

# i春秋网鼎杯网络安全大赛blend题目writeup

原创

iqiqiya 于 2018-10-24 10:56:35 发布 1846 收藏

分类专栏: [我的逆向之路](#) -----2018i春秋网鼎杯 [我的CTF进阶之路](#) 文章标签: [blend题目writeup](#) [i春秋网鼎杯](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xiangshangbashaonian/article/details/83042412>

版权



[我的逆向之路](#) 同时被 3 个专栏收录

108 篇文章 10 订阅

订阅专栏



[-----2018春秋网鼎杯](#)

6 篇文章 0 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

下载后解压 发现只有1KB what? ? ?

file 一下 说是main.bin: x86 boot sector

The screenshot shows a terminal window with a file manager view on the left and a terminal output on the right. The file manager shows a file named 'main.bin' with a size of 1 KB, dated 2018/8/17 9:08, and type 'BIN 文件'. The terminal output shows the command 'file main.bin' being executed, resulting in the output 'main.bin: x86 boot sector'.

百度了一下下

说这个东西是linux的引导扇区

Boot sector是硬盘(严格来说是所有可引导的存储介质)上的第一个扇区, 大小为512字节, 这个扇区对于计算机启动来说至关重要。

主要分为三个部分, 分别是:

MBR(master boot record,主引导记录)446字节

DPT(disk partition table,磁盘分区表)64字节

BRID(boot record ID引导记录标识)2字节

然后直接010 Editer打开 发现

```
启动 main.bin x
编辑为: Hex v 运行脚本 v 运行模板 v
 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
100h: 7D 66 C7 87 61 7D 20 3D 3D 3E E9 26 FF B4 01 CD }fÇ+a} ==>é&y'.Í
110h: 16 74 37 30 E4 CD 16 3C 08 74 16 3C 0D 74 2B BB .t70äí.<.t.<.t+»
120h: 34 12 8A 0E C8 7D 01 CB 88 07 FE 06 C8 7D E9 02 4.Š.È}.È^.p.È)é.
130h: FF 80 3E C8 7D 01 0F 8C F9 FE B8 34 12 FE 0E C8 ýε>È}..Èùp,4.p.È
140h: 7D 8A 1E C8 7D 01 C3 C6 07 5F E9 E6 FE C6 06 78 }Š.È}.ĂÆ._éæpÆ.x
150h: 12 04 BF 80 7D EB 88 90 90 90 90 90 90 90 90 90 .:ç)š^.....
160h: 3D 3D 20 45 4E 54 45 52 20 46 4C 41 47 20 3D 3D == ENTER FLAG ==
170h: AF AF AF 20 43 4F 52 52 45 43 54 21 20 AE AE AE — CORRECT! @@@@
180h: 21 21 20 57 52 4F 4E 47 20 46 4C 41 47 20 21 21 !! WRONG FLAG !!
190h: FF FF FF FF FF FF FF FF 00 FF FF FF FF FF FF FF YYYYYYYYY·YYYYYYY
1A0h: 00 FF FF FF FF FF FF FF F6 02 DD 02 E8 02 DC 02 .yyyyyyyyö.Ý.è.Û.
1B0h: ED 02 D8 02 E2 02 CE 02 E2 02 C4 02 DB 02 D4 02 í.ø.â.î.â.Ă.Û.Ô.
1C0h: CD 02 D9 02 04 03 11 03 00 00 00 00 00 00 00 00 í.Û.....
1D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1F0h: 00 00 00 00 00 00 00 00 00 00 00 00 55 AA .....U
https://blog.csdn.net/xiangshangbashaojian
```

这道题目与其他的题目不一样 文件既不是Linux也不是Windows下的可执行文件，而是需要在QEMU全系统仿真器下才能运行的MBR(主引导记录)

QEMU就是一个通用的开源机器模拟器和虚拟机

运行的命令为: **qemu-system-i386 -drive format=raw,file=文件名**

等补坑

参考链接:

<https://github.com/TechSecCTF/writeups/blob/master/CSAWQuals2017/realism/README.md>

<https://xz.aliyun.com/t/2608#toc-11>

<https://www.jianshu.com/p/005bda1f8535>

<https://blog.csdn.net/ww1473345713/article/details/51602825?locationNum=5&fps=1>