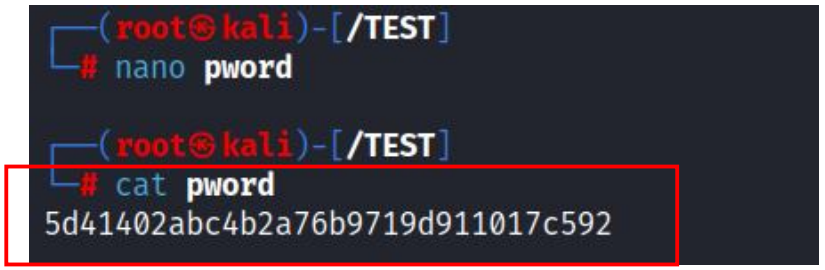
사전 대입 공격 (Dictionary attack)	패스워드로 사용할 만한 사전 파일을 미리 만들어 놓고 하나씩 대입하여 패스워드 일치 여부를 확인
무차별 대입 공격 (Brute-force attack)	가능한 모든 경우의 수를 모두 대입
레인보우 테이블 공격 (Rainbow table attack)	패스워드와 해시로 이루어진 체인을 무수히 만들어 테이블에 저장한 다음, 암화화 값을 데이블에서 찾는 방법
사회공학 기법 (Social Engineering)	개인 정보가 들어 있는 비밀번호 사용 자신의 이름을 사용 또는 생년월일, 전화번호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

Lab 1. 해쉬 값 기반의 패스워드 크래킹

❶ 해쉬 값 생성



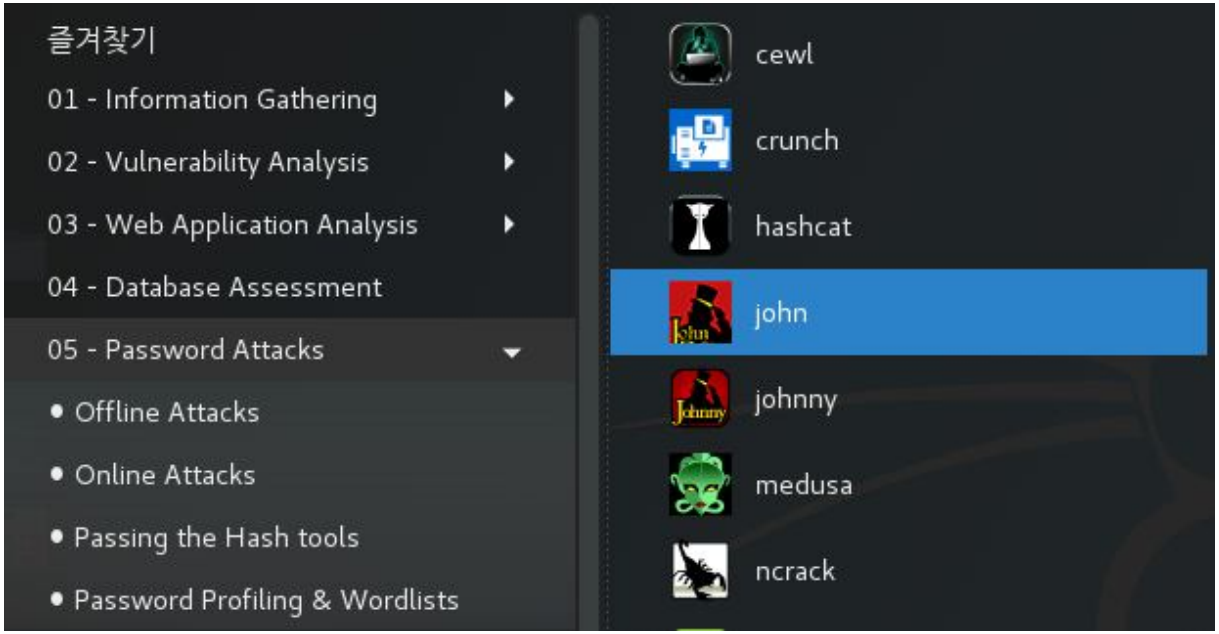
❷ 해쉬 파일 생성



#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

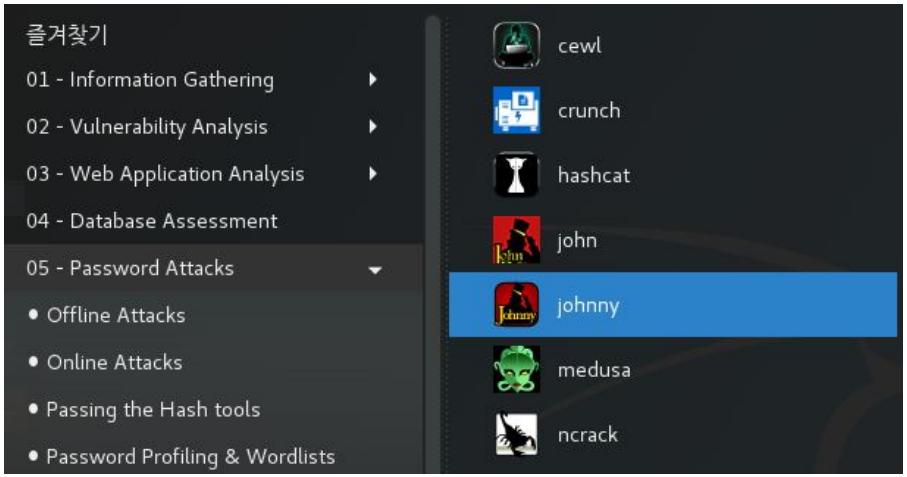
Lab 3. GUI John The Ripper를 이용한 패스워크 크래킹

❶ John The Ripper 설치 및 실행

#apt-get update

#apt-get install -y johnny

즐겨찾기 > 05. Password Attacks > johnny



❷ Crack 파일 만들기

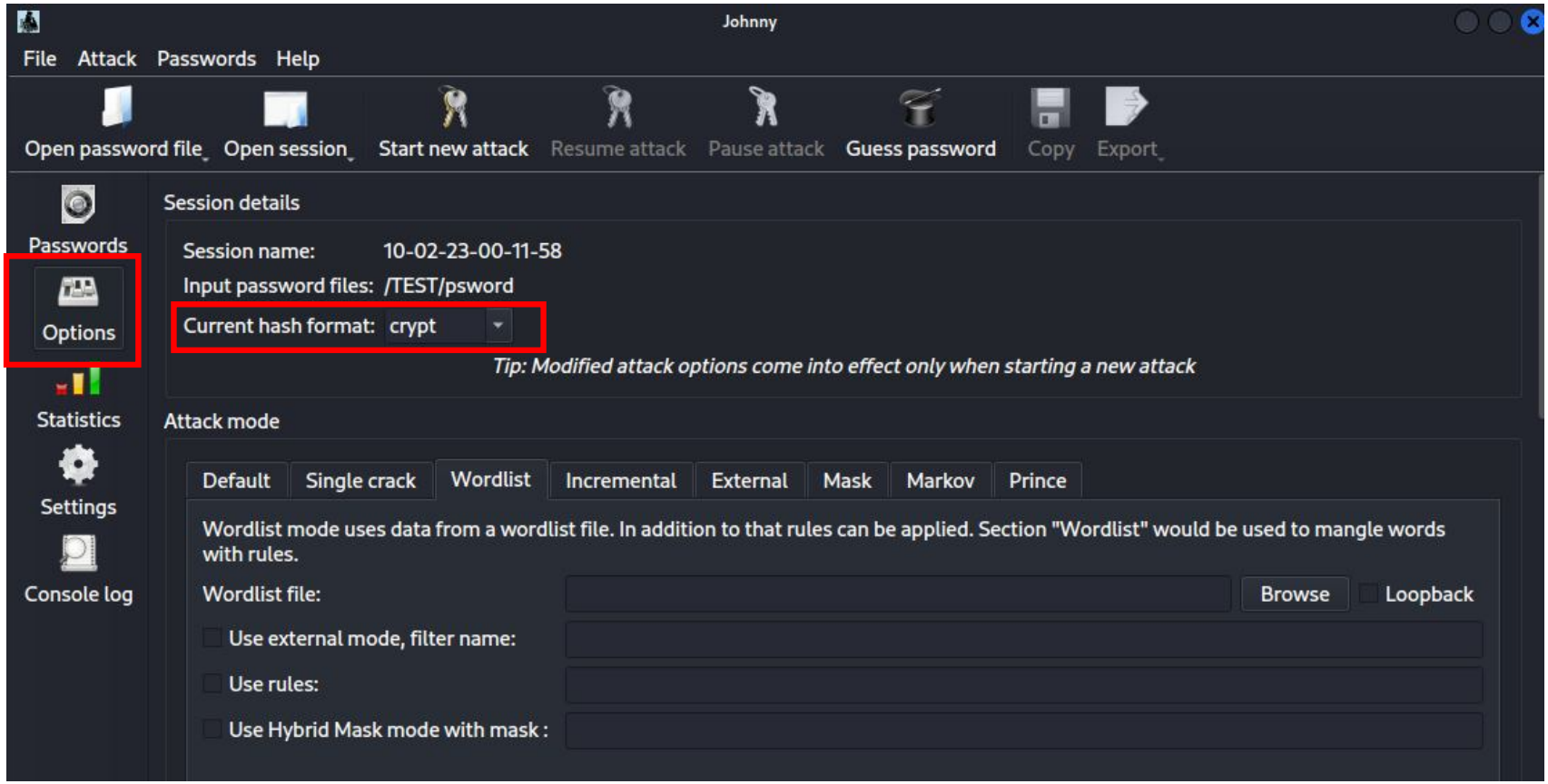
#unshadow passwd shadow | grep '\$y' | tee psword

```
┌──(root㉿kali)-[/TEST]
└─# ls -l
total 8
-rw-r--r-- 1 root root 3267 Oct  1 23:14 passwd
-rw-r----- 1 root root 1609 Oct  1 23:14 shadow

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

┌──(root㉿kali)-[/TEST]
└─# cat psword
kali:$y$j9T$lR7REZ4XgU56yXNl9PFiN/$oI3B/OeQGXOoTb7opQ.azBMOgG2IM0neRj4MN3HCqQ.:1000:1000:,,,:/home/kali:/usr/bin/zsh
gildong:$y$j9T$6lVdyOfzeXObyp8nMdWr30$UJ8DOvSh11DHnwkQLEypo3Jz9fyfmBwmNleRJyRueC1:1001:1001:,,,:/home/gildong:/bin/bash
hong:$y$j9T$icu6Yki9TxcTBmcRNjldr0$xaXrYzTwmhUHeaLuZAuDlMrKOdpkAPtMkWdksCK3DaC:1002:1002:,,,:/home/hong:/bin/bash
```

❸ Cracking환경 설정



❹ Password Cracking