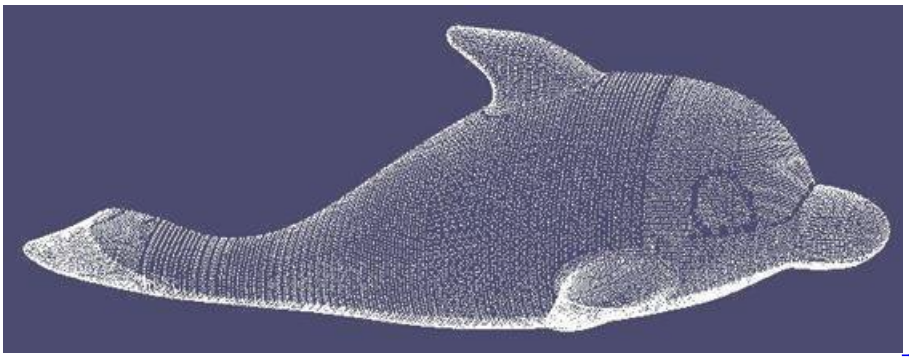
一、从零开始学逆向之XCTF-simple-unpack

原创

nini_boom 于 2020-07-02 15:45:09 发布 894 收藏

分类专栏： 逆向学习 文章标签： 逆向

本文链接：https://blog.csdn.net/nini_boom/article/details/107085391



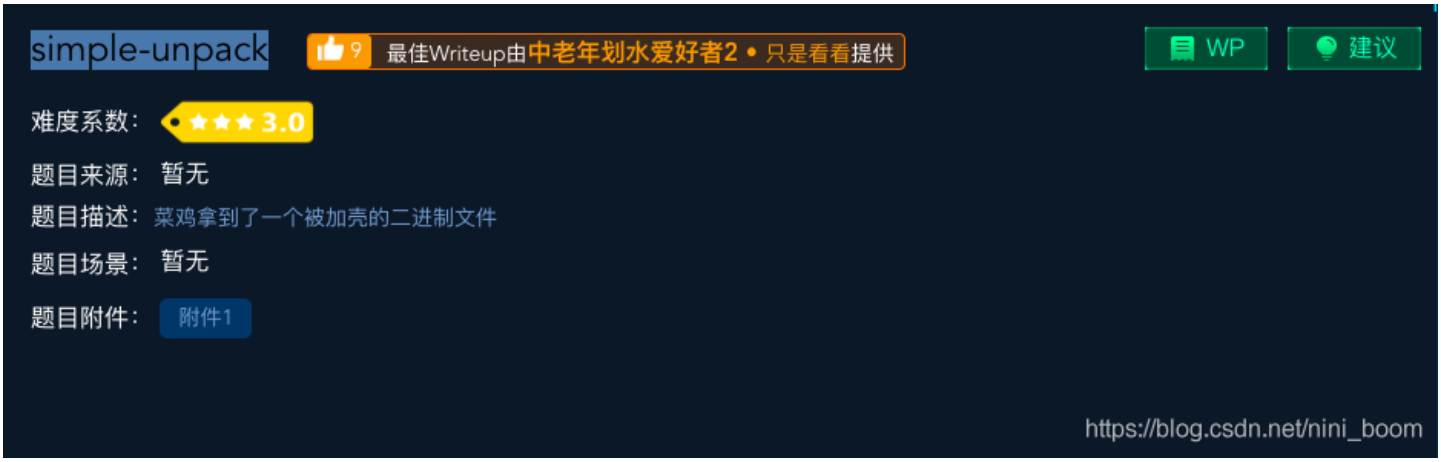
逆向学习 专栏收录该内容

4 篇文章 1 订阅

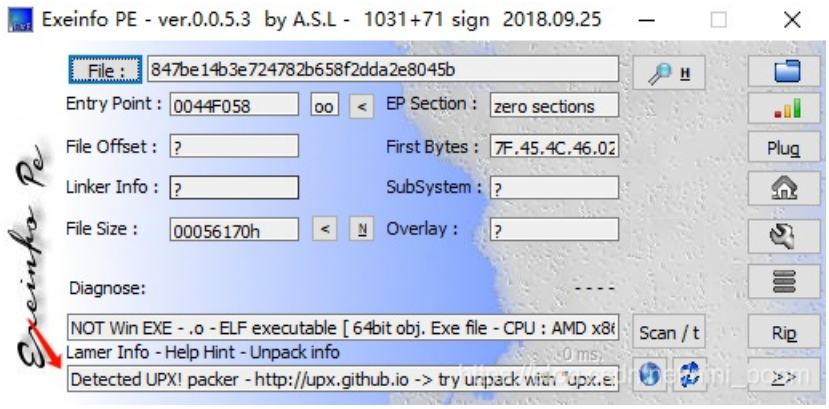
订阅专栏

使用工具:upx、exeinfo、IDA。

题目描述，简简单单的一个二进制文件。



没有格式，题目提示是加过壳的，使用exeinfo pe查看详细信息。



linux文件，exeinfo把脱壳推荐都写出来了：使用 UPX。

```
Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io

C:\Users\liyang>
C:\Users\liyang>
C:\Users\liyang>
C:\Users\liyang>
C:\Users\liyang>"\\vmware-host\Shared Folders\桌面\windows工具\windows逆向工具\upx-3.96-win64\upx.exe" -d "\\vmware-host
\Shared Folders\桌面\学习仓库\ctf\xctf\包\847be14b3e724782b658f2dda2e8045b"
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    912808 <-    352624   38.63%   linux/amd64   847be14b3e724782b658f2dda2e8045b

Unpacked 1 file.
```


IDA打开，搜索flag

```
.data:00000000006CA099                  db    0
.data:00000000006CA09A                  db    0
.data:00000000006CA09B                  db    0
.data:00000000006CA09C                  db    0
.data:00000000006CA09D                  db    0
.data:00000000006CA09E                  db    0
.data:00000000006CA09F                  db    0
.data:00000000006CA0A0                  public flag
.data:00000000006CA0A0 ; char flag[]
.data:00000000006CA0A0 flag             db 'flag{Upx_1s_n0t_a_d3liv3r_c0mp4ny}',0
.data:00000000006CA0A0                                  ; DATA XREF: main+31↑o
.data:00000000006CA0C3                  align 8
.data:00000000006CA0C8                  public _dl_tls_static_size
.data:00000000006CA0C8 _dl_tls_static_size dq 800h      ; DATA XREF:   libc setup tls+7E↑r
.data:00000000006CA0C8                                  ;   libc setup tls+1B5↑r ...
.data:00000000006CA0D0                  public _nl_current_default_domain
.data:00000000006CA0D0 _nl_current_default_domain dq offset _nl_default_default_domain
.data:00000000006CA0D0                                  ; DATA XREF:   dciqettext:loc 4031F5↑r
.data:00000000006CA0D0                                  ; free mem:loc 49ECE9↑r
.data:00000000006CA0D0                                  ; "messages"
.data:00000000006CA0D8                  public __exit_funcs
.data:00000000006CA0D8 __exit_funcs     dq offset initial       ; DATA XREF: exit+9↑o
.data:00000000006CA0D8                                  ;   cxa atexit+A↑o
.data:00000000006CA0E0                  public _IO_list_all
.data:00000000006CA0E0 _IO_list_all     dq offset _IO_2_1_stderr_
.data:00000000006CA0E0                                  ; DATA XREF:   IO cleanup+D↑r
.data:00000000006CA0E0                                  ;  IO cleanup+58↑r ...
.data:00000000006CA0E8                  align 20h
.data:00000000006CA100                  public _IO_2_1_stderr_
.data:00000000006CA100 _IO_2_1_stderr_ db  86h          ; DATA XREF: .data: IO list all↑o
.data:00000000006CA100                                  ; .data:stderr↓o
```


填入flag，结束。

学习点

- 使用exeinfo进行文件分析。
- 使用upx脱壳。