radamsa fuzz 移植 win 平台下的使用

asp**** / 2018-10-28 08:35:00 / 浏览数 2775 安全工具 工具 顶(0) 踩(0)

0x00 Radamsa简介

Radamsa是一个用于稳健性测试的测试用例生成器，也就是一个模糊测试器。它通常用于测试程序如何能够承受格式错误和潜在的恶意输入。它的工作原理是读取有效数据
类似于project zero
的开源项目domato，Radamsa只负责样本生成。而区别于domato的一点是，Radamsa需要输入原始样本来进行变异得到新的的样本(Radamsa很牛逼一点在于
不需要你指定你的原始样本的格式，他会自动判定，对于fuzzer来说真的超级方便)。
Radamsa 的项目是用于linux平台上面的项目，并没有开放windows版本。

0x01 Radamsa linux 构建

Radamsa fuzz project
linux上的构建方法如下：

```
$ sudo apt-get install gcc make git wget
   $ git clone https://gitlab.com/akihe/radamsa.git && cd radamsa && make && sudo make install
```

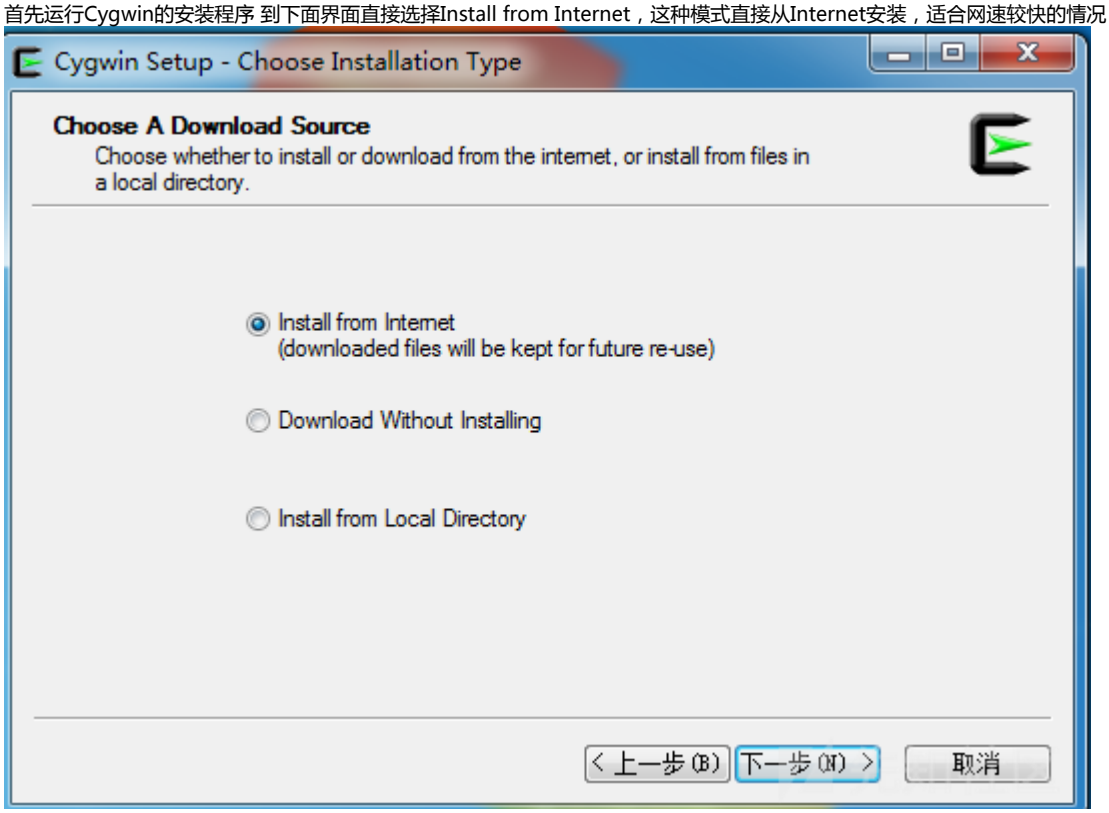
0x02 Radamsa win 构建

但是如果需要对win平台的目标程序进行fuzz 则需要想办法进行移植。
下面给出一种比较简单方式,win上使用Cygwin用Cygwin编译radamsa。

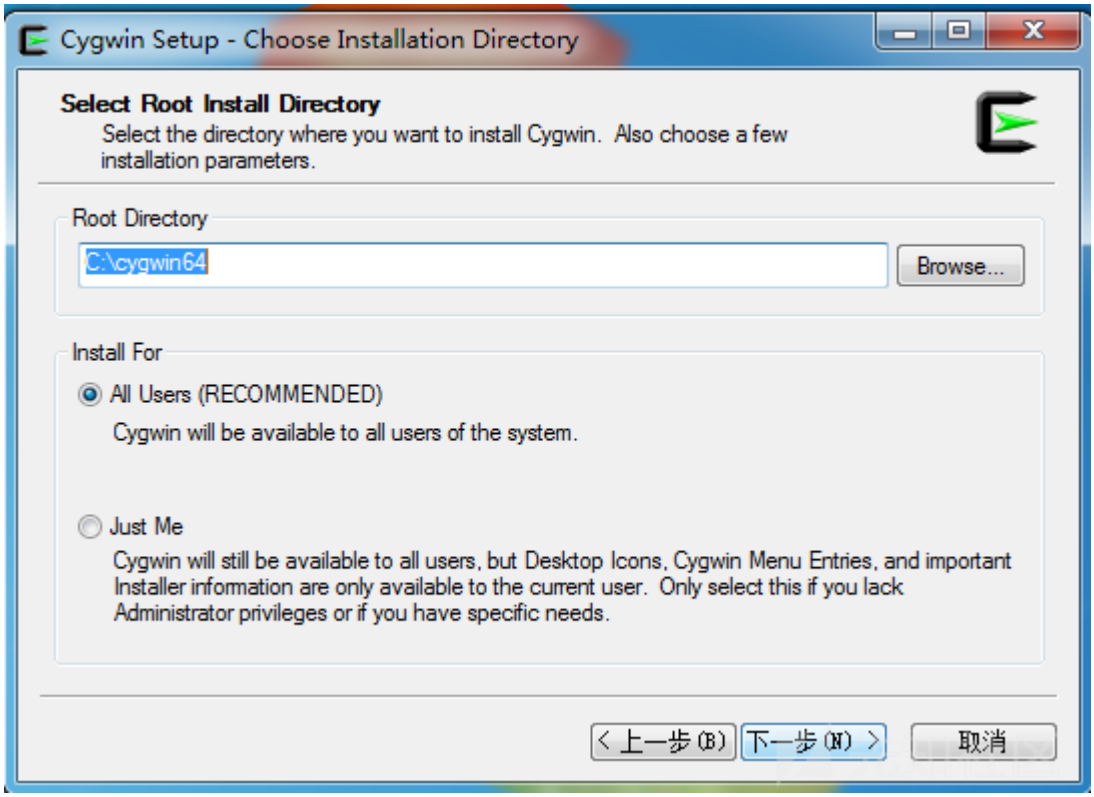
Cygwin的安装

通过下面的链接选择你需要的cygwin版本。
Cygwin download
下载完成后就需要通过Cygwin来安装linux上构建Radamsa需要的工具了，gcc/clag、git、wget、make

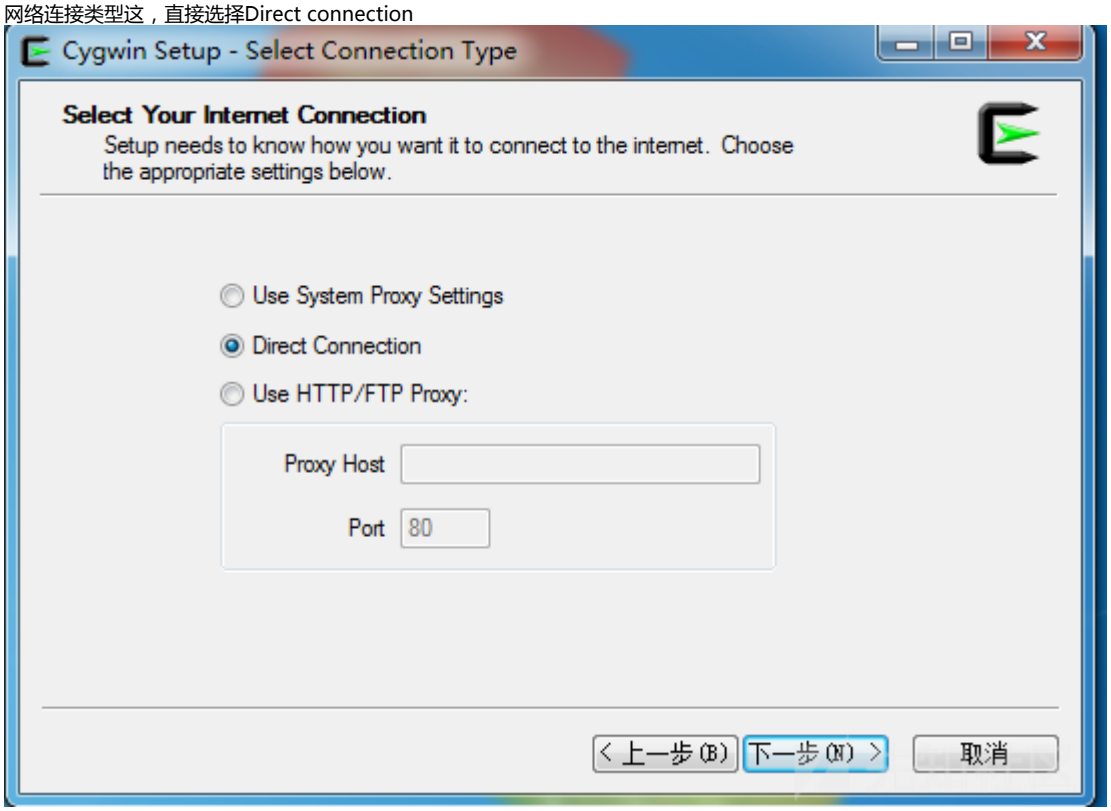
首先运行Cygwin的安装程序 到下面界面直接选择Install from Internet，这种模式直接从Internet安装，适合网速较快的情况；



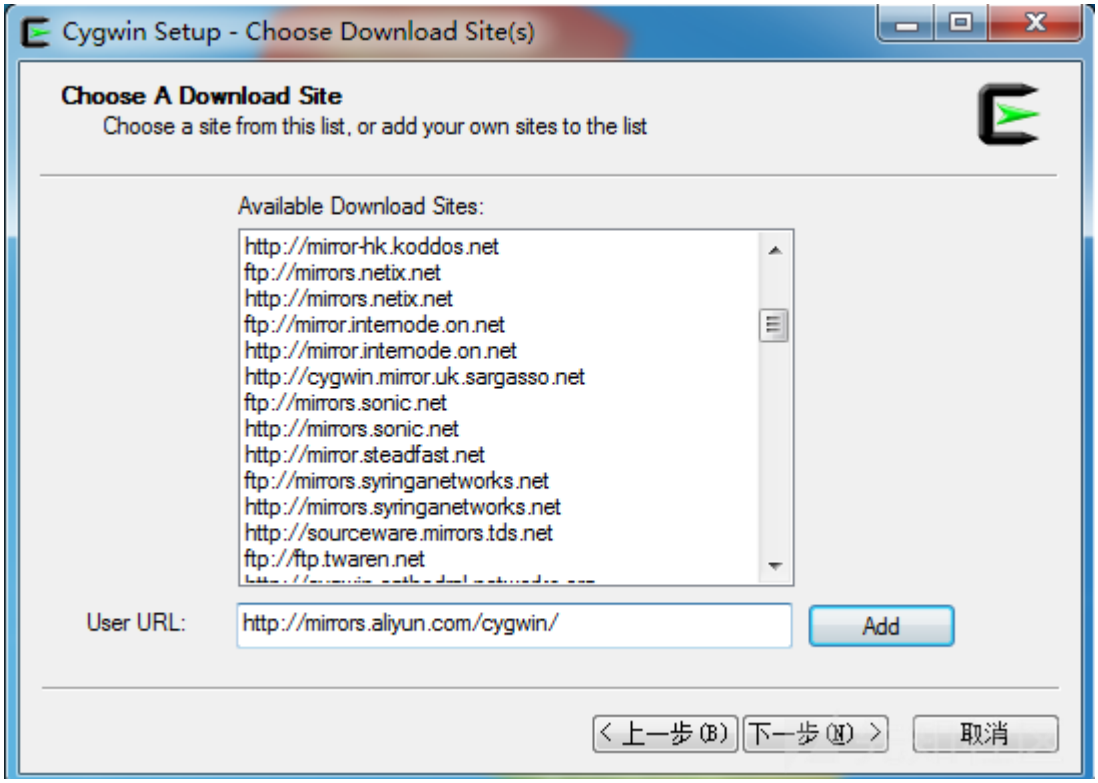
然后就是一些设置Cygwin 模拟linux环境的文件存储位置设定，看个人喜好定吧，我是直接默认



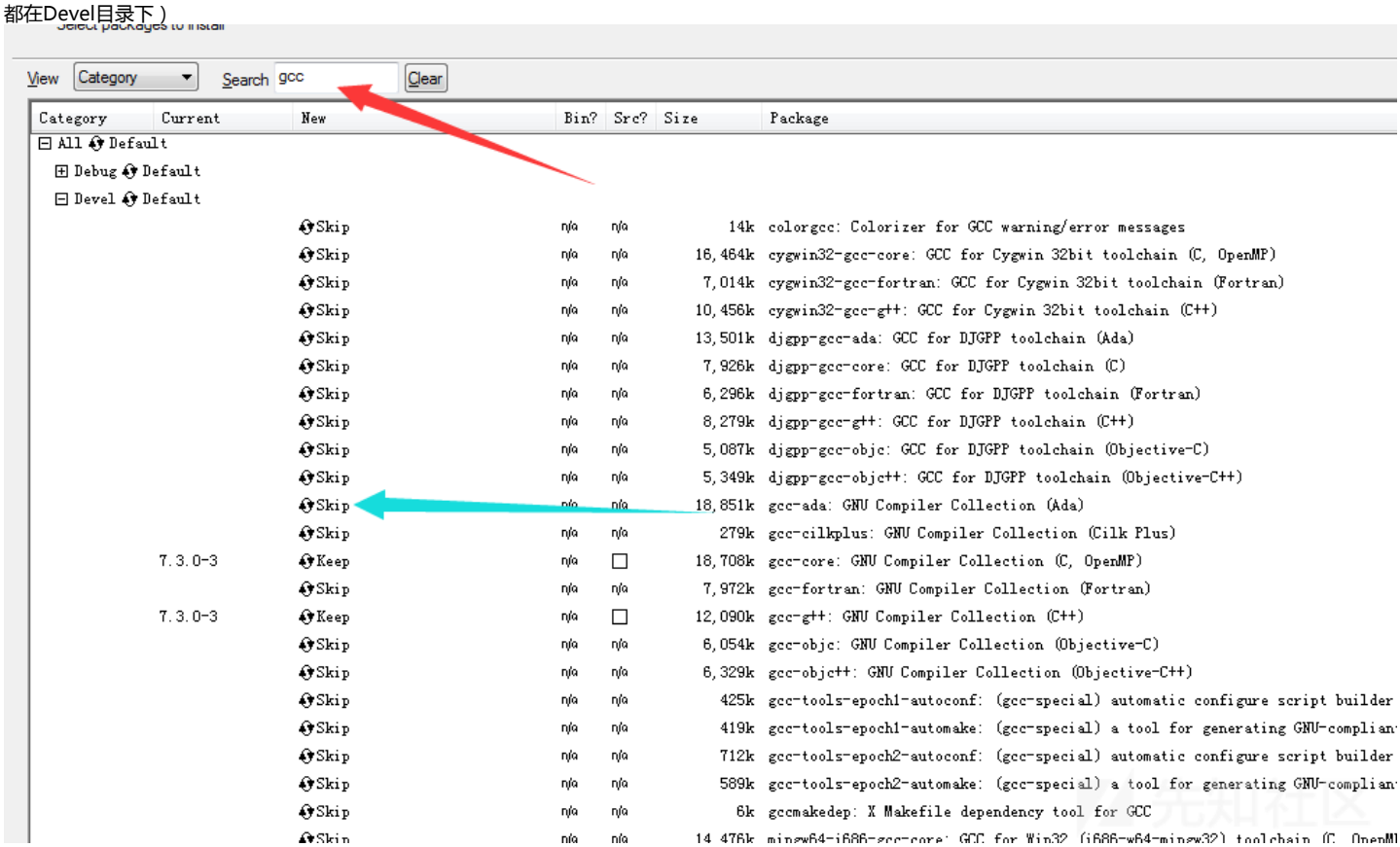
网络连接类型这，直接选择Direct connection



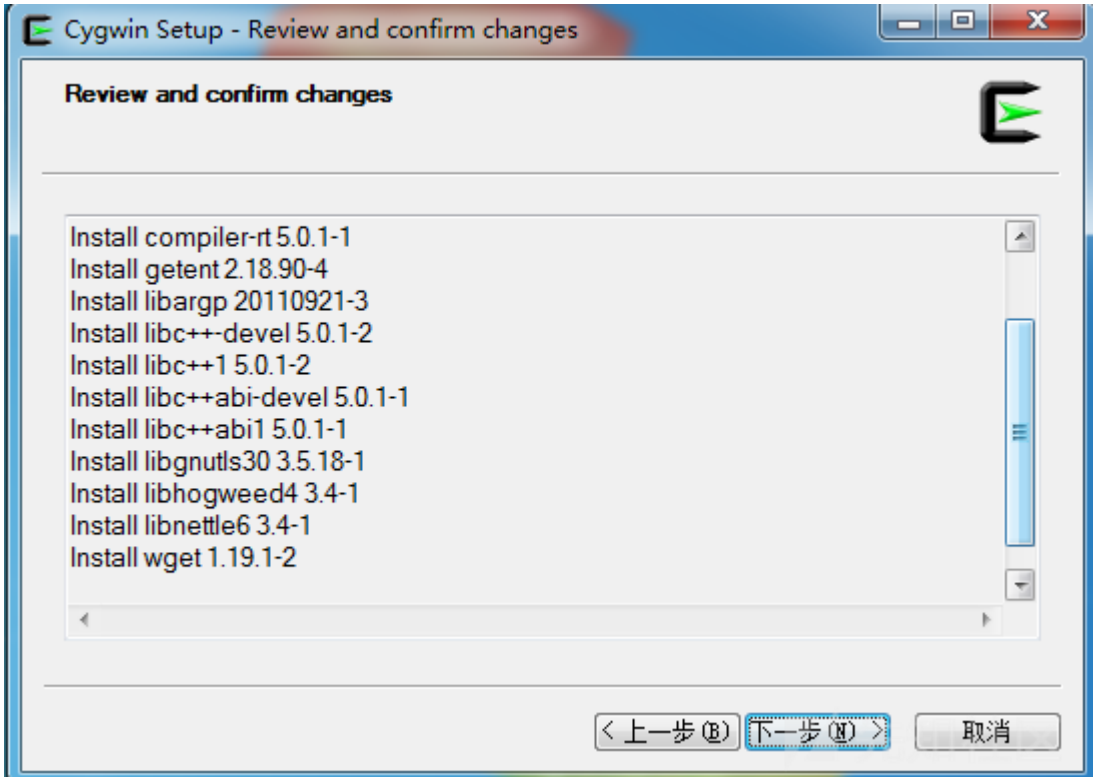
添加使用阿里云镜像这个比较快 http://mirrors.aliyun.com/cygwin/



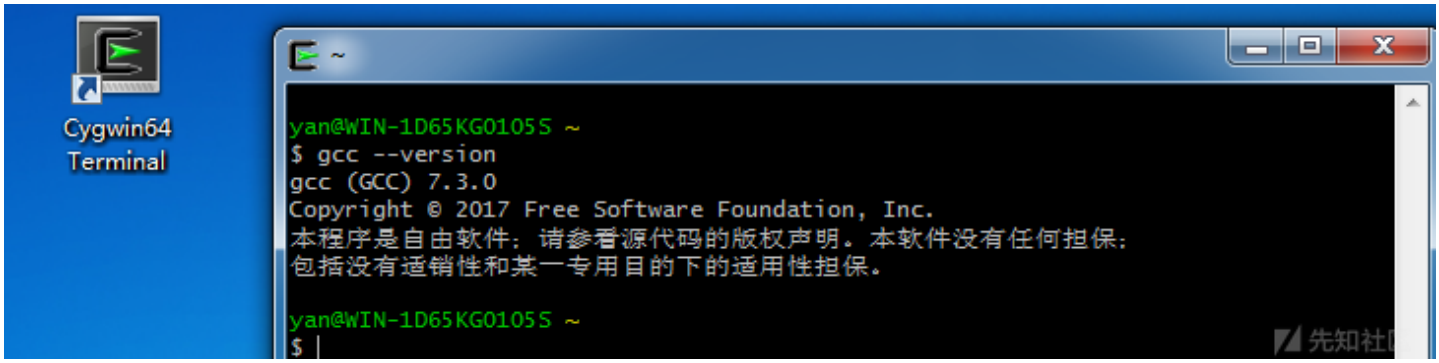
以gcc为列子说一下，在下图中搜gcc 然后把蓝色箭头指向Skip 点击一下就会显示当前能安装的版本。这就代表你需要安装的套件以及版本（gcc/clang 、git 都在Devel目录下）



最后就是喜闻乐见的无脑最后一步了

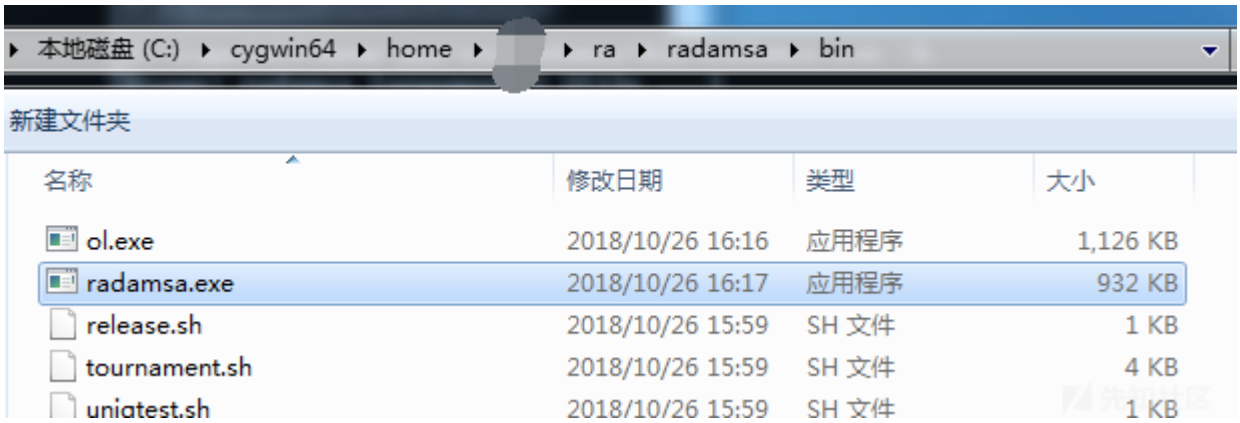


安装完成后通过cygwin terminal启动一个shell 查看一下gcc --version

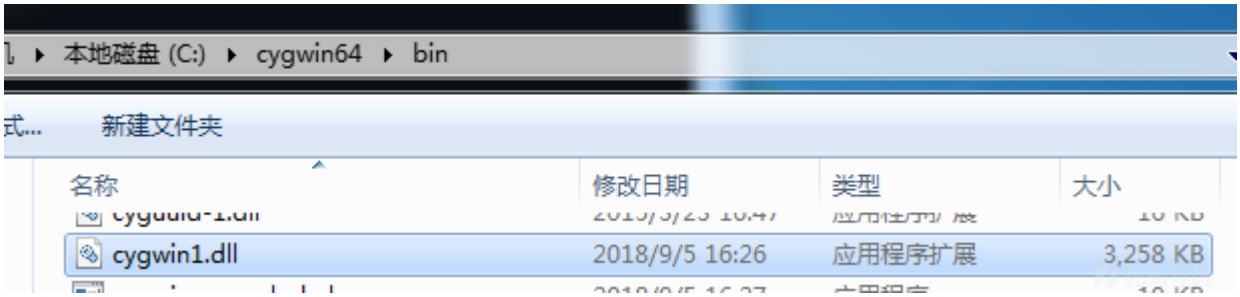


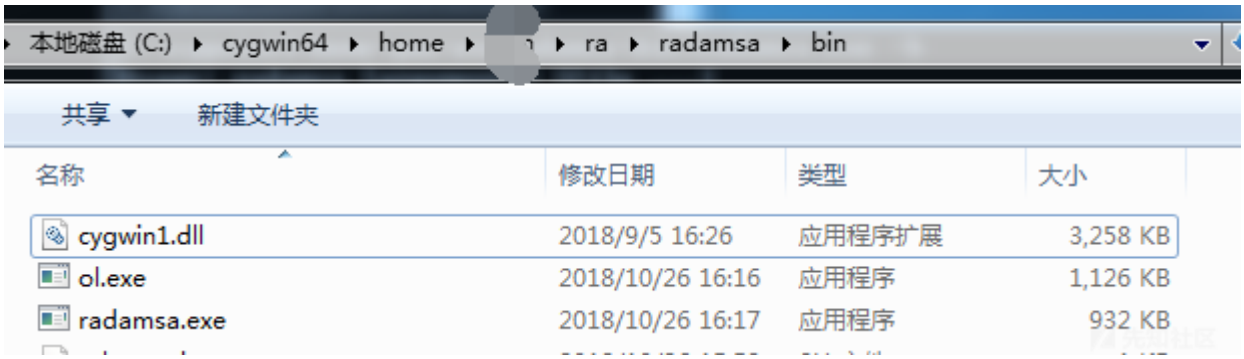
Cygwin 下构建Radamsa

■Cygwin■■linx■■■■■■■■linux■■■■■■■■
■make ■■■make install■■■■■■■ /radamsa/bin ■■■■■■■■■ radamsa.exe



■■■■exe■■cygwin■■■■■■■■■■cygwin■■■■cygwin1.dll ■cygwin■■■■■■■/bin/■■■■■■cygwin1.dll ■■■ radamsa.exe ■■■■■■■■■■cmd■■■■






```
C:\cygwin64\home\yan\ra\radamsa\bin>radamsa.exe -h
Usage: radamsa [arguments] [file ...]
  -h | --help, show this thing
  -a | --about, what is this thing?
  -V | --version, show program version
  -o | --output <arg>, output pattern, e.g. out.bin /tmp/fuzz-%n.%s, -, :80 or 1
27.0.0.1:80 [-]
  -n | --count <arg>, how many outputs to generate (number or inf) [1]
  -s | --seed <arg>, random seed (number, default random)
  -m | --mutations <arg>, which mutations to use [ft=2,fo=2,fn,num=5,td,tr2,ts1,
tr,ts2,ld,lds,lr2,li,ls,lp,lr,lis,lrs,sr,sd,bd,bf,bi,br,bp,bei,bed,ber,uw,ui=2,x
p=9,ab]
  -p | --patterns <arg>, which mutation patterns to use [od,nd=2,bu]
  -g | --generators <arg>, which data generators to use [random,file=1000,jump=2
00,stdin=100000]
  -M | --meta <arg>, save metadata about generated files to this file
  -r | --recursive, include files in subdirectories
  -S | --seek <arg>, start from given testcase
  -d | --delay <arg>, sleep for n milliseconds between outputs
  -l | --list, list mutations, patterns and generators
  -C | --checksums <arg>, maximum number of checksums in uniqueness filter (0 di
sables) [10000]
  -v | --verbose, show progress during generation

C:\cygwin64\home\yan\ra\radamsa\bin>_
```


hava fun :)

上一篇：HITCON CTF 2018 W... 下一篇：使用DNS over HTTPS (...

1. 0 条回复
   - 动动手指，沙发就是你的了！

目录