DUM DUM:P

32기 안현진

문제 파일을 다운받으면 bin 파일이 나온다. bin 확장자? 처음 들어본다.

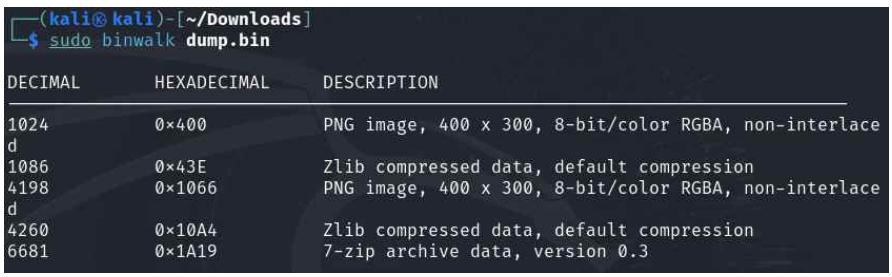
BIN이란, Binary File(바이너리 파일)이라고 부르는 컴퓨터가 사용하는 0과 1로 이루어진 이진 텍스트 파일이다. 컴퓨터에서는 바이너리 파일을 CPU가 직접 읽어들여 명령어를 수행한다. 이진 파일 형식의 문자열이 포함되어 있으며 완전한 텍스트 파일이다. 여러 가지 형태로 사용이 가능하다.

Linux에서 제공하는 분석 도구들을 사용하여 바이너리 파일을 분석할 수 있다. 리눅스에서는 바이너리 파일이 /bin, /sbin, /lib, /opt/bin과 같은 바이너리 디렉토리에 위치하며, 사용자들은 해당 파일들을 실행할 수 있다.

bin파일을 가지고 문제를 풀기 위해서는 우선 dump.bin 파일을 실행시켜야 할 것 같다.

1. binwalk 툴 사용

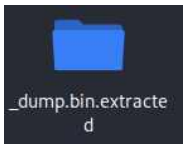
이 문제는 포렌식 문제다. 그러니 cute tiger 문제(포렌식 문제)를 풀 때 사용했던 툴을 사용해보자. binwalk는 파일 시그니처를 기반으로 숨겨진 파일을 찾을 수 있는 도구이다.



#sudo binwalk dump.bin 명령어를 사용한 결과 PNG 파일과 zip파일이 bin파일 안에 있는 것을 확인했다 (Zlib는 데이터 압축 오픈소스 라이브러리이다)

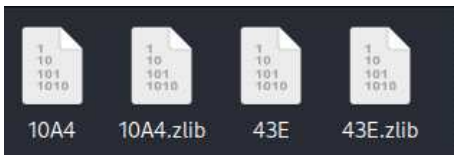
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# binwalk -e --run-as=root dump.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1024          0x400           PNG image, 400 x 300, 8-bit/color RGBA, non-interlace
d
1086          0x43E           Zlib compressed data, default compression
4198          0x1066          PNG image, 400 x 300, 8-bit/color RGBA, non-interlace
d
4260          0x10A4          Zlib compressed data, default compression
6681          0x1A19          7-zip archive data, version 0.3
```



-e 옵션은 binwalk이 파일을 추출하도록 지시한다. #binwalk -e —run-as=root dump.bin 명령어를 사용해서 bin파일 안에 있는 내용을 추출했다. 그러면 사진과 같은 폴더가 만들어진다.

2. zlib 라이브러리 사용하여 압축 파일 풀기



추출된 폴더 안에는 이런 파일이 있었다. 파일을 클릭해서 열어보려고 했는데, 일반적인 방식으로는 열리지 않는다.

찾아보니 10A4, 43E는 확장자가 없는 파일이다. 그리고 zlib 확장자를 가진 파일은 Zlib 형식으로 압축된 파일들로, Zlib를 지원하는 도구를 사용해야 데이터를 확인할 수 있다고한다. 근데 왜 파일명이 같은게 다른 확장자로 나뉘어져있을까....?

파일 압축을 풀면 여러 가지 텍스트 파일이 나온다. 이 중 djye.txt파일의 내용이 플래그였다.

```
3S{EA5Y_DUMP_F1L3_G00D_:P}
```

<참고자료>

[Linux 이론] Binary란? (tistory.com)
[Multimedia Forensic] 답을 찾고 제출해라! :: Yum_Yum (tistory.com)