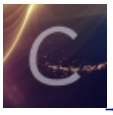
【WhaleCTF逆向题】第一期风险和回报writeup

原创

iqiqiya 于 2018-09-27 15:16:27 发布 1610 收藏
分类专栏： 我的逆向之路 我的CTF之路 ------WhaleCTF 我的CTF进阶之路 文章标签： 【WhaleCTF逆向题】第一期风险和回报writeup 【WhaleCTF逆向题】 风险和回报writeup

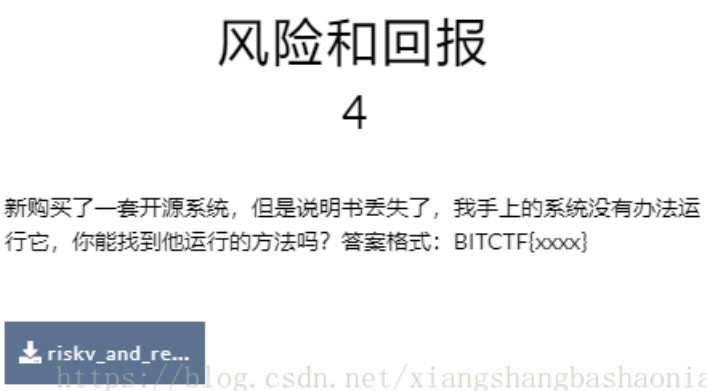

我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏


------WhaleCTF
8 篇文章 0 订阅
订阅专栏

下载地址：http://daka.whaledu.com:9999/challenges

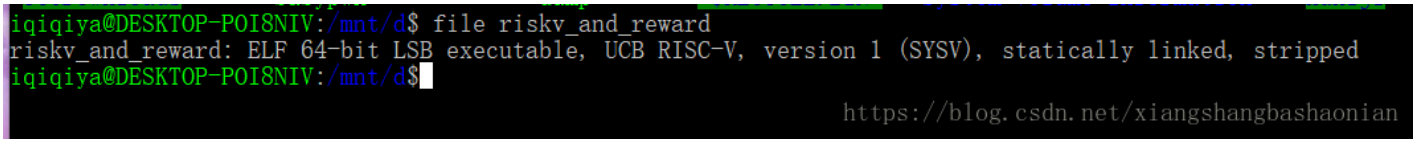
题目信息：



题目信息：新购买了一套开源系统，但是说明书丢失了，我手上的系统没有办法运行它，你能找到他运行的方法吗？

下载后file查看

riskv_and_reward: ELF 64-bit LSB executable, UCB RISC-V, version 1 (SYSV), statically linked, stripped



看到是ELF 64-bit的文件，想着先运行一下

结果报错

-bash: ./riskv_and_reward: cannot execute binary file: Exec format error

```
iqiqiya@DESKTOP-POI8NIV:/mnt/d$ ./riskv_and_reward
-bash: ./riskv_and_reward: cannot execute binary file: Exec format error
```

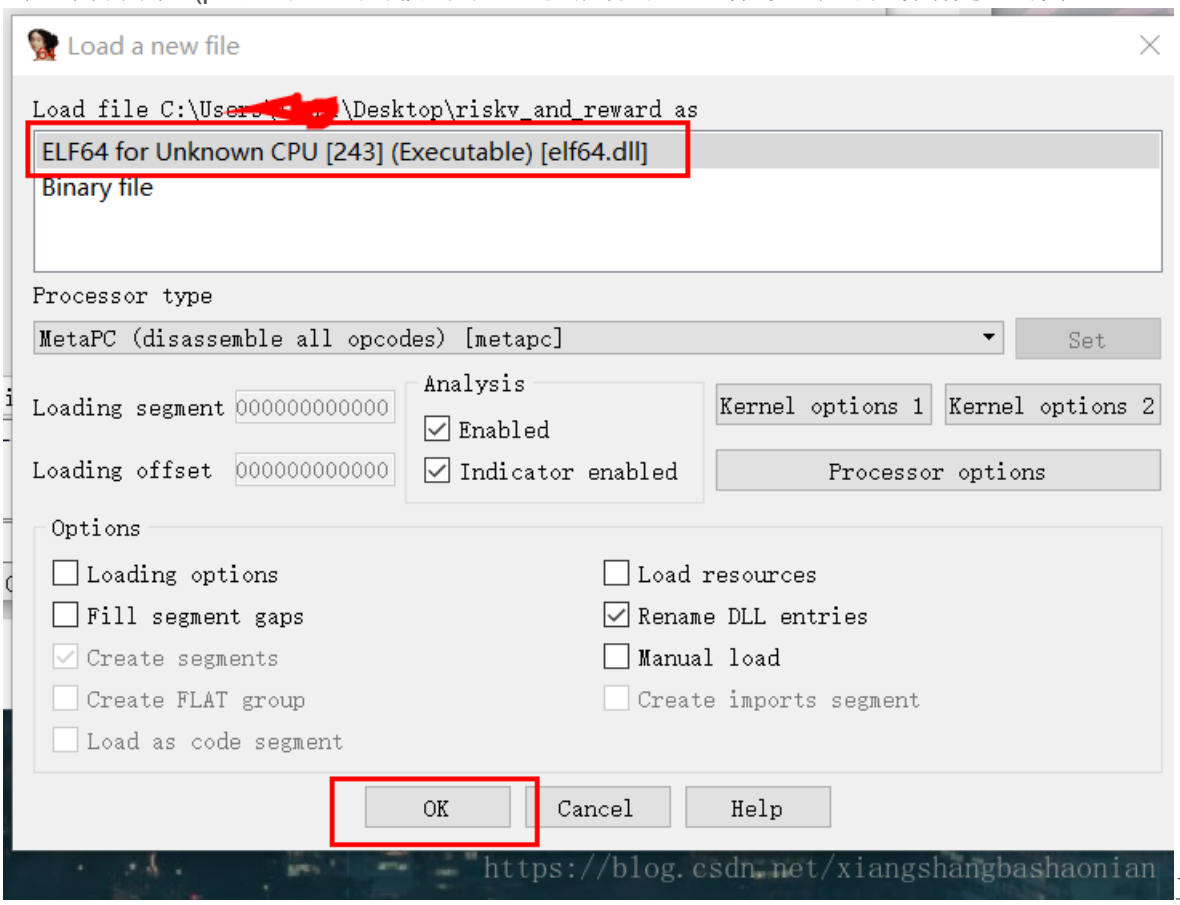
百度了一下 猜测是2的原因

linux系统下遇到cannot execute binary file的问题，一般由以下情况造成：

1. 非root用户或者无执行权限
2. 编译环境不同（程序由其他操作环境复制过来）

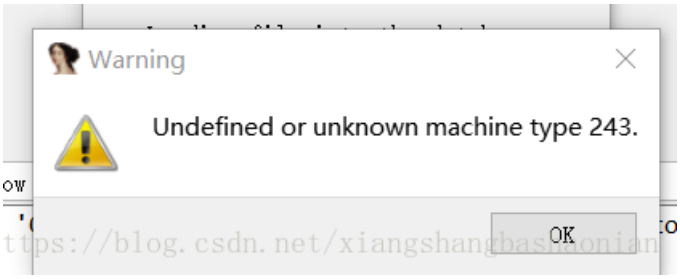
心想着直接载入IDA看看吧

到这个界面了 (ps:点击OK的时候当时心里挺激动的 心想着马上就可以看清楚它的真



正面目啦)

结果报错(ps:这时候心凉了一大截儿) 说是什么 Undefined or unknown machine type 243



翻译了一下 意思是未定义或未知机器类型243 就是IDA不支持这种架构

20181018来补坑(方法是蓝鲸塔主师父教的 http://www.whaledu.com/course/138/task/1287/show)

readelf -h

查看下ELF文件头

可以看到Machine字段显示为RISC-V　百度可以知道这是一种处理器架构

这里想要执行这个文件　有两种办法

> 一种是KVM虚拟机+https://github.com/riscv/riscv-qemu(非常麻烦)
>
> 另一种是直接用docker(推荐) pull对应镜像

就第二种来接着说

ubuntu 14.04安装可以看https://blog.csdn.net/xiangshangbashaonian/article/details/83149528

启动命令

```
iqiqiya@521:~/Desktop$ sudo service docker start
start: Job is already running: docker
```

pull镜像

```
iqiqiya@521:~/Desktop$ sudo docker run --privileged -v /home:/home -it sorear/fedora-riscv-wip
```

第一次下载有点慢 (翻墙可能会快一点 自测 我直接手机开的热点　速度还不错)

好不容易下好了　结果报错**FATAL: kernel too old**

【20181025】来补坑　这次换了Ubuntu16.04的版本

安装docker请参考：https://jingyan.baidu.com/article/0aa223756cf6e388cc0d6412.html

先启动docker

接着pull镜像

如果发现用户名与主机名变成这种**[root@df9f8627627d /]#**就代表成功啦

```
iqiqiya@521:~$ sudo service docker start
[sudo] password for iqiqiya:
iqiqiya@521:~$ sudo docker run --privileged -v /home:/home -it sorear/fedora-riscv-wip
Unable to find image 'sorear/fedora-riscv-wip:latest' locally
latest: Pulling from sorear/fedora-riscv-wip
bc87223043b7: Pull complete
c25ab3a6d613: Pull complete
Digest: sha256:833f47ad45358d9838d759ee9f1579b2d16ec03d87a416a52d329c51adb2872d
Status: Downloaded newer image for sorear/fedora-riscv-wip:latest
exec: Exec format error

Starting architecture emulation failed.  Attempting to reconfigure the
binfmt_misc mapping for RISC-V ELF files.

[root@df9f8627627d /]# ls
bin   checksetup  etc   lib    lost+found  mnt  proc  run   srv  tmp  var
boot  dev         home  lib64  media       opt  root  sbin  sys  usr
```

这里把文件移到**/home**目录下(这个相当于docker与我们的共享文件夹)

赋予执行权限 **chmod +x 文件名**

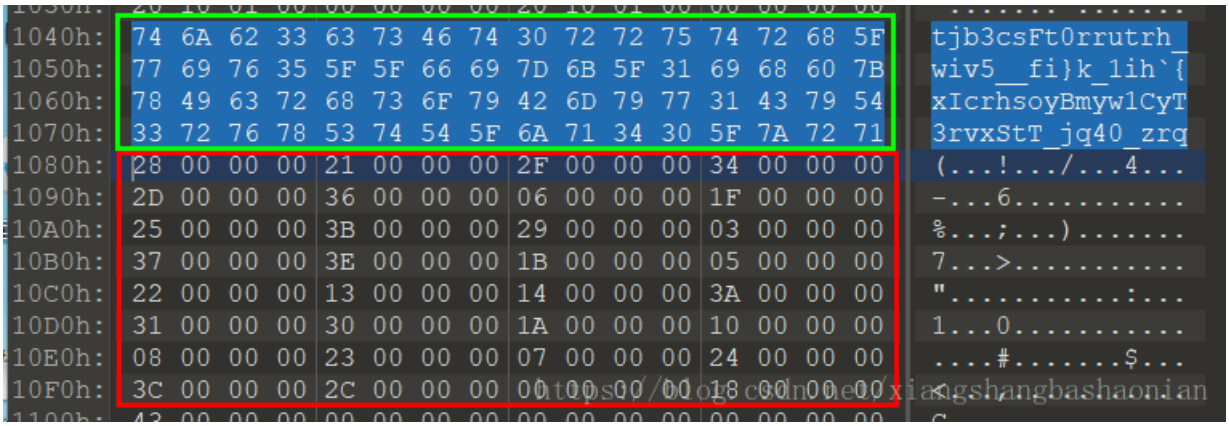
运行即可吐出flag

```
[root@df9f8627627d home]# ls
iqiqiya  riskv_and_reward
[root@df9f8627627d home]# ./riskv_and_reward
BITSCTF{s0m3_r1sc5_4r3_w0rth_1t}
```

下面是以前写的方法：

后来做题时 发现十六进制编辑器可能看到不一样的东西

结果还真发现有玄机



很明显可以看出上边绿色框中共有64个字符 下边红框32个字符

发现没有大于64的

根据经验(ps:其实就是瞎搞一通) 将它们抠出来 匹配一下看看

就是将数组b中的元素当作a中的序号 输出即可

下边直接看py代码就能明白：