동국대학교
dongguk university

제출일	2023.03.21	학과	컴퓨터공학전공
과목	컴퓨터보안	학번	2018112007
담당교수	김영부 교수님	이름	이승현

1) 실습 환경

운영 체제: Microsoft Windows 11 Home 64bit
프로세서 : Intel(R) Core(TM) i7-10510U @ 1.80GHz (8 CPUs), ~ 2.3GHz
메모리 : DDR4 16GB 2,667MHz
그래픽 카드 : Intel UHD Graphics

2) 실습 진행

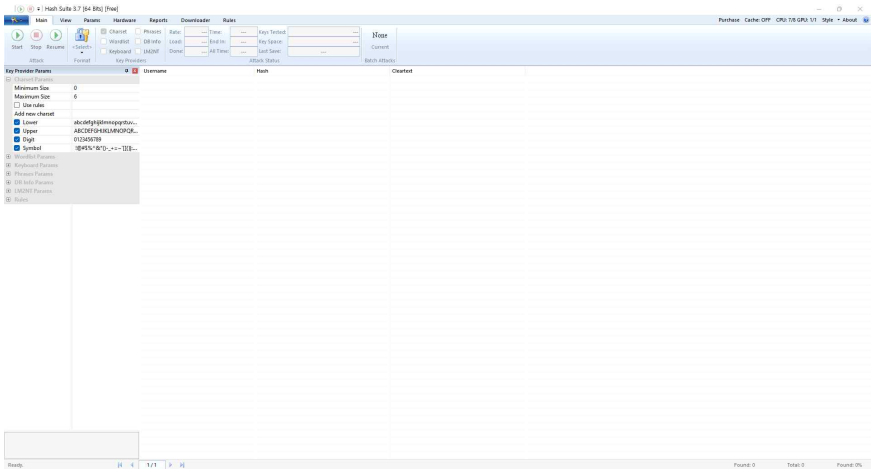
1. 문제 분석

패스워드 크래킹이란 컴퓨터 시스템에 저장된 데이터 또는 네트워크상에서 전송되는 데이터를 이용하여 암호를 복원하는 기술로써 암호를 잊어버려 암호를 복구하거나, 허가되지 않은 채 시스템에 접속하거나, 관리자가 자신이 설정한 암호가 풀기 쉬운지 확인하려는 목적으로 시행된다. 대부분의 패스워드 크래킹 기법은 다수의 후보 암호를 생성하여 크래킹하고, 암호를 푸는 데 걸리는 시간은 암호 강도에 비례한다. 따라서 이번 실습에서는 사용자 계정 3개를 생성하고 암호를 각각 apple, b4n4n4, P@ssw0rD로 설정하여 1) 소문자만 2) 소문자와 숫자 3) 소문자와 대문자, 특수문자, 숫자를 조합했을 때 암호 강도에 따라 암호 해독에 얼마나 많은 시간이 걸리는지 이번 실습에서 확인한다.

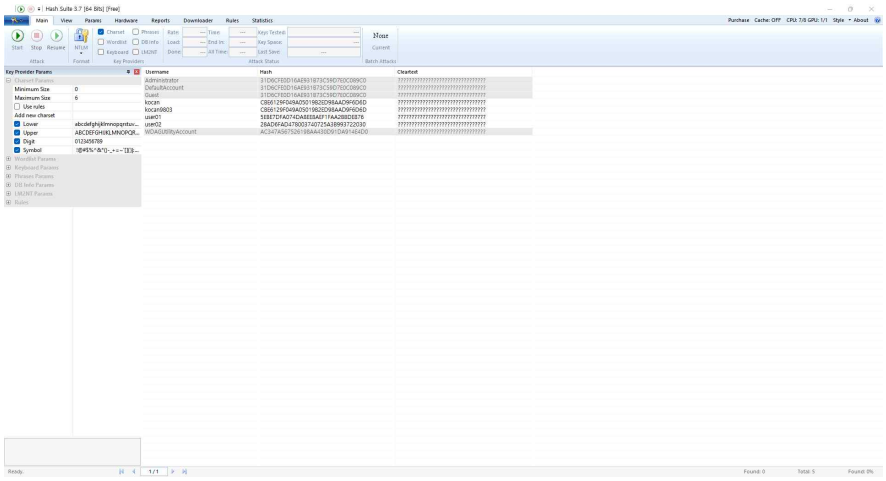
암호 해독은 Windows 운영 체제와 칼리 리눅스 운영 체제로 나눠서 진행한다. Windows 운영 체제에서는 로컬 사용자 계정을 생성한 후 위와 같이 암호를 설정하고 Hash Suite에서 로컬 사용자 계정을 불러와 해독을 진행한다. 칼리 리눅스 운영 체제에서는 Windows 운영 체제와 마찬가지로 사용자 계정을 생성하고 암호를 설정한 뒤 John the Ripper를 실행하여 암호 해독을 진행한다. 참고로 칼리 리눅스 운영 체제는 WSL2 이라는 Linux 용 Windows 하위 시스템에서 작동하게 된다.

2. 문제 해결 과정

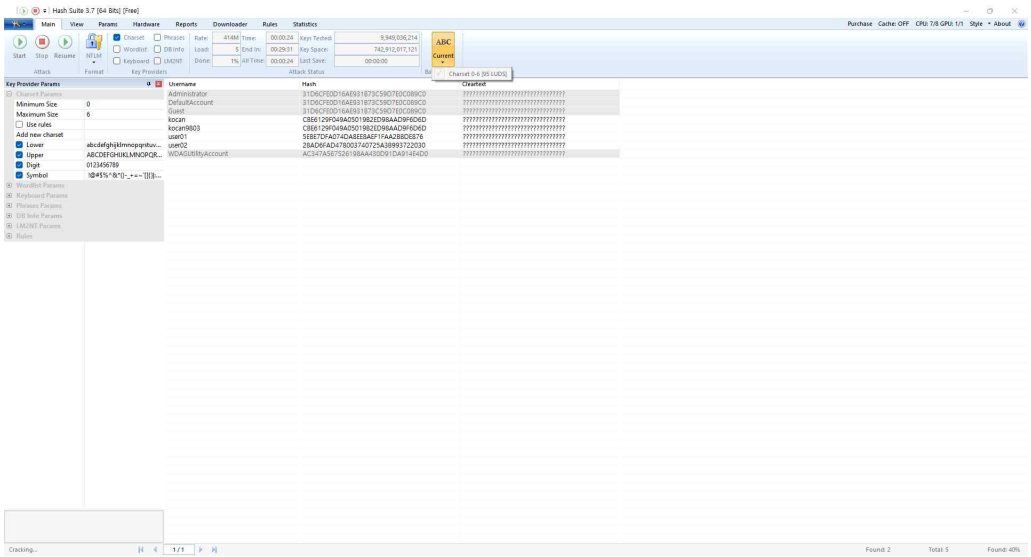
a) Hash Suite



- Hash Suite를 실행한 모습이다. 왼쪽 상단에 있는 열쇠 모양 아이콘을 클릭한 후 Import - Local accounts를 클릭하면 목록에 계정이 로드된다. 이때 사용자 계정만 안 보일 수 있는데 Main - Format에서 NTLM을 선택하면 된다. NTLM이라는 이름에서 볼 수 있듯이 Windows에서 제공하는 인증 프로토콜이며 MD4 암호화 방식을 사용한다. (현재 Windows는 NT 커널을 사용한다.)



- 이렇게 사용자 계정까지 보이면 Main - Start를 클릭해 사용자 계정의 암호 크래킹을 시행한다. 이때 왼쪽에 있는 Key Provider Params 메뉴에서 패스워드 길이의 최솟값과 최댓값을 지정할 수 있으며 문자열의 조합 또한 변경할 수 있습니다.



- 패스워드 크래킹이 진행 중인 모습이며 약 7,000억의 key를 테스트하여 사용자 계정의 패스워드를 알아내게 된다. 테스트하는 키의 구성은 알파벳 소문자와 대문자, 0에서 9까지의 정수와 특수문자의 조합으로 이루어지며 패스워드가 나올 수 있는 경우의 수는 92 ^ n이라는 엄청난 수가 나오게 된다. (이때 n은 패스워드의 자릿수이다.)

- 참고로 Hardware 메뉴에 들어가게 되면 패스워드 크래킹하는데 필요한 하드웨어 리소스를 조절할 수 있으며 (쓰레드 수 조절), CPU 대신 GPU 연산으로 크래킹할 수 있다. GPU 연산을 사용하여 패스워드를 크래킹하는 시간이 CPU 연산을 사용하여 크래킹하는 것보다도 속도가 확연히 빠르다. GPU 연산이 CPU 연산보다 병렬연산이 뛰어나서 그런 것이다.

b) John the Ripper

```
┌──(kocan㉿DESKTOP-6UMUOFM)-[~]
└─$ sudo su
[sudo] password for kocan:
```

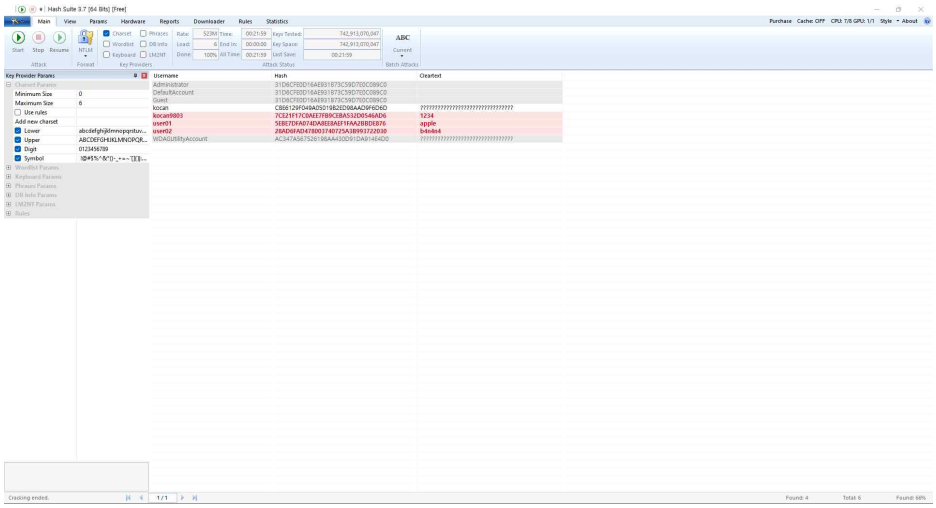
- sudo su 명령어를 통해 관리자 권한을 획득한다.

```
┌──(root㉿DESKTOP-6UMUOFM)-[/home/kocan]
└─# john -format=crypt /etc/shadow
```

- john -format=crypt /etc/shadow 명령어로 현재 시스템에 존재하는 사용자 계정에 대해 패스워드 크래킹을 시행한다. /etc/shadow를 입력하는 이유는 Unix 계열의 시스템에서는 사용자 계정의 패스워드를 암호화해서 shadow 파일에 저장하기 때문에 shadow 파일을 크래킹하는 것이다. Windows에서 shadow 파일이 존재하지 않기 때문에 PWDump 프로그램을 사용해서 shadow 파일과 같은 형식으로 변환한다.

3. 결과 및 결과 분석

a) Hash Suite



- 현재 Windows 시스템에 존재하는 사용자 계정의 비밀번호를 크래킹한 모습이다. 내가 추가한 로컬 사용자 계정 외에 의문의 계정(kocan9803) 또한 크래킹이 되었고 패스워드가 1234로 설정된 모습을 볼 수 있다.

```
C:₩Windows₩System32>net user kocan9803
사용자 이름                    kocan9803
전체 이름                      kocan9803
설명                           ISC BIND Service Account
사용자 설명
국가/지역 코드                 000 (시스템 기본값)
활성 계정                      예
계정 만료 날짜                 기한 없음

마지막으로 암호 설정한 날짜   2022-04-08 오후 5:11:04
암호 만료 날짜                 기한 없음
암호를 바꿀 수 있는 날짜       2022-04-08 오후 5:11:04
암호 필요                      예
사용자가 암호를 바꿀 수도 있음 아니요

허용된 워크스테이션            전체
로그온 스크립트
사용자 프로필
홈 디렉터리
최근 로그온                    2023-03-15 오후 1:35:16

허용된 로그온 시간             전체

로컬 그룹 구성원
글로벌 그룹 구성원             *없음
명령을 잘 실행했습니다.
```

- 명령 프롬프트에서 net user 명령어를 통해 계정의 정보를 확인한 모습이다. 계정 설명을 보면 ISC BIND Service Account이라고 기재되어있는데 Windows 시스템에서 DNS 서비스를 운용하기 위해 사용되는 계정

인 듯하다. 왜 사용자 계정 외에 저 계정이 생성된 것인지 알아보았는데 이 실습을 하기 전에는 사용자 계정을 Microsoft 메일과 연동하고 있었다(그 계정이 kocan9803). 그런데 실습할 때 한번 메일과의 연동을 풀고 로컬 계정으로 전환했다가(kocan) 다시 메일과 연동했었다. 그 과정에서 ISC BIND 서비스가 관리자 계정에서 실행될 수 없으므로 로컬 계정(kocan)은 그대로 관리자 권한이 남고 메일과 연동된 계정(kocan9803)이 ISC BIND Service Account로 지정되었다고 생각한다. ISC BIND Service Account라서 그런지 패스워드를 변경할 수 없고 로컬 그룹 구성원이 존재하지 않은 모습을 볼 수 있다.

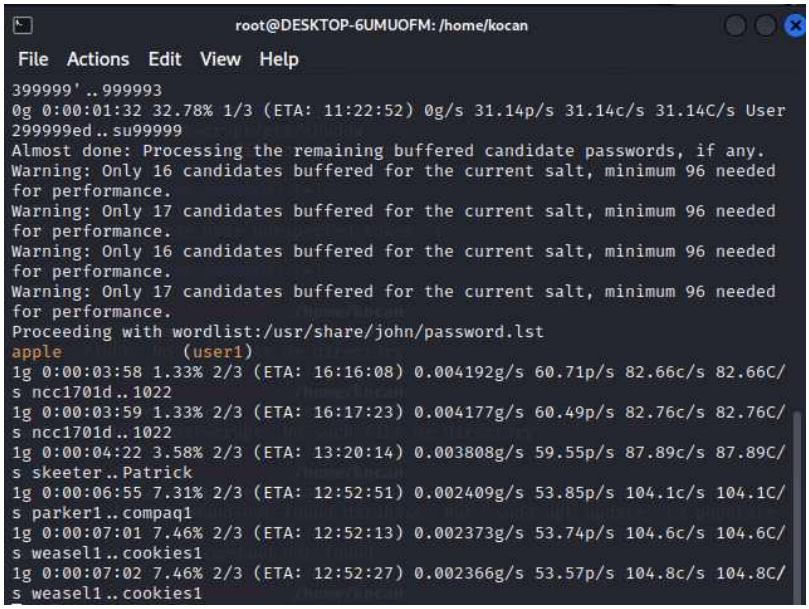
```
C:₩Windows₩System32>net user kocan
사용자 이름                          kocan
전체 이름                            이승현
설명
사용자 설명
국가/지역 코드                       000 (시스템 기본값)
활성 계정                            예
계정 만료 날짜                       기한 없음

마지막으로 암호 설정한 날짜          2023-03-15 오후 1:33:06
암호 만료 날짜                       기한 없음
암호를 바꿀 수 있는 날짜             2023-03-15 오후 1:33:06
암호 필요                            예
사용자가 암호를 바꿀 수도 있음       예

허용된 워크스테이션                  전체
로그온 스크립트
사용자 프로필
홈 디렉터리
최근 로그온                          2023-03-15 오후 1:33:04

허용된 로그온 시간                   전체

로컬 그룹 구성원                     *Administrators
                                     *Hyper-V Administrator
                                     *Users
글로벌 그룹 구성원                   *없음
명령을 잘 실행했습니다.
```

- 로컬 계정(kocan)을 살펴보면 관리자 권한이 메일과 연동된 계정(kocan9803)으로 넘어가지 않고 그대로 남은 모습을 볼 수 있었다. ISC BIND Service Account 과 달리 패스워드를 바꿀 수 있고 로컬 그룹 구성원 또한 존재하는 모습을 볼 수 있다.

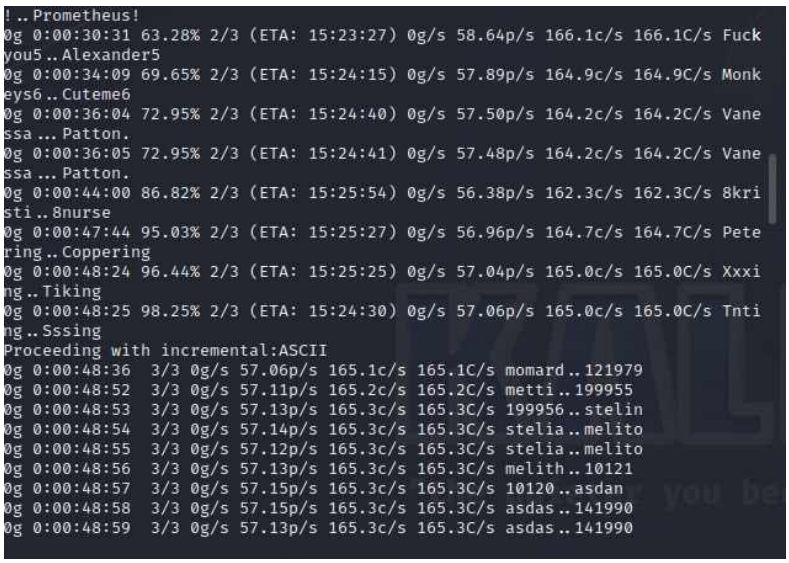
b) John the Ripper

```
┌──(root㉿DESKTOP-6UMUOFM)-[/home/kocan]
└─# john -format=crypt /etc/shadow
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Remaining 3 password hashes with 3 different salts
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
```

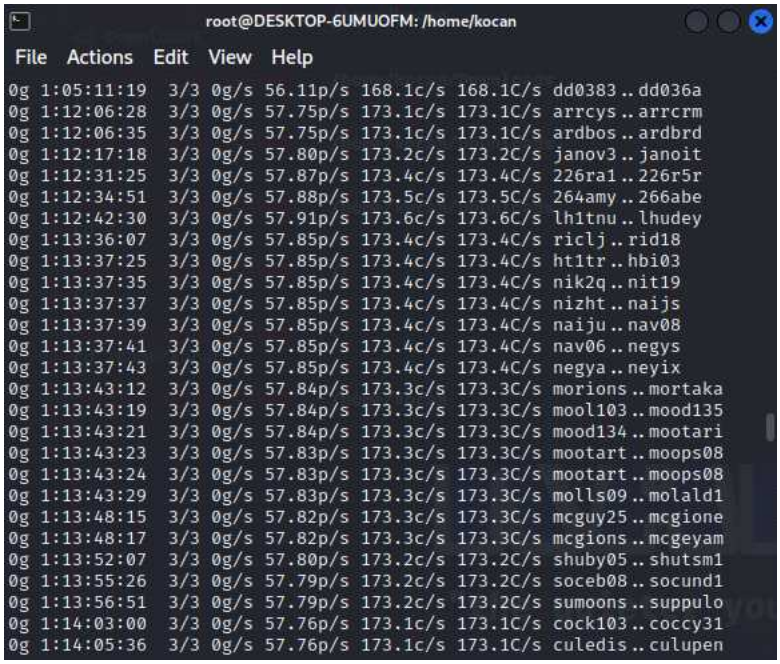
- 크래킹을 시작할 때 single 모드로 크래킹이 진행되었다. single 모드는 크래킹을 시작할 때 반드시 실행되는 모드이며, John the Ripper에서 가장 빠른 크래킹 모드이다. 이 모드는 shadow 파일 안의 GECOS 필드에 있는 사용자의 Full name, 홈 디렉토리 명을 후보 암호로 사용하며 수많은 mangling 규칙을 적용한다.

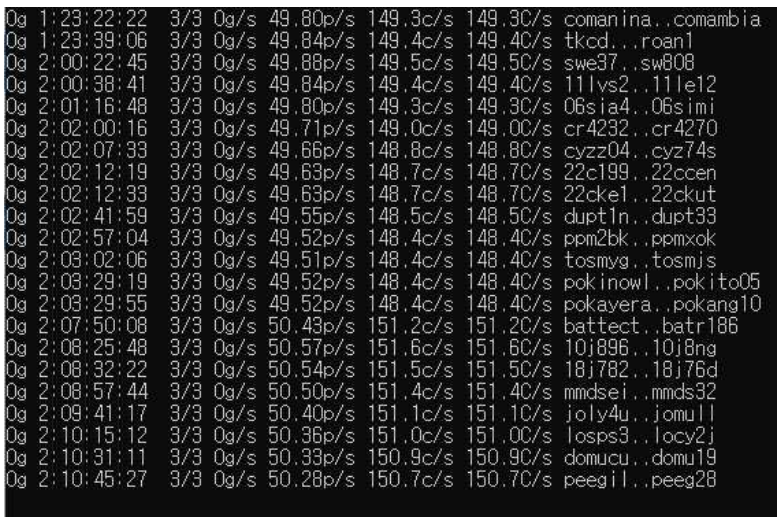


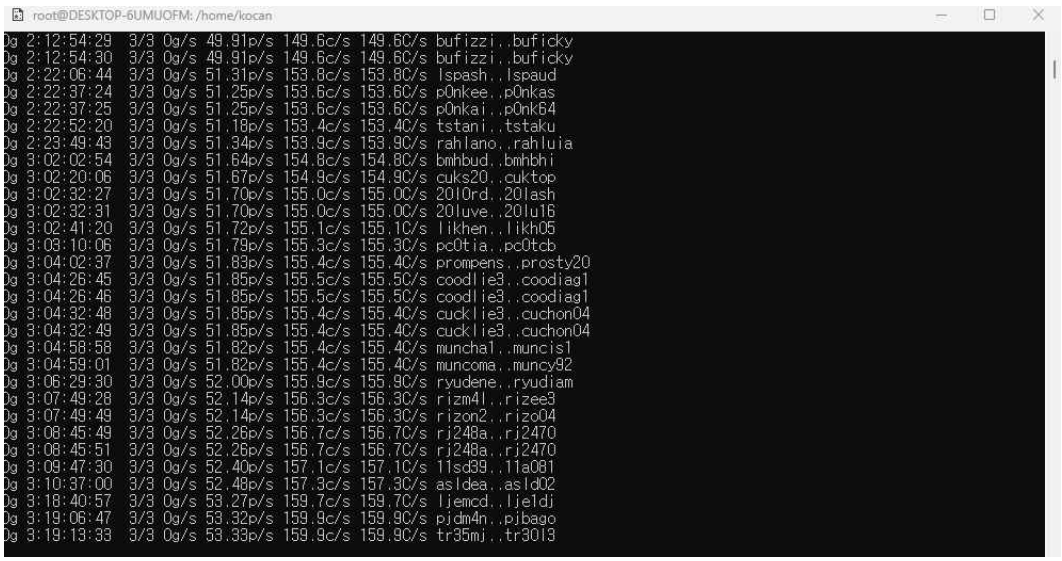
- 첫 번째 로컬 계정에서 패스워드 apple이 크래킹 된 모습을 볼 수 있다. wordlist 모드로 전환된 후 패스워드가 크래킹 된 모습을 확인할 수 있다. wordlist 모드는 단어 목록을 지정하고 단어 목록 파일의 모든 줄에 대해 단어 mangling 규칙을 적용해서 패스워드를 크래킹하게 된다. 첫 번째 로컬 계정의 경우 비밀번호가 간단했기 때문에 약 4분 만에 크래킹이 끝났다.



- 두 번째 로컬 계정부터 크래킹이 되지 않았다. wordlist 모드로 넘어가서도 크래킹이 되지 못했는데, 첫 번째 계정과 달리 패스워드가 알파벳 소문자와 숫자가 조합되었기 때문이고 약 48분이라는 시간이 소요되었고 incremental 모드로 변경된 모습을 볼 수 있다. 이 모드는 John the Ripper에서 가장 강력한 모드이며 가능한 모든 문자 조합을 시도한다. 이 모드에 사용할 수 있는 문자 세트는 ASCII(95개의 출력 가능한 ASCII 문자), LM_ASCII(LM 해시에 사용), Alnum(62개의 영숫자 문자), Alpha(알파벳 소문자와 대문자, 총 52개), LowerNum(소문자 + 숫자, 총 36개), UpperNum(대문자 + 숫자, 총 36개), LowerSpace(소문자 + 공백, 총 27개), Lower(소문자), Upper(대문자) 및 Digits(숫자만)가 존재하고, 여기서는 ASCII가 사용되었다. 따라서 패스워드의 길이가 n이면 필요한 조합의 수는 95^n이므로 패스워드가 길어질 때마다 어마어마한 경우의 수가 될 것이고 크래킹하는 데 많은 시간이 소요될 것으로 예측한다.







- 현재 incremental 모드가 진행되는 모습이며 약 나흘의 시간이 지나도 크래킹을 하지 못한 모습을 볼 수 있다. 왜냐하면 알파벳 소문자와 대문자, 숫자와 특수문자가 조합되어 설정되어서 ASCII 셋으로 진행하는 경우 경우의 수가 많기 때문이다. 만약 incremental 모드를 모든 사용자 계정에 적용하면 1) 첫 번째 계정의 경우에는 Lower 셋을 사용하면 26^5 = 11881376, ASCII 셋을 사용하는 경우 95^5 = 7737809375라는 경우의 수가 나오고, 2) 두 번째 계정의 경우에는 LowerNum 셋을 사용하면 36^6 = 2176782336, ASCII 셋을 사용하는 경우 95^6 = 735091890625라는 경우의 수가 나오고, 3) 세 번째 계정의 경우에는 ASCII 셋을 사용하는

경우 95^8 = 6634204312890625라는 경우의 수가 나온다. 따라서 첫 번째 계정의 경우 금방 크래킹이 되지만 두 번째 계정, 세 번째 계정의 경우 각각 7,000억, 6,000조라는 경우의 수를 확인해야 하므로 슈퍼컴퓨터가 아닌 이상 일반적인 컴퓨터 환경에서 며칠이라는 시간이 소요되는 것이다. 지금 보고서를 작성하고 있을 때도 열심히 크래킹하고 있지만, 아직도 크래킹을 마치지 못해 보고서를 작성하게 되었다.

- /etc/shadow 파일을 열어 크래킹 된 패스워드를 열람한 모습이다. 첫 번째 계정의 패스워드인 apple이 크래킹 되었고, 두 번째와 세 번째 계정의 패스워드는 크래킹 되지 못한 모습을 볼 수 있다.

3) 느낀 점

이번에 처음으로 보안과 관련된 실습을 진행했는데 이 실습이 컴퓨터 자원을 많이 사용해서 데스크톱이 아닌 랩톱으로 실습을 진행할 때 인내심을 갖고 진행했어야 했다. 특히나 John the Ripper를 실행할 때 kali linux에서 그래픽 카드가 인식하지 않아 그래픽 가속을 사용할 수 없어 순전히 CPU를 가지고 연산을 진행해서 컴퓨터가 전반적으로 느려져서 다른 작업을 진행하지 못하는 점에서 불편함과 어려움을 느꼈다. 특히나 랩톱에서 실행할 때는 시스템의 사양이 전반적으로 높지 않고, 패스워드 강도가 높은 경우에는 며칠이라는 시간이 소요되기 때문에 CPU가 풀로드 되는 상황을 며칠 동안 지속시켜야 해서 랩톱의 수명이 줄어들 가능성이 크다고 생각했다. 따라서 만약에 이번 실습과 같이 컴퓨터 자원을 많이 사용하는 실습을 할 때는 가능하면 데스크톱을 사용하고, 자주 사용하는 컴퓨터는 사용하지 않기를 유의해야겠다. 이 실습을 진행하면서 알게 된 내용이라면 John the Ripper에 다양한 모드가 존재하고, single, wordlist, incremental, external 모드가 이에 해당한다는 점이다. 또한 Unix 계열의 시스템에서는 패스워드가 shadow 파일에 암호화되어 저장되는데, Windows 시스템에서는 shadow 파일이 존재하지 않기 때문에 크래킹을 진행하는 경우 PWDump 프로그램을 사용하여 shadow 파일과 같은 형식의 파일로 변환하고 크래킹한다는 점을 알게 되었다. 그리고 이번 실습과 관련 없는 내용인데 계정 정보를 확인하면서 ISC DNS 서비스에 대해 알아보는 기회를 가질 수 있었다.