Q1IQ

北京邮电大学 网络空间安全专业

IDA打PATCH学习

keypatch基本使用

Edit –> Keypatch –> Patcher

选中一行指令patch

可以输入汇编代码 nop啥的

Edit –> Keypatch –> Fill Range

选中一定范围的指令一起patch

可以输入汇编代码

也可以输入16进制“90”“0x90”“90,91”“AAh”等。

Edit –> Patch program –> Apply patches to input file

撤消上一个操作，而且可以撤销多次（好像是无限制？亲测20次还是能继续撤销（好哎

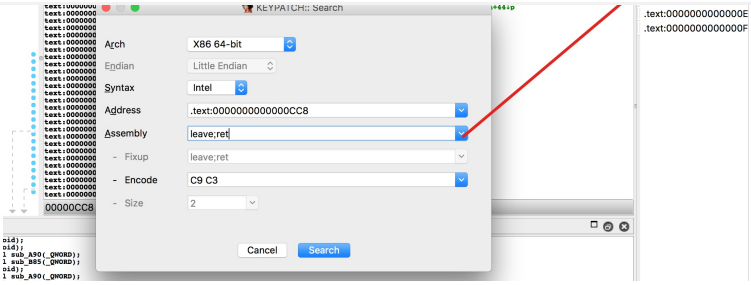
Edit –> Patch program –> Apply patches to input file

将修改保存到一个新的二进制文件（这是ida原本就有的功能

Edit –> Keypatch –> Search

可以搜索汇编指令，不能直接搜索16进制

多条指令用 `;` 分隔



Q1IQ

北京邮电大学 网络空间安全专业

备注

keypatch怕你忘了patch前的指令是啥，还加了个备注提醒。太贴心了

打patch方法

UAF

增加置0的环节

off by one

改读的字节数

栈溢出

改读的字节数

堆溢出

改读的字节数

格式化字符串

增加合适的参数

Q1IQ

北京邮电大学 网络空间安全专业

nop 掉 free

nop 掉 malloc

在读的字节中过滤一些特殊的字符

打乱got表

Keystone库 安装踩坑

环境：macOS

python:2.7

python终端报错信息如下，网上说少so库，我没在系统里找到。

```
>>> import keystone
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "/usr/local/lib/python2.7/site-packages/keystone/__init__.
    from .keystone import Ks, ks_version, ks_arch_supported, versi
  File "/usr/local/lib/python2.7/site-packages/keystone/keystone
    raise ImportError("ERROR: fail to load the dynamic library.")
ImportError: ERROR: fail to load the dynamic library.
```

解决方法：

```
//下载
https://pypi.python.org/packages/9a/fc/ed0d3f46921bfaa612d9e
```

```
//安装
cd keystone-engine-0.9.1-3
sudo python setup.py install
```

这下终端不报错了，ida还是报错

```
appledeMacBook-Pro-2:keystone-engine-0.9.1-3 apple$ python
Python 2.7.16 (default, Jun 19 2019, 07:41:28)
[GCC 4.2.1 Compatible Apple LLVM 10.0.0 (clang-1000.11.45.5)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> import keystone
>>>
```

```
Python>import keystone
Traceback (most recent call last):
  File "<string>", line 1, in <module>
  File "/Applications/IDA Pro 7.0/ida.app/Contents/MacOS/python/keystone/__init__.py", line 2, in <module>
    from . import arm_const, arm64_const, mips_const, sparc_const, hexagon_const, systemz_const, ppc_const, x86_const
ImportError: cannot import name arm_const
```

解决方法：

```
Type "help", "copyright", "credits" or "license" for more information.
>>> import keystone
>>> print keystone
<module 'keystone' from '/usr/local/lib/python2.7/site-packages/
>>> print keystone.arm_const
<module 'keystone.arm_const' from '/usr/local/lib/python2.7/site
```

```
//将其复制到ida.app里
$ sudo cp -r ./keystone /Applications/IDA\ Pro\ 7.0/ida.app/Conte
$ sudo cp -r ./keystone /Applications/IDA\ Pro\ 7.0/ida64.app/Co
$ pwd
/usr/local/lib/python2.7/site-packages
```

最后重启ida

成功!

```
Python>import keystone
Python>print keystone.arm_const
<module 'keystone.arm_const' from '/Applications/IDA Pro 7.0/ida.app/Contents/MacOS/python/keystone/arm_const.py'>
```

2019-08-16 学习

Post Anterior Próximo post

Q1IQ

北京邮电大学 网络空间安全专业