

<3주차 디지털포렌식 이론 정리 및 문제풀이>

디지털포렌식 필요성-> e-Discovery(전자적으로 저장된 정보)제도 국내 도입

사례1)

듀폰 vs 코오롱인터스트리

(코오롱-듀폰 영업비밀 침해 사건 일지)-> 소송 진행 중 불리한 이메일 삭제

사례2) 애플 vs 삼성전자

(이메일 자동 삭제 및 google측의 경고 취지 문서)

애플이 삼성을 상대로 아이폰의 둥근 모서리 디자인 특허 침해

사례3) 하이닉스와 램버스 소송 사례

.

*.디지털포렌식과 e-discovery

-공통성: 디지털 데이터, 증거를 취급하는 절차를 다루며, 증거능력을 가져야 한다는 점

-위험성: 디지털 데이터는 특성상 생성, 수정, 삭제 등 증거 조작이 용이함

-엄격성(법률적인 측면): 전문가에 의한 특별한 절차와 방법에 따라 자료의 수집, 이송, 분석, 보관, 보고에 이르는 과정이 엄격하게 준수되어야 함

-적용대상-디지털 증거 즉, 흔적이 남아있는 디지털 저장 장치를 총망라

-기밀 유출 유형- 외부 저장장치(usb)를 이용한 유출, 외부 서비스(웹브라우저 사용 흔적, 웹 클라우드 사용흔적)를 이용한 유출, 이메일을 이용한 유출 등등

*디지털 포렌식 기술 유형

-디스크 포렌식- 데스크탑, 노트북 등 디지털 저장매체에서 삭제 변경된 데이터 복원, 디지털 데이터를 분석해서 단서를 찾는 기법

-네트워크 포렌식-네트워크 트래픽과 전송 데이터를 수집하여 증거를 추출하고 분석

-데이터베이스 포렌식-분석회계 횡령 및 탈세 사건 발생시 분석 기술

-소스코드 포렌식-악성코드 분석, 프로그램 실행코드와 소스코드와의 상관관계 분석

-모바일/임베디드 포렌식-스마트폰, 태블릿pc와 같은 모바일 기기에 설치된 어플 사용으로 저장된 데이터를 수집 및 분석

-멀티미디어 포렌식-디지털 비디오, 오디오, 이미지 등의 멀티미디어 데이터를 대사로 분석

-안티포렌식-암호가 설정되어 있는 디지털 증거물에 대한 복호화

Ex) 스테가노그래피 등

*디지털 포렌식 장비 및 솔루션

- 이미징 툴-encase imager, ftk imager

- 복구 분석 툴-encase forensic

-안티포렌식 행위- 디스크 암호화(풀 디스크 암호화, 파일 기반 암호화)

*디지털포렌식의 기본 5원칙

-정당성의 원칙-수집한 증거는 적법절차를 거쳐서 획득

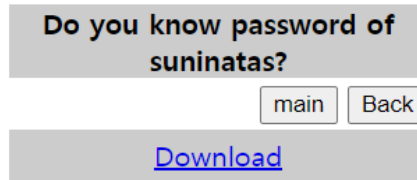
-재현의 원칙-피해 당시와 같은 조건에서 현장검증을 하였다면 동일한 결과 입증

-신속성의 원칙-신속하게 진행되었는가?

-연계보관성의 원칙-증거물 수집 이송 분석 보관 법정 제출 과정 동안의 각 단계에서 담당자 및 책임자를 명확하게

-무결성의 원칙-수집된 증거가 위 변조되지 않았음을 증명(hash값 무결성)

<써니나타스 14번>



이번 문제는 먼저 파일을 다운받아야 하는 문제였다. 다운로드를 해보았다.

다운로드를 했더니 2개의 파일이 있음을 알 수 있었다.(passwd, shadow)

위의 두 파일을 읽기 위해서는 note pad++라는 프로그램이 필요하다

아래의 사진은 note pad++를 이용해 파일을 열어본 사진이다


```
10 news:x:9:9:news:/var/spool/news:/bin/sh
11 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
12 proxy:x:13:13:proxy:/bin:/bin/sh
13 www-data:x:33:33:www-data:/var/www:/bin/sh
14 backup:x:34:34:backup:/var/backups:/bin/sh
15 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
16 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
18 libuuid:x:100:101:/var/lib/libuuid:/bin/sh
19 syslog:x:101:103:/home/syslog:/bin/false
20 sshd:x:102:65534:/var/run/sshd:/usr/sbin/nologin
21 landscape:x:103:108:/var/lib/landscape:/bin/false
22 messagebus:x:104:112:/var/run/dbus:/bin/false
23 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
24 mysql:x:105:113:/var/lib/mysql:/bin/false
25 avahi:x:106:114:/var/run/avahi-daemon:/bin/false
26 snort:x:107:115:Snort IDS:/var/log/snort:/bin/false
27 statd:x:108:65534:/var/lib/nfs:/bin/false
28 usbmux:x:109:46:/home/usbmux:/bin/false
29 pulse:x:110:116:/var/run/pulse:/bin/false
30 rtkit:x:111:117:/proc:/bin/false
31 festival:x:112:29:/home/festival:/bin/false
32 postgres:x:1000:1000:/home/postgres:/bin/sh
33 haldaemon:x:113:122:Hardware abstraction layer,,:/var/run/hald:/bin/false
34 suninatas:x:1001:1001:/home/suninatas:/bin/sh
35
```

밑줄 친 부분을 눈 여겨 보아야 하는데, 이는 칸마다 의미가 다르기 때문이다.

계정명, 패스워드, 사용자ID, 그룹ID, Comment, 홈 디렉토리, 기본 쉘로 이루어져있다.

여기서, 알고 넘어가야 하는 것이 바로 x인데, x는 암호화가 되어 있다는 뜻이다. 두번째 자리인 패스워드에 x가 표시되어 있으니 패스워드가 암호화가 되어 있다는 것을 알 수 있고, 이를 shadow에서 확인할 수 있다.

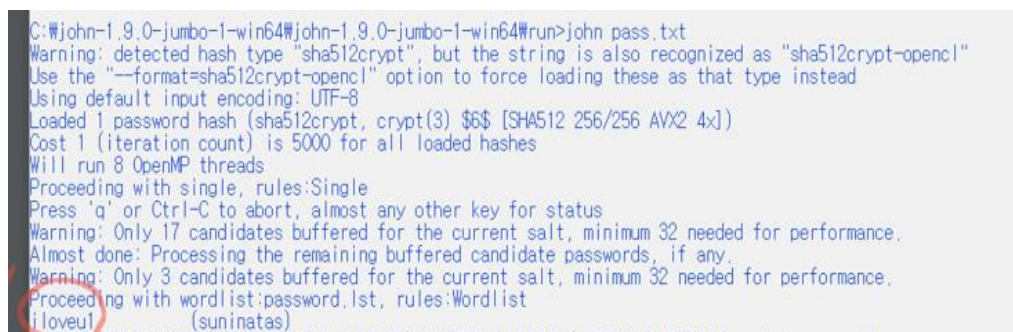
shadow파일은 txt파일로 열어보았는데, 나중에 cmd창에서 읽어들이기 위해서이다.



```
shadow - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
backup:x:15426:0:99999:7:::
list:x:15426:0:99999:7:::
irc:x:15426:0:99999:7:::
gnats:x:15426:0:99999:7:::
libuuid:x:15426:0:99999:7:::
syslog:x:15426:0:99999:7:::
sshd:x:15426:0:99999:7:::
landscape:x:15426:0:99999:7:::
messagebus:x:15426:0:99999:7:::
nobody:x:15426:0:99999:7:::
mysql!:15426:0:99999:7:::
avahi:!:15426:0:99999:7:::
snort:!:15426:0:99999:7:::
statd:!:15426:0:99999:7:::
usbmux:!:15426:0:99999:7:::
pulse:!:15426:0:99999:7:::
rtkit:!:15426:0:99999:7:::
festival:!:15426:0:99999:7:::
postgres:!:15426:0:99999:7:::
haldaemon:!:15426:0:99999:7:::
suninatas:$6$QlRlqGhj$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP/zYtI8O2dsshndwnsJT/1IZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/:15427:0:99999:7:::
```

shadow파일에서도 가장 마지막 부분을 보면, 계정명, 암호화된 패스워드, 패스워드 수정된 일 수, 패스워드 변경 전 최소 사용기간, 패스워드 변경 전 최대 사용기간, 패스워드 만기 전 알림을 제공하는 일수, 로그인 접속 차단 일수, 로그인 금지 일수, 예약필드로 나누어져 있다.

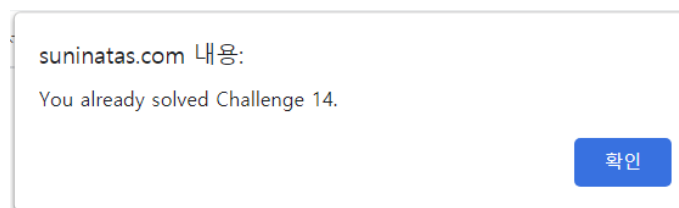
이제 저기 화면에 암호화 된 것을 해독하기 위해서 john the ripper라는 프로그램을 이용해야 하는데 이를 cmd에서 실행시켜보면 다음과 같다



```
C:\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64#run>john pass.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 17 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 3 candidates buffered for the current salt, minimum 32 needed for performance.
Proceeding with wordlist:password.lst, rules:Wordlist
iloveui (suninatas)
```

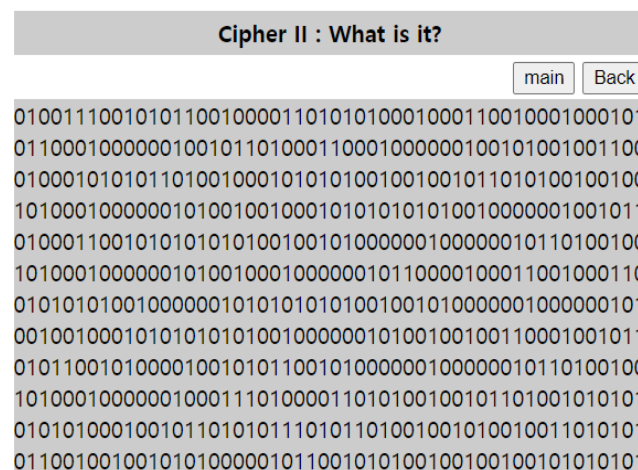
그 다음, run폴더 아래에 복사 붙여넣기를 해준 다음 `john shadow.txt --show`를 입력하면 suninatas의 비밀번호인 `iloveu1`이 출력하게 된다.

이를 Auth창에 입력하고 제출했더니 정답이었다.



<써니나타스 19번>

이번 문제는 첫 화면에 0,1 바이너리코드로만 이루어진 것을 볼 수 있다.



Convert text to binary 사이트를 통해 위의 바이너리코드를 해석해줄 수 있다.

사진처럼 알 수 없는 영문자 배열이 추출되었다. 문자 사이의 알 수 없는 문자가 아닌 알파벳으로 이루어져 있기 때문에 치환 암호일 가능성이 있다. 치환암호는 일정한 법칙에 따라 평문의 문자 단위를 다른 문자 단위로 치환하는 암호화 방식이다. 치환 암호를 변환시켜주는 사이트에 들어가 아래의 문자열을 입력해준다.

```

0100111001010110010000110101010001000110010001000101
0110001000000100101101000110001000000100101001001100
0100010101011010010001010101001001001011010100100100
10100010000001010010010001010101010010000001001011
01000110010101010100100101000000100000010110100100
1010001000000101001000100000010110000100011001000110
0101010100100000010101010101001001010000001000000101
0010010001010101010100100000010100100100110001001011
0101100101000010010101100101000000100000010110100100
1010001000000100011101000011010100100101101001010101
0101010001001011010101110101101001001010010011010101
0110010010010101010000010110010101001001001001010101
  
```

binary numbers to text

NVCTFDV KF JLEZERKRJ REU KFURP ZJ R XFFU URP REU RLKYBVP ZJ
GCRZUTKWZJMVIPYRIU

치환 암호 사이트에 들어가서 위의 문자열을 입력해주었더니 그나마 이해할 수 있는 문장이 나왔다.

```

UCJAMKC RM QSLGLYRYQ YLB RMBYW GQ Y EMMB BYW YLB YSRFCIW GQ NJYGBARDGQTCPUWF
VDBNLD SN RTMHMZSR ZMC SN CZX HR Z FNNC CZX ZMC ZTSGJDX HR QKZHCSEHRUDQXG
WELCOME TO SUNINATAS AND TODAY IS A GOOD DAY AND AUTHKEY IS PLAIDCTFISVERYHARD
1: XFMDPNF UP TVOJOBUT BOE UPEBZ JT B HPPE EBZ BOE BVULFZ JT QMBJEDUGJTWFSZIBSE
2: YGNEQOG VQ UWPKPCVCU CPF VQFCA KU C IQQF FCA CPF CWVJMG A KU RNCKFEVHKUXGT AJ
3: ZHOFRPH WR VXQLQDWDV DQG WRGDB LV D JRRG GDB DQG DXWKNHB LV SODLGFWILVYHL
4: AIPGSQI XS WYRMREXEW ERH XSHEC MW E KSSH HEC ERH EYXLOIC MW TPEMHGXJMWZIVCLE
5: BJQHTRJ YT XZSNSFYFX FSI YTIFD NX F LTTI IFD FSI FZYMPJD NX UQFNIHYKNXAJWDMFWI
  
```

엄청 이상한 문자열들 사이에 저 한문장만 우리가 알 수 있는 영문장을 발견할 수 있었다.

하지만 여기서 중요한 것은 저 문장을 다 입력하면 안되고 Authkey is PLAIDCTFISVERYHARD 중 PLAIDCTFISVERYHARD을 입력해야 정답이다. 이를 Auth key에 입력하였더니 정답이었다.

suninatas.com 내용:

You already solved Challenge 19.

확인