教程一：什么是逆向工程

一、什么是逆向工程？

逆向工程是通过编译的二进制文件，尝试重建（或简单理解）程序原始的工作方法。程序员最初在写程序时，一般使用像 C++、VB、God forbid、Delphi 等高级语言。因为计算机本身不能够理解这些语言，所以程序员所写的代码需要被组装成特定的更机器化的格式，也就是计算机所能理解的格式。这个足够原始的代码被叫做机器语言。对人类而言这些代码不太友好，经常需要耗费大量的脑力才能准确的明白程序员的思想。

二、逆向工程是干什么的？

逆向工程能够被用于计算机科学的很多领域，不过这里有几个通用分类：

- 它使得与历史遗留代码（就是已经没有了源代码）进行交互成为可能
- 打破拷贝保护（即打动你的朋友和省钱）
- 研究病毒和恶意软件
- 评估软件质量和稳健性
- 向软件中添加功能

第一个分类就是当源代码不可用时，通过逆向工程编码与已存在的二进制程序进行交互。关于这个我不会讨论太多，因为它太枯燥了。

分类二（也是最大的）是打破拷贝保护。就是禁用限时试用限制，干掉注册，以及免费获得商业软件的其他所有功能。这方面我们会进行大量的讨论。

分类三是学习病毒和恶意软件代码。之所以需要逆向工程，是因为没有几个病毒编写者会向外说出他是如何编写的代码，应该具有什么功能，以及怎样完成这些功能（除非他们真的很愚蠢）。这真是一个让人兴奋的领域，不过这也需要大量的知识。现在我们不会讨论太多，具体的都在后面章节。

分类四是评估软件安全和漏洞。当创建大型应用（想想 Windows 操作系统），逆向工程被用来确保系统不会包含任何主要的漏洞、安全缺陷。坦率的说，是让破解者破解软件时尽可能的困难。

最后一个分类是向现有软件中添加功能。就我个人来说，我认为这是最有趣的地方之一。不喜欢你的网站设计软件中的图片？换掉它们。想在你最喜欢的字处理软件中添加一个加密文档的菜单项？那就加上。想要在 windows 计算器中添加一个损人的消息框去无止尽的作弄你的同事？那就干他一票。在后面的系列中我们将进入这个世界。

三、需要什么知识？

与你猜测的一样，成为一名合格的逆向工程师需要大量的知识。幸运的是，在开始逆向工程时大量的知识都不是必须的。这正是我想要开始的地方。也就是说，享受逆向的乐趣以及从本教

程中收获一些东西。然后你应该至少对一个程序是如何工作的有一个基本的理解（比如，你应该知道一个基本的 if.....then 语句是什么样,数组是什么样,至少理解一个基本的 hello world 程序)。第二，强烈建议熟悉汇编语言。即使没有汇编基础你也可以通过本教程，不过在有些地方你就会希望自己是 ASM 的大牛，以便真正理解你正在做什么。另外，你需要大量的时间来学习怎样使用工具。这些工具对于逆向工程来说是无价的，也需要学习这些工具的快捷键、缺陷和特性。最后，逆向工程需要大量的实践。与不同的壳/保护/加密设计玩耍。学习编写程序的原始语言（甚至 Delphi)、破解反逆向工程的技巧等等。本教程的最后，我加上了“进一步阅读”部分，有一些建议。如果你真的想要学好逆向，强烈建议你进一步阅读其他内容。

四、使用哪种工具？

在逆向领域中有很多种不同的工具可用。在逆向二进制时有许多特别的保护需要被解决 。有一些可以让逆向者的生活更轻松。有一些我认为是“订书针”项目，就是经常用到的那些。对于大部分工具来说，是符合几种分类的：

1、反汇编器

反汇编器尝试将二进制形式的机器语言代码以一种友好的形式显示出来。它们也进行数据推断比如函数调用、传递变量和文本字符串。这就让可执行文件看起来更像人类可读的代码，而不是一串数字串起来的样子。反汇编器非常多，它们中的一些专

门做一些特定的工作（比如 Delphi 中的写二进制）。主要是你找一个你觉得最舒服的。我喜欢用 IDA（ http://www.hex-rays.com/上有免费版本可用），以及一些不太知名的在特定情况下比较有用的工具。

2、调试器

调试器是逆向工程师的面包和黄油。它们首先分析二进制文件，这一点特别像反汇编器。然后调试器允许逆向者单步执行代码，一次运行一行并且查看结果。这对于发现一个程序是如何工作来说是无价的。最后，一些调试器允许对改变的代码做说明，然后带着那些变化再次允许。示例调试器是 Windbg 和 Ollydbg。我几乎只用 Ollydbg（http://www.ollydbg.de/），除非调试内核模式的二进制文件，不过我们不久就会接触到的。

3、十六进制编辑器

十六进制编辑器可以让你查看二进制文件的指定字节，并且可以更改它们。也提供了搜索指定字节，保存部分二进制数据到磁盘等等。有许多免费的十六进制编辑器，并且大部分都挺好用。本教程的大部分都不会用到它们，不过有时候它们是无价的。

4、PE 和资源 查看器/编辑器

每一个被设计在 windows 上运行的二进制文件（linux 也是一样），在它的起始地方都有一个数据区用于告知操作系统如何设置和初始化程序。它告诉 OS 它需要多少内存、它需要借用哪些 DLL 的代码、对话框的相关信息等等。它叫做可移植的执行体

（Portable Executable），所有被设计用来在 windows 上运行的程序都需要有一个。

在逆向工程的世界里，这个结构的字节就变得非常重要，因为它给逆向者需要的关于二进制文件的信息。最终，你想要（或需要）改变这个信息，要么让程序做一些和它初衷不一样的事情，要么让程序回到它以前的样子（像保护器让代码变得很难理解之前的样子）。有非常多的 PE 查看器和编辑器工具。我用 CFF Explorer (http://www.ntcore.com/exsuite.php) 和 LordPE (http://www.woodmann.com/collaborative/tools/index.php/LordPE)，不过你可以随意使用你觉得舒服的工具。

大多数的文件也有资源区。包括图像、对话框、菜单、图标和文本字符串。有时候你只看（和修改）资源区就觉得很有意思。此教程的最后我会给你展示一个例子。

5、系统监视工具

在逆向程序时，有时候观察应用程序对系统做出的改变也很重要（在研究病毒和恶意软件时尤其重要），是不是有注册表项被创建或查询？是不是有.ini 文件被创建？是不是有进程被创建，或许用来阻挠软件被逆向？系统监视工具有 procmon、regshot 和 process hacker。后面我们会讨论这些。

6、其他工具和信息

在学习过程中有其他工具我们将用到，比如脚步、脱壳工具、

壳识别器等。一些 Windows API 参考工具也归于此类。这个 API 是巨大的，有时也很复杂。在逆向工程中知道被调用的 API 在干什么是非常有用的。

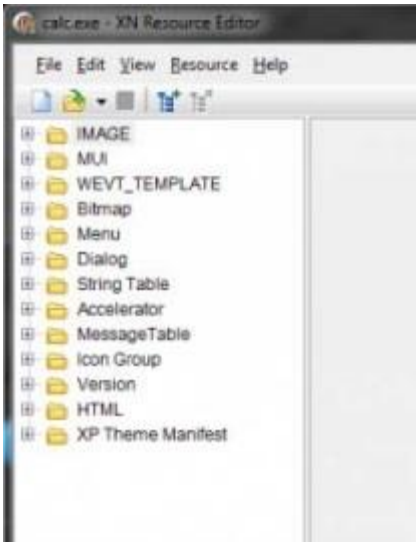
7、啤酒

五、那么，我们开始吧！

即使我们在拥有很少知识的情况下开始，在第一课中我想让你尝尝逆向的滋味。此教程中包含有一个资源查看/编辑器，叫做 XN Resource Editor。

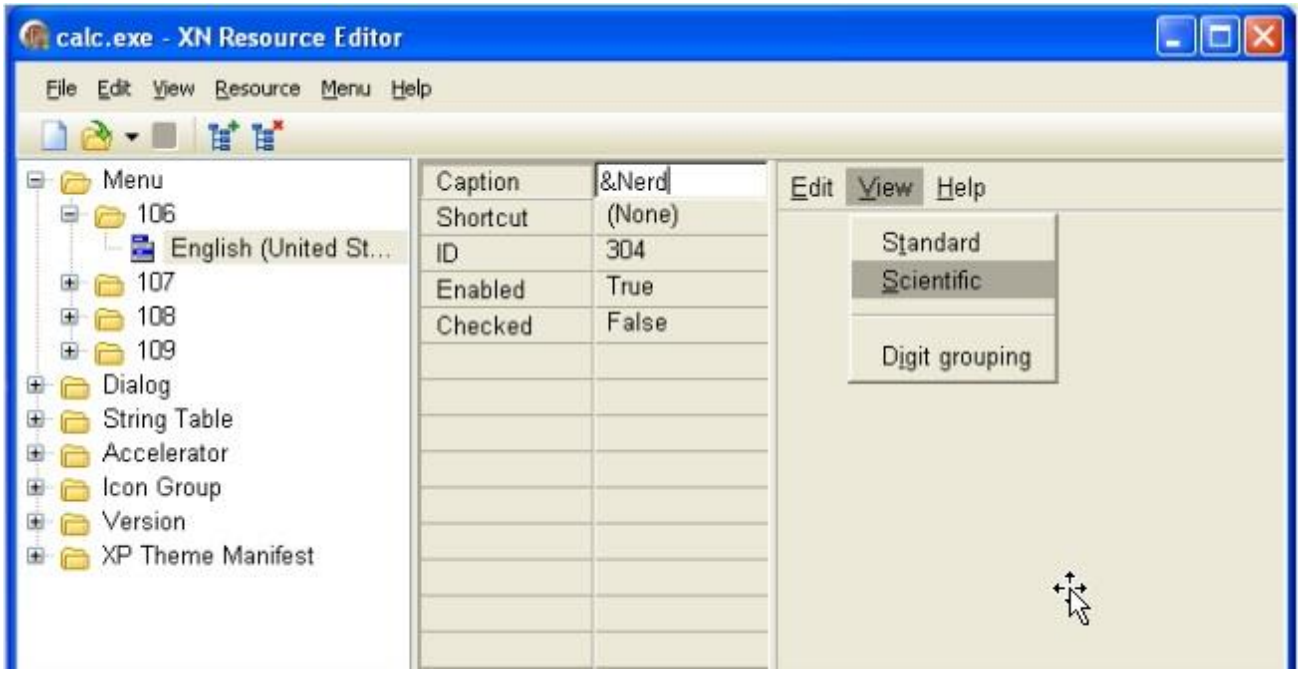
它是免费的。基本上，这个程序可以让你查看 exe 文件的资源区，当然也可以修改这些资源。我已经感觉到你对“这些”的巨大兴趣，你可以修改程序中的菜单、图标、图片、对话框，你可以给它命名。下面我们来改一个试试：

首先，运行 XN。点击顶部的载入图标，找到 Windows\System32\并且载入 calc.exe（你的 windows 默认的位置可能不同）。你会看到一堆可用的文件夹：



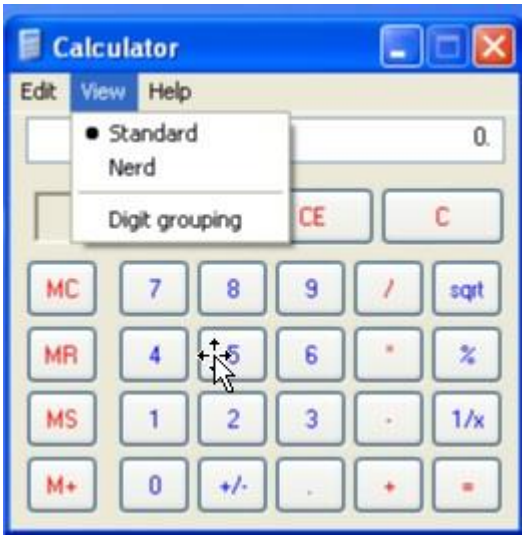
可以看到有 Bitmaps 文件夹（程序显示的任何图片），Menu（顶级菜单项），Dialog（对话框，相关文本和按钮），String Table,，IconGroup 等。你可以对它们为所欲为了。确保另存为一个不同的文件（你肯定不喜欢因为一个 XX 计算器就重装 windows）。细节如下：

点击那个靠近 Menu 的加号。你会看到以数字命名的文件夹。它是程序中资源的 ID，以便 windows 用来访问相关资源。同样打开该文件夹。你可以看到一个“English (United States)”图标或者类似的东西。如果你点击它，你会看到一个有关菜单外观的图表（你能点击旁边一个类似真实菜单的菜单）。

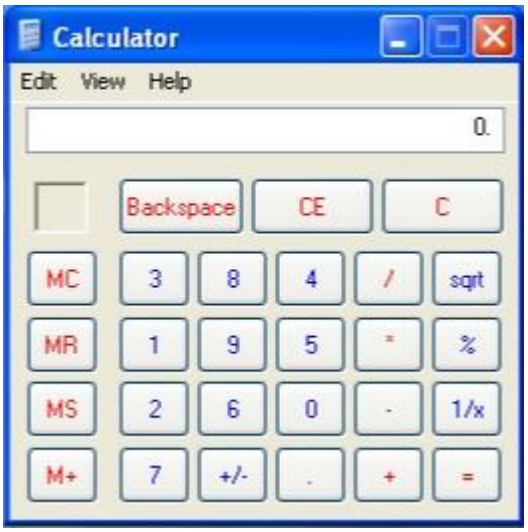


现在，点击菜单项“Scientific”。那个 Caption 字段应该改成“&Scientific”。那个符号是告诉你“热键”是什么，这里是大写的“S”。假如我想用“e”代替作为热键，应该是这样

的“Sci&entific”。好了，和内建的计算器热键不一样吧？仅仅修改了它们!! 不过，我们做一些其他的吧。在 Captial 字段，将 &Scientific 替换成 “&Nerd”。这将会把菜单项修改成“Nerd”并且使用热键“N”（我们看看菜单中其他选项以确保没有其他的菜单项使用“N”作为热键)。你应该对所有的菜单项做这个工作。现在，到上面的 File 菜单（在 XN Resource 中）并且选择“Save As...”。用不同的名字保存你的新版计算器（最好保存到不同的路径)，然后运行它。



当然，你不需要止步于此。为了开动我同事的榆木脑袋，我修改了他的计算器的所有数字。



如你所见，限制你的只有天空。

延伸阅读（译者注：这里都是英文书，可能部分有中文翻译，未经查证）：

1、汇编语言。*Assembly Language For Intel Based Computers* 中是一本关于汇编的书。你也可以查看一些网站，提供了大量的下载 ，说明 ，示例代码 和帮助。另一个好的资源是“The Art of Assembly”。我将会在今后的某个章节中包含进来，不过你也可以从这里下载。

2、PE 文件结构。最好的资源是微软自己的“An in-depth look into the Win32 Portable Executable File Format”。另一个好的文档（有很多漂亮的图片）是“PE File Structure”。它是一个可下载的 PDF 文件。

3、Windows 操作系统内核。有 Mark Russinovich 的书

“Microsoft Windows Internals”。它想女人的棒球(baseball)一样让人兴奋，不过它是 THE 资源。

4、破解教程。www.Tuts4You.com 就是这样的一个地方。