**John the Ripper**

John the Ripper 이하 John은 password cracking tool이다. Kali Linux에는 john과 johnny 두 개가 있는데 johnny의 경우 GUI 환경이며 john의 경우 CLI이다. John의 사용법을 익히기에 앞서 Linux에서 계정 정보가 저장되는 법에 대해 알 필요가 있다. 크게 두 가지의 파일을 알 필요가 있는데 하나는 passwd 파일이며 다른 하나는 shadow 파일이다. 두 파일 모두 기본적으로 /etc밑에 존재한다.

/etc/passwd 파일의 경우 User의 정보가 들어있는 기본적인 파일이다. 여기서 User란 사용자가 로그인할 때 쓰는 계정 뿐만 아니라 Service에서 사용하는 계정 또한 포함된다. User의 정보가 있다는 듯은 곧 해당 User에 대한 Password도 있어야 한다는 의미가 된다. 허나 보안 상의 이유로 password의 경우 /etc/shadow 파일에 별도로 기억된다. 물론 암호화도 되어있다.

John the Ripper의 경우 Password Cracker이기 때문에 user의 password를 알아내기 위해서는 passwd 파일과 shadow 파일을 하나의 형태로 변환하여 cracking을 시도해야 한다. 해당 과정을 위해 unshadow 명령어를 사용하면 된다. 사용법의 경우 다음과 같다.

“unshadow <passwd file> <shadow file>”

passwd 파일과 shadow 파일의 경우 각각의 내용을 다른 파일에 복사하여 해당 파일들을 가지고 진행하여도 상관 없다. 또한 출력의 경우 terminal에 출력되기 때문에 Redirect를 이용하여 파일로 출력하면 된다.

John의 사용법은 다양한 방법이 있겠지만 우선은 기본적인 것에 대하여 정리하였다. Password crack을 위해서는 참조할 파일이 필요한데 해당 파일의 경우 --wordlist= 옵션을 통해 지정할 수 있다. 여기서는 Kali Linux에 기본적으로 있는 /usr/share/wordlist/rockyou.txt 파일을 사용하여 진행하였다. 하나 팁이 있다면 –wordlist= 옵션을 지정 후 경로를 입력할 때 바로 붙여서 진행하면 자동완성이 먹히지 않기 때문에 한 칸 띄어서 자동완성을 통해 경로를 지정 후 다시 공백을 없애주면 된다.

그리고 결과를 화면에 display 하기 위해서는 --show 옵션을 사용해주면 된다. Show와 wordlist가 동시에 사용하지 못하는 것인지 아니면 두 가지 이상의 옵션을 동시에 사용하지 못하는 것인지는 아직 확실치 않으나 두 개를 동시에 사용했을 경우 정상적으로 동작하지는 않는다. 우선은 약 세 가지 정도의 Command를 기억하면 될 것으로 보인다.

1. “john <filename>”

→ 가장 처음 crack 대상 file을 지정. 여기서 지정하는 파일은 unshadow 된 파일이어야 함.

2. “john --wordlist=<list file> <filename>”

→ wordlist에서 지정한 파일을 이용하여 file의 hash를 decrypt한다.

3. “john --show <filename>”

→ decrypt 된 결과를 출력한다. 이 또한 terminal에 직접 출력되므로 redirection을 사용하여 파일로 저장하면 된다.

John the Ripper의 동작 모드에는 세 가지 모드가 있다.

1. Single crack mode

- 가장 간단하고 빠른 cracking mode로 기존의 정보를 이용하여(id, username 등등) 시도한다.

2. Dictionary Attack

- 사전 파일을 사용하여 대입하며 시도한다.

3. Incremental mode

- 가장 강력한 cracking mode로 사용 가능한 모든 문자 조합을 시도한다. 만약 12 – 14 이상의 길이를 가지는 password를 제공할 경우 이를 수동으로 종료해야 한다.