CTF Binary小技巧

Wins0n

2015-01-10

一（ ）关于我

- Wins0n
- Light4Freedom战队成员
- 业余CTF选手
- 关注二进制相关内容
- ~~*逆向、编程、算法样样精通*~~
- ~~*号称蓝莲花最怕选手*~~

微博：@HiWinson

博客：http://www.programlife.net/

二（）赛前准备

工欲善其事，必先利其器

常用的工具有:
Windbg / OllyDbg / Immunity Debugger / PEiD
IDA Pro / Hex-Rays Decompiler / ARM / x64 ……
ILSpy
Metasploit
Python
Putty / WinSCP / nc
C32Asm / 010Editor
SysinternalsSuite / PCHunter
ApkTool /JD-GUI/dex2jar…

二（ ） 赛前准备

提前准备好虚拟机镜像

- 出于安全性考虑，不要在物理机上运行题目所给的程序；
  - ✓ HDUSEC 2013 关机
  - ✓ HCTF 2014 蓝屏
- 64位的ELF经常出现于RE和PWN（**Linux x64**）；
- 64位的PE文件偶尔也会出现（Mdebug / Windbg）（**Windows x64**）；
- 给虚拟机打个快照，可以快速恢复调试状态；

二（ ） 案例分析

加了VMP的x64驱动

在HCTF线下赛中，有一个题目所给的驱动是x64的，而且还加了VMP，想要进行调试需要配置Windbg和VMWare，最好还能事先下载好符号文件！

实际情况是，Windbg无论如何都连不上VMWare……

解决方法：在虚拟机加载驱动文件后，使用PCHunter把驱动Dump出来，然后拖入IDA分析，在字符串中看到Flag明文。

Address	Length	Type	String
".…" .vmp1:000…	0000001C	C	烫烫[VMM]Vmx Check Already!
".…" .vmp1:000…	00000020	C	HCTF{HCTF_THIS_IS_NOT_THE_KEY}\n
".…" .vmp1:000…	00000014	C	10.11.14.47:23333\n
".…" .vmp1:000…	0000001E	C	[VMM]Unknown MSR READ/WRITE!\n
".…" .vmp1:000…	0000001B	C	HCTF{ERCIYUAN#__QIUBUDAA}\n
".…" .vmp1:000…	00000017	C	[Vmm]VMM CONTROL I/O!\n
".…" .vmp1:000…	00000014	C	[VMM]Split a page!\n
".…" .vmp1:000…	00000018	C	[VMM]UnHandled Action!\n

二（ ） 案例分析

带“隐写”的逆向题

在逆向分析时，偶尔会遇到一些有“隐写”有关的题目，包括对常见文件类型的识别等。

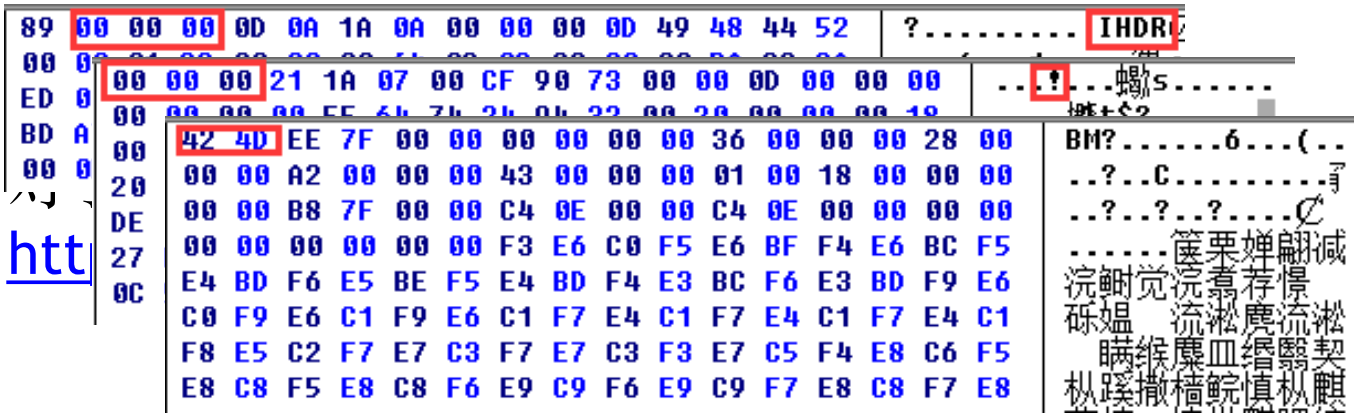
在HDUSEC 2013中，在分析一个逆向题时提取出一段二进制内容，文件开头内容为RIFF WAVEfmt，实际上是一个wav音频文件，而且声音经过了反转处理。

二（ ） 案例分析

带“隐写”的逆向题

在逆向分析时，偶尔会遇到一些有“隐写”有关的题目，包括对常见文件类型的识别等。

在HDUSEC 2013中，出现过许多抹去了文件头的情况，PNG / BMP /



htt

二（ ） 案例分析

解压缩工具妙用

有些可执行程序附加了一些资源，如果要通过调试分析来进行提取可能十分麻烦，在某些情况下，使用7zip/WinRar等工具可以进行快速提取。

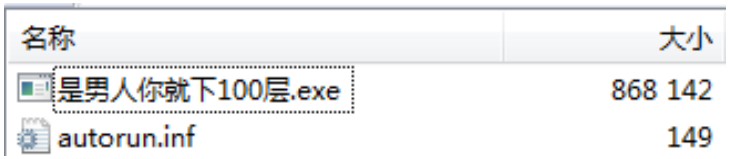
在ISCC 2013中，一个CrackMe实际上是个自解压文件，直接用WinRar处理就好了。

二（ ） 案例分析

解压缩工具妙用

有些可执行程序附加了一些资源，如果要通过调试分析来进行提取可能十分麻烦，在某些情况下，使用7zip/WinRar等工具可以进行快速提取。

在SSCTF中，使用7zip可以快速提取出EXE文件里的有用信息。



名称	大小
是男人你就下100层.exe	868 142
autorun.inf	149

名称	大小	压缩后大小
1.vbs	98	83
2.exe	593 957	548 385
1.exe	361 948	208 759

二（ ） 案例分析

借助现有工具加速分析

对于加壳、加密等各种措施进行保护的程序，可以尝试利用已有的工具加速分析过程。

在0ops CTF中，有一个逆向分析题给了一个Inno Setup的安装包，但是需要密码才能进行下一步安装操作，网上找了一个InnoExtractor工具，可以直接提取安装包中的文件

二 案例分析

事先准备好提交脚本

有时候无法通过逆向分析得到完整的Flag，因此可以尝试通过脚本来批量提交（如果不需要验证码的话）。

在HCTF线下赛中，某逆向分析题通过分析无法得到完整的flag字符串，如**hctf{??a_y*c7%etk!}**，其中问号代表一个数字，所以这里有100种可能，因此可以使用脚本提交Flag，当然也可以使用BurpSuite。

Flag提交脚本在攻防模式解题时是必备工具。

二（ ）案例分析

关于流量重放

在攻防模式的比赛中，定时抓取和分析对手的攻击流量是必要的，从对手的攻击流量中或许就能提取出exploit。

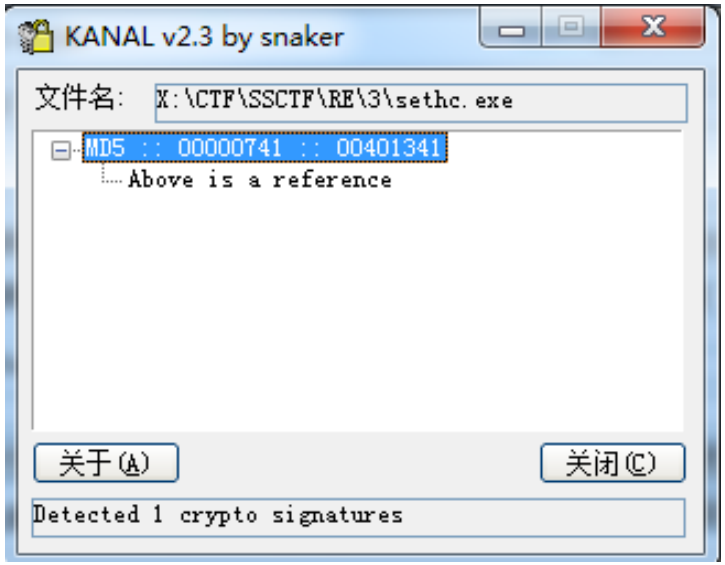
注意：不要在物理机重放流量，否则可能被rm -rf / 

二（ ） 案例分析

PEiD不止能查壳

识别程序内部所使用的加密算法，可以在一定程度加快我们的分析效率。

PEiD附带的Krypto ANALyzer可以快速识别成熟的密码算法。



二（ ） 案例分析

.NET程序分析

对于简单的.NET程序，可以直接使用ILSpy工具进行分析，在ILSpy中可以看到反编译的源码。

HCTF资格赛送分题：

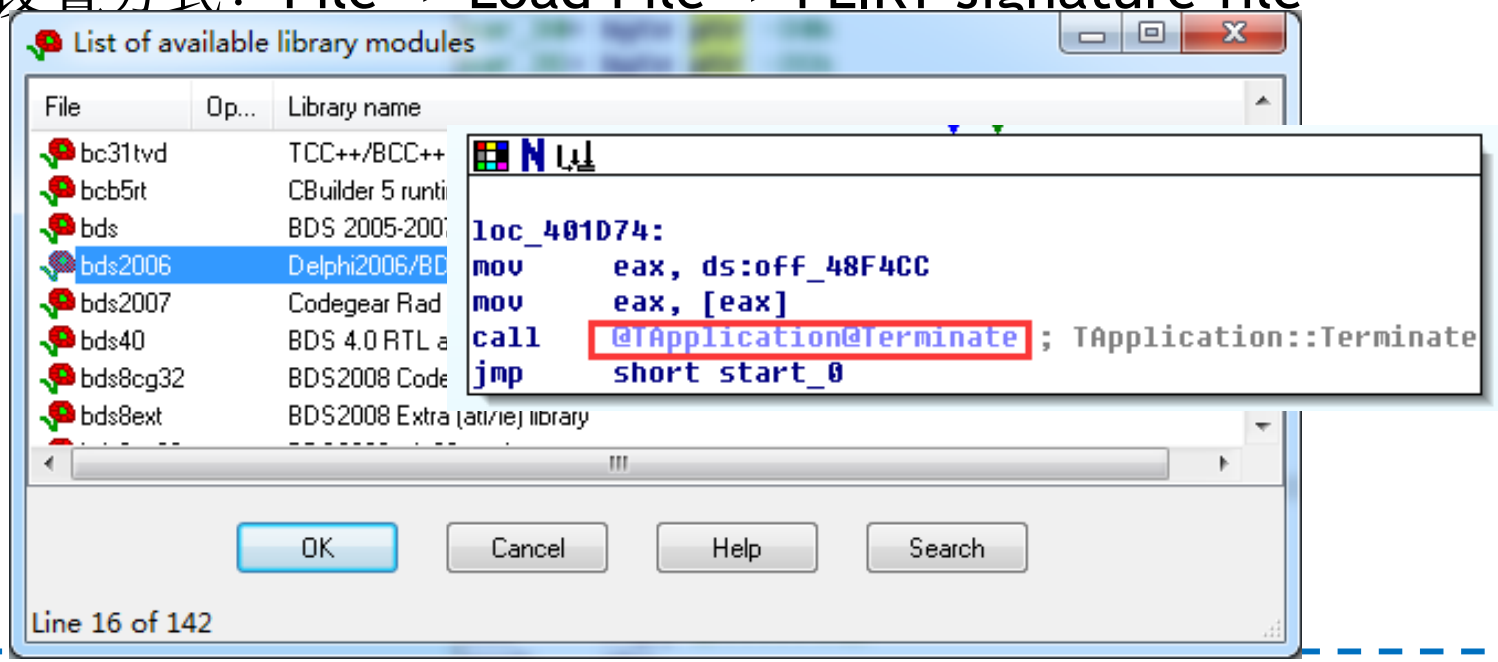
```
private void button1_Click(object sender, EventArgs e)
{
    bool flag = false;
    Config.user = this.textBox1.Text;
    string user = Config.user;
    string text = "hctf{bABy_CtsvlmE_!}";
    int num = text.CompareTo(user);
    if (num == 0)
    {
        flag = true;
    }
    if (flag)
    {
        MessageBox.Show("good !!!");
    }
}
```

二（ ） 案例分析

IDA设置FLIRT Signature

有时候IDA无法正确应用FLIRT Signature，比如一个Delphi编译的程序，如果没有被正确识别，那么很多库函数都无法自动识别。

设置方式：File -> Load File -> FLIRT signature file



二 案例分析

逆向与编程

除了逆向分析之外，动手写代码也是必须具备的技能。

AliCTF RE400：给定一个编译好的Gh0st，分析出其中的隐藏功能，完成从主控端下载一个文件。

思路：下载Gh0st源代码，配合给定的二进制程序进行逆向对比分析，找到隐藏的文件下载协议，给服务端添加下载功能完成文件下载。

二（ ） 其他技能

可以了解的东西

- IDA脚本（花指令处理）；
- OD脚本（脱壳处理）；
- 易语言；
- ……

- PWN学习（https://exploit-exercises.com/）
- CTF Writeups（https://github.com/ctfs/write-ups）
- CTF Time（https://ctftime.org/）
- ……

三

如何混入赛棍圈子

- 关注各种赛事动向，多参加比赛，尤其是线下比赛，这是混入圈子的绝佳机会！

  XCTF https://time.xctf.org.cn/

  BCTF / HCTF / SCTF / ACTF / 0CTF

  XDCTF http://ctf.xdsec.org/

  360 http://is.campus.360.cn/

  ISG http://isg.e365.org/

  ……

- 加入一个合理的团队，团队成员全面覆盖Web / Bin / Misc / Crypto等知识点。

- 多和身边的小伙伴交流

三（ ）我的参赛经历

ISCC	2011
ISCC	2013
XDSEC	2013
HDUSEC	2013
BCTF	2014

起步入门，第一次参加安全技术类比赛；

ISCC特点：

1. 考察范围广；
2. 内容比较基础；
3. 比赛时间长，新手也有充分的学习时间；
4. 决赛随机组队，可以认识各种牛逼选手；

三（ ）我的参赛经历

ISCC	2011
ISCC	2013
XDSEC	2013
HDUSEC	2013
BCTF	2014

认识新的小伙伴，在比赛中认识了Puzzor、菊花等，从这里开始接触到各种早期赛棍，为后来混入赛棍圈子奠定基础。

三（ ）我的参赛经历

ISCC	2011
ISCC	2013
XDSEC	2013
HDUSEC	2013
BCTF	2014

两三个人一起玩比赛，有时间就玩，找人一起去线下赛打酱油。

三（ ）我的参赛经历

ISCC	2011
ISCC	2013
XDSEC	2013
HDUSEC	2013
BCTF	2014
AliCTF/XCTF	

加入Light4Freedom战队，认识了更多的小伙伴，参加ACTF、0opsCTF等作为练习赛。

有了固定的团队，不定期参加国内各种比赛，成功混入赛棍圈子。

……

谢谢观看