Network Administration/System Administration (NTU CSIE, Spring 2019) Homework #0

Network Administration

True or False

1. A DNS server stores its records locally.
False.
從wiki可以看到一段話，“The domain name space consists of a tree data structure. Each node or leaf in the tree has a *label* and zero or more *resource records* (RR)”，查詢DNS紀錄的時候，如果DNS沒有持有cache，DNS會從根域名伺服器開始一層一層向權威域名伺服器查詢，直到返回A紀錄，所以DNS不會在本地儲存所有的紀錄。

Reference: https://en.wikipedia.org/wiki/Domain_Name_System

2. TCP is preferable over UDP in all cases since it provides reliable data transfer while UDP Doesn't.
False.
當資料不需要正確性但需要速度時，UDP是更好的選擇，例如實況或是遊戲等。前一陣子也有看到消息表示HTTP/3將會使用UDP取代TCP

Reference:
https://thenewstack.io/http-3-replaces-tcp-with-udp-to-boost-network-speed-reliability/
https://en.wikipedia.org/wiki/Transmission_Control_Protocol
https://en.wikipedia.org/wiki/User_Datagram_Protocol

3. VPN may increase download speed in certain cases.
True.
正常情況下這不會發生，除非提供服務的伺服器對你的地區等有些"特殊政策"，那使用VPN才有可能會增加連線速度

4. NAT is necessary for devices with private IP to connect to devices with public IP.
True. -0.5分
如果沒有public IP，那網際網路上的其他裝置就沒辦法直接找到你，透過擁有public IP的NAT才有辦法跟網際網路溝通。

Reference: https://en.wikipedia.org/wiki/Network_address_translation

5. DHCP is necessary in configuring private IP of a device.
False.
DHCP 只是方便大家一插上網路線就可以連線和集中管理的手段，自己設定IP, gateway, DNS server也可以連線成功

6. A device can have only one IP at a time.
False.
舉個簡單的例子，NAT就一定要至少擁有一個private ip和一個public ip來達成網路位置轉換。

7. Each IP will be associated with only one device.
False.
這個問題有點神祕，他沒有特別指定時間和區網的問題，IP是具有租貸時間的，在不同區網的兩個裝置也可能擁有相同的private ip.

8. A 1Gbps network connections gaurantees a connection speed of 1Gbps for any user at any time.
False.
1Gbps network是一個總流量可以達到1Gbps的網路，那當然只要有複數的使用者在使用時，就沒辦法每個人都達到1Gbps的速度。

9. A firewall basically filters traffic according to configured rules.
True.
恩...防火牆根據寫好的規則過濾流量...對阿www
通常會有allow, drop, log等基本的規則，有時候也有病毒掃描引擎等進階功能。

10. Wifi connections over WEP and WAP have known security problems while WPA2 have no known vulnerabilities.
False.
2017年就有人發過一篇關於WPA2的漏洞，雖然該漏洞主要是實作上的問題，可以在相容原本的WPA2的狀況下修復，但WiFi聯盟還是推出了WPA3提供更安全的防護，包括
* Privacy on Public Wi-Fi Networks
* Protection Against Brute-Force Attacks
* Higher Security for Government, Defense, and Industrial Applications

Reference:
https://www.krackattacks.com/
https://www.howtogeek.com/339765/what-is-wpa3-and-when-will-i-get-it-on-my-wi-fi/

11. Traffic between devices inside the same LAN will not pass through any router or switch.
False.

switch就不用說了，如果沒有switch/hub，在區網中連接大量裝置將會變得很麻煩。而且LAN中也可以包括其他更小的區網，那其中就會有router的存在。

12. 5G wireless band (802.11ac Wi-Fi) is preferable over 2.4G band in all cases due to its faster Speed.
False.
在5GHz上實作的無線網路，雖然速度更快，但因為其物理性質，訊號的穿透力會降低，訊號的範圍會顯得小很多。

Short answer

1. The five layer internet protocol stack is essential for understanding the internet. List the five layers, briefly explain what each layer does, and give one example of service provided for each layer.
5 Process & Applications　　與網路相關的程式與其他程式溝通用的，主要和應用的範圍有關
Example: HTTP, DHCP, SSH
4 Transport　　保證資料可靠性及傳輸順序等問題
Example: TCP, UDP
3 Internet　　將資料從來源傳輸到目標，為封包選擇路由
Example: IP, ICMP
2 Link　　定義連接(物理)著的設備要怎麼溝通
"The link layer includes the protocols that define communication between local (on-link) network nodes"
Example: ARP, PPP
1 Physical　　物理
Example: 雙絞線

Reference:
https://en.wikipedia.org/wiki/Internet_protocol_suite
https://en.wikipedia.org/wiki/Link_layer
https://www.ischool.utexas.edu/~wyllys/ITIPMaterials/NotesOnInterconnection.html
https://www.itread01.com/content/1506423485.html

2. IPv4 is facing address exhaustion problem nowadays. Briefly explain what IPv4 exhaustion is, why it is happening, and illustrate 2 real-world workarounds for this problem.
新的設備太多，再加上一些永遠開著的設備不會釋放ip，IPv4所定義的ip就不夠用了
一些解決方法:

1. NAT: 透過位置轉換來讓一群設備可以只使用少量的public ip來和網際網路溝通
2. IPv6: 位址長度增長到了128位元，透過增加位置的數量來根本的解決問題

Reference:
https://en.wikipedia.org/wiki/IPv4#Address_space_exhaustion

3. DoS attacks are becoming more and more common. Please briefly explain what DoS and DDoS are.
DoS: 使用大量的請求使目標的運算或流量來不及反應的攻擊，攻擊細節也包括反射式攻擊、特製封包占用目標主機更多資源等等。
DDoS: 使用複數的主機進行DoS攻擊。

Reference: https://en.wikipedia.org/wiki/Denial-of-service_attack

4. Explain what a MAC address is and its usage.
MAC address用來指定一個唯一的網卡，通常在出廠時已經訂好，但也可以用工具修改。
ARP協定，就是用來對應更上層使用的ip address與實體的區網使用的MAC address。

Reference:
https://en.wikipedia.org/wiki/Address_Resolution_Protocol
https://en.wikipedia.org/wiki/MAC_address

Command line utility

1. Perform a DNS query for csie.ntu.edu.tw from a network outside NTU and show the delegation path from the root name servers for the query.

```
 common@wildfoot  ~  dig +trace csie.ntu.edu.tw

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> +trace csie.ntu.edu.tw
;; global options: +cmd
.                       168550  IN      NS      m.root-servers.net.
.                       168550  IN      NS      b.root-servers.net.
.                       168550  IN      NS      c.root-servers.net.
.                       168550  IN      NS      d.root-servers.net.
.                       168550  IN      NS      e.root-servers.net.
.                       168550  IN      NS      f.root-servers.net.
.                       168550  IN      NS      g.root-servers.net.
.                       168550  IN      NS      h.root-servers.net.
.                       168550  IN      NS      i.root-servers.net.
.                       168550  IN      NS      j.root-servers.net.
.                       168550  IN      NS      a.root-servers.net.
.                       168550  IN      NS      k.root-servers.net.
.                       168550  IN      NS      l.root-servers.net.
.                       168550  IN      RRSIG   NS 8 0 518400
20190305050000 20190220040000 16749 .
C3GLi1NWFamKE+UTE5SZhrFcDNcwVbAhXh5bhr6JbS31rU/+u/rUTiGk k/9L0KmqeM3oTyN6
C7SKlQ8JhUdsRw+vfDrwUpr3B8Sn+I2T4N9E1Ci6
F+sdB76DxHgcmCw3dFyo5ixol5i0euzWTo5Ras+u9mfcDLp67s9Qy9Yf
```

```
jC66sjdWlaYN+LZrAa8C4w+VDVp6CBbPl1S7oB36mq5B1cJmx1dz+hC4 AtIDI9rc1y6/XxEMHT
tMQZDJeoacJyfv6lFM6qbKF6mM3BhGYEzd3esL
mu2GJPXYVf7SLidRSqv6R1DWL4b1TwaOfVX1bd02EbX1FqSOED7Owp3v 3YllRw==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 267 ms

tw.                     172800  IN      NS      ns.twnic.net.
tw.                     172800  IN      NS      b.dns.tw.
tw.                     172800  IN      NS      c.dns.tw.
tw.                     172800  IN      NS      d.dns.tw.
tw.                     172800  IN      NS      e.dns.tw.
tw.                     172800  IN      NS      f.dns.tw.
tw.                     172800  IN      NS      g.dns.tw.
tw.                     172800  IN      NS      a.dns.tw.
tw.                     172800  IN      NS      h.dns.tw.
tw.                     172800  IN      NS      anytld.apnic.net.
tw.                     86400   IN      DS      40792 8 2
A05DB4B0DEB971031361BB621E8BB1B8D7346665A3D1B06EC1431ADB 7D015EE9
tw.                     86400   IN      RRSIG   DS 8 1 86400 20190307050000
20190222040000 16749 .
lTD7WoWovROn6vPEUOhUxYKIoFYY3BXHiEzJbRU11ugFa8PbTpSaUK2S 3/61NoJviDBjLgDtc
Fg6Isp/kcOv+BmjNgM2xLBCVwtwh8juWALyk6Bw
t4eJ6GsMeLNfKzr2rtudkXqOu2HkuSGpxZAHvnbeKjBx7VdhmuJ6S60D
6uPri8+NrHAUmiCWhLM++XFi9LyV7uAjttwiIhkGo0r1YaLDRoOoOq8I
lq0epp2Yh35NFi8Ns6/
USjl3MuhnP7pdYKOkSMBgoVNkxINON2Zz6aE7
lkECTOsewcx1anR939RdGLANGxbjZhu94Gq6l3xlYUVGjY2iwaBD3R28 uyvqEQ==
;; Received 976 bytes from 192.203.230.10#53(e.root-servers.net) in 191 ms

edu.tw.                 3600    IN      NS      d.twnic.net.tw.
edu.tw.                 3600    IN      NS      b.twnic.net.tw.
edu.tw.                 3600    IN      NS      moestar.edu.tw.
edu.tw.                 3600    IN      NS      c.twnic.net.tw.
edu.tw.                 3600    IN      NS      a.twnic.net.tw.
edu.tw.                 3600    IN      NS      moemoon.edu.tw.
edu.tw.                 300     IN      DS      40234 8 2
289D061D208C871915EB07F63FB175B21022422D5365D4E945BCE397 104A9C08
edu.tw.                 300     IN      DS      40234 8 1
5A8AB67C461F4330D146EE4E2E5A08CE279B7BEB
edu.tw.                 300     IN      RRSIG   DS 8 2 300 20190324080403
20190222080403 3984 tw.
Zo/v0CRHhWRJmKynl/kf84F9wPf8HIdGG/DvmrC1pUkNmK3rmaxI2rKB 6f+VjU7MbbuVoLFJb4
qGXFf3y+Jqv8EWV3NfAXpL0jkPbINFLIx5GEBy
```

```
FWEbHUUBOlcu2yJWYfRS/4r1qABDLkI+uvx94nQdO0c0AeNqoZRIPLfx 3F4=
;; Received 648 bytes from 203.73.24.25#53(a.dns.tw) in 139 ms

ntu.edu.tw.             300     IN      NS      dns.tp1rc.edu.tw.
ntu.edu.tw.             300     IN      NS      ntu3.ntu.edu.tw.
ntu.edu.tw.             300     IN      NS      dns.ntu.edu.tw.
F46P8I1F3S71GISH8KPLHIGFOK2BSV3H.edu.tw. 300 IN NSEC3 1 0 10 3CA5A3726C
F4KOJP7HBDRAV4SQ91CG0OJ4B4TUC9A8 NS
F46P8I1F3S71GISH8KPLHIGFOK2BSV3H.edu.tw. 300 IN RRSIG NSEC3 8 3 300
20190226023844 20190222023724 37203 edu.tw.
DWlll+ETcxO78YpCLd38V32Zmh6SKbsPGvSB73XxKnP+J9tRNY1YPXHw TckY
1vyG/ymbwLIdW4XYtChWij4EOKojq0OBcXrb1U1hvZJ8Lm1rSDnB
eJNgtmCute1a1f++0ESXBvuH/ipx6OWbLatSeAvkMokTNur5FTq/2cLv p/g=
;; Received 382 bytes from 211.73.64.22#53(a.twnic.net.tw) in 100 ms

csie.ntu.edu.tw.        86400   IN      NS      csman3.csie.ntu.edu.tw.
csie.ntu.edu.tw.        86400   IN      NS      csman.csie.ntu.edu.tw.
csie.ntu.edu.tw.        86400   IN      NS      csman2.csie.ntu.edu.tw.
;; Received 154 bytes from 140.112.2.2#53(ntu3.ntu.edu.tw) in 162 ms

csie.ntu.edu.tw.        600     IN      A       140.112.30.28
csie.ntu.edu.tw.        600     IN      NS      csman2.csie.ntu.edu.tw.
csie.ntu.edu.tw.        600     IN      NS      csman.csie.ntu.edu.tw.
csie.ntu.edu.tw.        600     IN      NS      ntuns.ntu.edu.tw.
;; Received 153 bytes from 140.112.30.14#53(csman2.csie.ntu.edu.tw) in 18
ms
```

2. Trace the routing path from nasa-hw0.csie.ntu.edu.tw to google.com and show the AS# of each hop.

```
[b07611012@nasa-hw0 ~]$ traceroute -A google.com
traceroute to google.com (172.217.160.110), 30 hops max, 60 byte packets
 1  gateway (140.112.30.254) [AS17716/AS17709]  22.302 ms  22.739 ms
26.894 ms
 2  140.112.149.121 (140.112.149.121) [AS17716/AS17709]  0.667 ms  0.605 ms
0.588 ms
 3  140.112.0.214 (140.112.0.214) [AS17716/AS17709]  0.390 ms  0.345 ms
0.287 ms
 4  140.112.0.206 (140.112.0.206) [AS17716/AS17709]  1.634 ms  1.556 ms
1.472 ms
 5  140.112.0.34 (140.112.0.34) [AS17716/AS17709]  2.279 ms  2.503 ms
2.431 ms
```

```
 6  72.14.204.212 (72.14.204.212) [AS15169]  2.089 ms  1.882 ms  1.816 ms
 7  108.170.244.97 (108.170.244.97) [AS15169]  1.997 ms 108.170.244.129
(108.170.244.129) [AS15169]  3.434 ms 108.170.244.97 (108.170.244.97)
[AS15169]  1.836 ms
 8  216.239.48.135 (216.239.48.135) [AS15169]  2.298 ms  2.271 ms  2.203 ms
 9  tsa03s06-in-f14.1e100.net (172.217.160.110) [AS15169]  2.059 ms  2.316
ms  2.248 ms
```

3. List all Internet interfaces of nasa-hw0.csie.ntu.edu.tw.

```
[b07611012@nasa-hw0 ~]$ ip -c link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:55:64:3e brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:43:3f:d5 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:f6:e6:eb brd ff:ff:ff:ff:ff:ff
6: eth0.30@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:55:64:3e brd ff:ff:ff:ff:ff:ff
```

System Administration

1. Welcome aboard! (5 points)

```
ssh b07611012@nasa-hw0.csie.ntu.edu.tw
```

```
NASA{5pi0radTM}
```

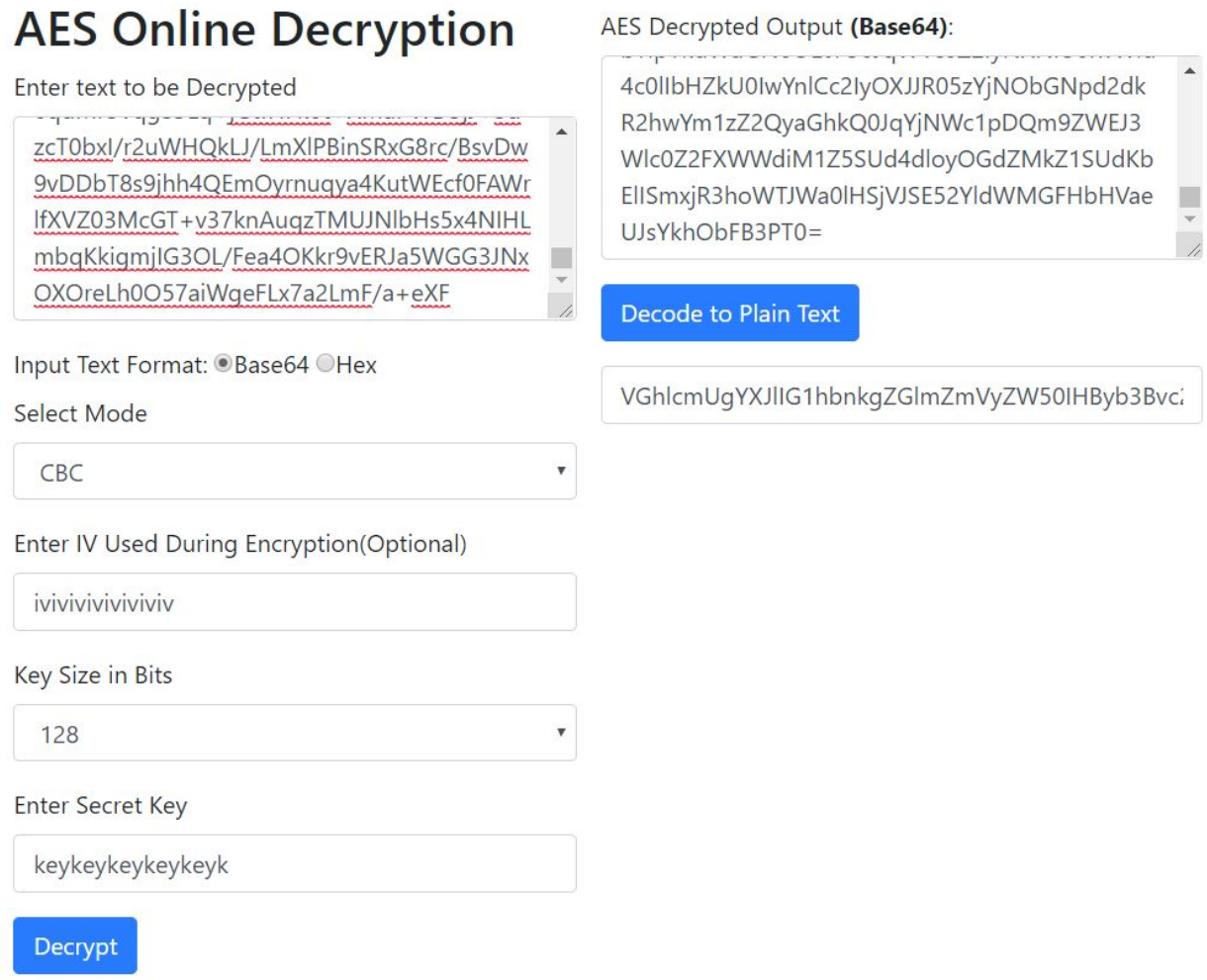
2. The Oracle (5 points)

```
[b07611012@nasa-hw0 ~]$ man Pittheus
[b07611012@nasa-hw0 The_Oracle]$ Pittheus -s > secret
```

```
[b07611012@nasa-hw0 The_Oracle]$ echo "keykeykeykeykeyk" > KEY
[b07611012@nasa-hw0 The_Oracle]$ echo "ivivivivivivivivv" > IV
```

```
[b07611012@nasa-hw0 The_Oracle]$ openssl aes-128-cbc -d -base64 -nosalt -iv
69766976697669766976697669766976 -pass
pass:6b65796b65796b65796b65796b65796b -in secret -out secr
et.dec
bad decrypt
140322358130576:error:06065064:digital envelope
routines:EVP_DecryptFinal_ex:bad decrypt:evp_enc.c:592:
```

不知道為什麼openssl的指令下不出來 [TODO]，只好用online decryption




```
[b07611012@nasa-hw0 The_Oracle]$ tail secret.dec
......IHNvbWV0aGluZyBlbHNlPw==
[b07611012@nasa-hw0 The_Oracle]$ base64 --decode ./secret.dec >
```

```
secret.dec.dec
[b07611012@nasa-hw0 The_Oracle]$ head ./secret.dec.dec
There are many different proposed resolutions surrounding the famous Ship
of Theseus problem. I'll briefly go over them up below.
```

這邊也蠻奇怪的，如果用openssl解這個base64(openssl enc -base64 -d -in ./secret.dec -out secret.dec.dec)，檔案會只解到最後面。[TODO]
最後發現flag在man裡面...

```
NASA{Y0u_w1ll_h4v3_4_50n}
```

Reference:

https://wiki.openssl.org/index.php/Enc
https://www.devglan.com/online-tools/aes-encryption-decryption

3. Know thy place (3 points)

```
[b07611012@nasa-hw0 ~]$ pwd
/home/NASA{D3sc3nd4n7_0f_G0d}/b07611012
```

4. Sandals and Sword (5 points)

```
[b07611012@nasa-hw0 Theseus's_Room]$ chmod -R 755 ./*
[b07611012@nasa-hw0 Theseus's_Room]$ mv big_rock/sword* .
[b07611012@nasa-hw0 Theseus's_Room]$ mv big_rock/sandals* .
[b07611012@nasa-hw0 Theseus's_Room]$ rm -rf ./big_rock/
[b07611012@nasa-hw0 Theseus's_Room]$ ./Aegeus
NASA{1_4m_y0ur_f4th3r}
```

5. Hargghh MATE! (3 points)

```
[b07611012@nasa-hw0 master_room]$ alias ll="ls -la"
[b07611012@nasa-hw0 master_room]$ ll
[b07611012@nasa-hw0 master_room]$ cat .captain
NASA{0H_my_d34r_fr1end}
```

6. Sinking ship (8 points)

```
[b07611012@nasa-hw0 ship]$ vim SINKING_SHIP
:1,$s/[Bb][Uu][Gg][Ss]//gc
NASA{Y0U_G07_R1D_0f_7h3_6Ug5}
```

7. Handy man (5 points)

```
[b07611012@nasa-hw0 master_room]$ ./THE_OLD_MAN
The KEY which can open the tool-box is the unique one ...
[b07611012@nasa-hw0 master_room]$ sort KEY | uniq -c
      1 KEY{>>UcMI}
[b07611012@nasa-hw0 master_room]$ unzip tool_box.zip
[b07611012@nasa-hw0 master_room]$ cat tool_box/tool.txt
NASA{3mp7y_70Olb0x_:(}
```

8. King of the Labyrinth (8 points)

```
[b07611012@nasa-hw0 ship]$ ./beast
No body can stop me hahahahahaha !!!
[b07611012@nasa-hw0 ship]$ htop
Pass signal 15 SIGTERM
NASA{7h3seus_4llm1gh7y}
```

9. Voyage back (8 points)

```
[b07611012@nasa-hw0 ship]$ find / -name "white_mast" 2> /dev/null
/opt/white_mast
[b07611012@nasa-hw0 ship]$ cat /opt/white_mast
NASA{t00_l4t3}
```

10. Ship of Theseus (12 points)

總之先跑看看

```
[b07611012@nasa-hw0 ship]$ python3 pong_game.py
Give me your name:
WildfootW
[+] Opening connection to 127.0.0.1 on port 10101: Done
[*] Closed connection to 127.0.0.1 port 10101
```

嘛...一瞬間閃過去很眼熟的東西，看來出題者平常有在打pwnXD

```
[b07611012@nasa-hw0 ship]$ nc localhost 10101
How did you see me?
Did you see the clue left in man?
Let me tell you something else,
Theseus is special
also, finding logo2 may help you
give me your mode:
```

Mode不知道是什麼

```
mode = 'Theseus'
r.sendlineafter('mode:\n',mode)
data = r.recv()[:-1]
```

Theseus.... 沒有想法
只好看看logo2

```
[b07611012@nasa-hw0 ship]$ find / -name logo2 2> /dev/null
/mnt/nasa/logo2
-rw-------. 1 root root 441 Jan 22 00:59 logo2
-rw-------. 1 root root 262 Jan 22 00:59 Meow
-rw-------. 1 root root 349 Jan 22 00:54 Zeus
```

打不開呢...，所以是要提權? 難道要exploit?
看一下 10101 port是誰在聽

```
root      5386  0.0  0.0  44064     4 pts/5    S+   Feb17   0:00 ncat -vc
python2 pong.py -kl 10101 -o nclog
```

是root權限呢，但卻是python，這樣也沒辦法overflow之類的...，難道是kernal提權
看看kernal版本

```
[b07611012@nasa-hw0 nasa]$ uname -r
3.10.0-862.el7.x86_64
```

雖然覺得應該可以，稍微試著幾個poc都沒有結果。
想說bonus如果要這樣玩好像有點太超過了XD
嘛...那現在是黑箱exploit、目標是python、pong.py的功能感覺是讀一個檔案再吐回來給pong_game.py使用
難道Theseus是檔名嗎?

```
give me your mode:
../../../../../mnt/nasa/logo2
                 _________
                /|       /
    _          / / NASA /
   / /_____   / /______/
```

```
  /Θ __  _/  / /
  \_/ / /   / /                              ______ /|
     / /---/ /--------------------------//      |/
    / /   / /___    //_) (_   //_) || |  \__    /|
   (_/   /  --/ /   \\_   _)  \\_  \\_/     \   |/
    \___/Θ/__/η/__/σ/__/ε/__/ύ/__/ς/_______// _/
 ~~~~~~/Θ/~~/η/~~/σ/~~/ε/~~/ύ/~~/ς/~~~~~~~~~~~~~~~~~
```

居然猜對一半，後來看檔案發現Theseus是關鍵字，還以為是相對路徑的檔名呢

```
give me your mode:
/mnt/nasa/Zeus
            _
     ___   /*\   _____        ___
   / __/   \_/  \_  _  \     /   |/|
  |__       |▉|   /_/+/ |    / /| / |
     \  __  |▉|  / _ \  /   / /+| | |
 __= / / _\|▉| /| O/| \  / _ __ | | |
/___/ / /_/|▉|//\___/\ \/ / /  _| |
     /_/   |▉|        \ \   | +/  \
           |▉|             \__ /\ \

  \ NASA{1000_po1nt_s0_e45y_huh} /
```

Reference:

https://www.exploit-db.com/exploits/45516
https://www.exploit-db.com/exploits/42887