Network Administration

DHCP

1. DHCP can instruct a client to use a specific gateway. Therefore, it comes to Eve that she can set up herownDHCPserverandredirectallnetworkdatatoherside,andthenshecaneavesdropeverything. As a network administrator, what should you do to prevent this from happening? (10%)

- 我們可以使用 DHCP Snooping 這個技術來避免使用者架設惡意的 DHCP Server，DHCP Snooping 的原理是在 Switch(Layer2) 上設定只允許特定部分的 Switch Port 放行 DHCP Server 的回應封包，其他的就不允許通過，這樣就可以避免別人隨便的架設 DHCP Server。

DNS

1. You can set up your own authoritative DNS server for csie.ntu.edu.tw and modify it whatever you like, but nobody except you will query it. Why? (5%)

- 因為你自己架的 authoritative DNS server 不會被上層的 DNS server 加入到他的管理列表內(也就是上層的 DNS server 不知道你自己架的 DNS server)，因此別人查詢的時候不會查到你的機器上。

2. A special domain name is reserved to facilitate reverse IP lookup (i.e. IP 反解) for IPv4 addresses. Therefore,"dig -x 140.112.30.21" equals to "dig -t PTR 21.30.112.140.A_SPECIAL_DOMAIN_NAME". What is that domain? (5%)
   Also, in the above command, why is 140.112.30.21 reverted to 21.30.112.140? (5%)

- 那個特殊的 domain name 是 in-addr.arpa，你可以輸入 dig -t PTR 21.30.112.140.in-addr.arpa 來反查 21.30.112.140
- 而他要把 140.112.30.21 翻轉成 to 21.30.112.140 的原因主要是因為 ip 的 mask 是從前面往後去 mask 的，但是在 DNS上的話則是後面的東西會比較優先，因此把他反過來之後會比較容易去分層查詢。

3. How (Where) can you find the information of a domain, such as the domain registrant's name, the administrator's email address, and so on? (2%) Use your aforementioned method to find out the registrant contact's email address for the domain icann.org. (Reminder: zone file's SOA record is NOT enough for this purpose.) (3%)

- 可以使用 whois 這個服務(或是指令)就能查到一個 domain 的註冊者姓名、管理員的信箱...等等
- Admin Email: domain-admin@icann.org

4. What is "DNS propagation time"? (5%) For the following example zone file, assume this zone belongs to you (you operate an authoritative DNS server of this zone), and assume TTL is honored by every server on the Internet. If you change 192.168.1.1 to 192.168.1.2, how long does it take for this modified record to "propagate"? Explain your answer. (5%)

```
@ 86400 IN SOA ns.example.com. admin.example.com. (
    2017041100 ; serial
    21600 ; refresh after 6 hours
```

```
    1800 ; retry after 30 minutes
    86400 ; expire after 1 day
    600 ); minimum TTL of 10 minutes
@ 10800 IN NS ns.example.com.
ns 7200 IN A 192.168.1.254
@ 3600 IN A 192.168.1.1
```

- DNS propagation time 就是指一個 DNS 紀錄傳播到整個網路所花的時間(會受許多因素影響)
- 10 分鐘，因為一個紀錄最多被記錄 10 分鐘後就失效了，接下來再查詢的話就會是更改過的值。

5. For DNS, what is open resolver? (5%) What problem may it pose? (5%)

- open resolver 就是指其 DNS Server 提供其管理網域範圍外的用戶，開放使用 DNS 遞迴查詢權限的服務。
- 會因為其能提供管理範圍外的用戶遞迴查詢資料，造成 DNS 放大攻擊(攻擊者僅需少量頻寬就是造成大量頻寬的攻擊)，並且攻擊可能還有匿名性。