IOT - Firm #1

Mips 파일이 하나 주어졌고, 지문은 다음과 같다.

```
Me and my time are trying to get the admin access of the gate
but we are not able to get into it you have to find the secret password
and what is the "kernel version" so that we can attack it.
```

펌웨어는 'binwalk' 어플리케이션을 통해 데이터를 추출할 수 있다.

```
┌──(kali㉿kali)-[~/Desktop/worm]
└─$ binwalk -e ./Firm-1.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header
CRC: 0x9871DE93, created: 2021-08-15 01:39:11, image size: 11075584 bytes,
Data Address: 0x0, Entry Point: 0x0, data CRC: 0x2761E29D, OS: Linux, CPU:
MIPS, image type: Firmware Image, compression type: none, image name: "jz_fw"
64            0x40            uImage header, header size: 64 bytes, header
CRC: 0xD3B9E871, created: 2019-02-14 03:00:10, image size: 1859813 bytes, Data
Address: 0x80010000, Entry Point: 0x80400630, data CRC: 0xE3786CEF, OS: Linux,
CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name:
"Linux-3.10.14"
128           0x80            LZMA compressed data, properties: 0x5D,
dictionary size: 67108864 bytes, uncompressed size: -1 bytes
2097216       0x200040        Squashfs filesystem, little endian, version 4.0,
compression:xz, size: 3353388 bytes, 407 inodes, blocksize: 131072 bytes,
created: 2021-08-15 01:35:08
5570624       0x550040        Squashfs filesystem, little endian, version 4.0,
compression:xz, size: 572594 bytes, 12 inodes, blocksize: 131072 bytes,
created: 2018-08-13 04:50:58

WARNING: Extractor.execute failed to run external extractor 'jefferson -d
'jffs2-root' '%e'': [Errno 2] No such file or directory: 'jefferson',
'jefferson -d 'jffs2-root' '%e'' might not be installed correctly
6225984       0x5F0040        JFFS2 filesystem, little endian
```

_Frim-1.bin.extracted가 하나의 디스크라고 보면 된다.

```
┌──(kali㉿kali)-[~/Desktop/worm]
└─$ ls
crypto       _Firm-1.bin.extracted  _Firm-2.bin.extracted  _Firm-3.bin.extracted
Firm-1.bin   Firm-2.bin             Firm-3.bin             u-boot.bin.lzma
```

처음에 접근할 때는 너무 어렵게 접근하였다. secret password라고 하고, admin에 관련된 게이트라고 해서 Mips 리버싱문제인줄 알고 바이너리로 의심되는 파일들을 다 찾기 시작했다.

그러다 문제 풀이자가 많아지는 것을 보고, 생각보다 단순하게 접근하면 되구나 싶어 /etc/shadow에 존재하는 root의 해시를 브루트포싱하기로 결정하였다.

아쉽게도, 대회 당시는 John the ripper의 디폴트 딕셔너리 파일로 실행시켜두고 다른 문제들을 풀고 있었다. 아무리 시간이 지나도 패스워드가 출력되지 않았다. 그래서 잘못 된 방식으로 접근했는가보다 하고 포기하고 다른 문제들을 계속 풀었다.

대회가 끝나고, 풀이자에게 물어보니 John the ripper로 푸는게 의도한 것이였고, rockyou.txt를 사용했어야한다고 한다. John the ripper를 사용한 적이 많이 없어서 당연히 rockyou.txt로 진행하겠지 싶었다. 개인적으로 이런 문제는 펌웨어 문제로 내면 안될 거 같다.

어쨌든, John the ripper로 root 패스워드를 찾으면 다음과 같다.

```
┌──(kali㉿kali)-[~/…/worm/_Firm-1.bin.extracted/squashfs-root/etc]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt  passwd.txt                    1 ×
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256
"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (root)
1g 0:00:00:02 DONE (2021-08-29 07:16) 0.4366g/s 3465p/s 3465c/s 3465C/s somebody..melania
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

커널 버전은 Firmware파일을 헥사에디터로 열람하면 바로 확인할 수 있다.

FILE: https://drive.google.com/file/d/1tIdtg2T5DdkawgUs-zTF6Ttl3C1PeDQ_/view?usp=sharing