秋明分享平台之

centos6.6下使用python构造DNS请求报文

撰稿人：秋明

撰稿人邮箱：tyumen@zhoufengjie.cn

QQ群：90122290

本文撰稿日期： 2015年2月25日星期三

本站口号：开源、分享、共进

版权所有：随便使用

注解：任何想通过本平台分享文档的，可以随时联系，文档里面注明出稿人和邮箱，方便文档使用者同撰稿的兄弟技术咨询沟通和交流；

目录

1 前言 3

2 基础环境安装 3

2.1 安装libnet： 3

2.2 安装pylibnet： 3

3 编写测试 3

# 前言

DDOS攻击里面有一招叫：DNS大包攻击；具体原理为：构造DNS请求报文，发送到公网的DNS服务器上面，请求具有返回大量数据报文的dns请求（比如：dig ANY isc.org +notcp +bufsize=4096）；

# 基础环境安装

## 安装libnet：

下载地址：http://sourceforge.net/projects/libnet-dev/

# tar zxvf libnet-1.2-rc3.tar.gz

# cd libnet-1.2-rc3

# ./configure

# make

# make install

## 安装pylibnet：

下载地址：http://sourceforge.net/projects/pylibnet/

# tar zxvf pylibnet-3.0-beta-rc1.tar.gz

# cd pylibnet-3.0-beta-rc1

# python setup.py install；

# 编写测试

代码如下：

#!/usr/bin/python

import sys

import libnet

from libnet.constants import \*

l = libnet.context(

RAW4, # The injection type

'eth0' # Device name

)

dst\_ip = l.name2addr4(

'223.236.117.2', # Let's get the network byte ordered representation of this IP

DONT\_RESOLVE

)

src\_ip = l.name2addr4(

'10.0.0.31', # Let's get the network byte ordered representation of this IP

DONT\_RESOLVE

)

#query

import struct

query=struct.pack('b3sb4sb3sbbbbb',3,'www',4,'sina',3,'com',0,0,1,0,1)

dns\_tag = l.build\_dnsv4(

h\_len=12,

id=2,

flags=256,

num\_q=1,

num\_anws\_rr=0,

num\_auth\_rr=0,

num\_addi\_rr=0,

payload=query,

)

udp\_tag = l.build\_udp(

dp=53, # destination port

sum=0,

len=38,

)

# Now onto the IPv4 header

#ipv4\_tag = l.autobuild\_ipv4(

ipv4\_tag = l.build\_ipv4(

# len=IPV4\_H + UDP\_H + 12, # IPV4 packet length

prot=IPPROTO\_UDP, # Protocol type

dst=dst\_ip,

src=src\_ip,

)

#send packet

l.write()