Homework #4 Solution

Contact TAs: vegetable@csie.ntu.edu.tw

Network Administration

1 DHCP

1.1 (10%)

Take Windows for example, you can use the following commands.

```
ipconfig /release
ipconfig /renew
```

1.2 (15%)

DHCP server may reserve IP addresses for each MAC address. As long as you use the same MAC address, you will get the same IP from the DHCP server.

2 DNS

2.1 (15%)

1. A single server lacks redundancy. If the server is down, then nobody can access DNS service.
2. A single server may cause high latency for cilents that are far from the server.
3. Holding all the DNS records on a single server is hard to maintain.

2.2 (15%)

```
00000000  00 00 85 80 00 01 00 01  00 03 00 03 03 77 77 77  |.............www|
00000010  04 63 73 69 65 03 6e 74  75 03 65 64 75 02 74 77  |.csie.ntu.edu.tw|
00000020  00 00 01 00 01 c0 0c 00  01 00 01 00 00 02 58 00  |..............X.|
00000030  04 8c 70 1e 1c c0 10 00  02 00 01 00 01 51 80 00  |..p..........Q..|
00000040  08 05 63 73 6d 61 6e c0  10 c0 10 00 02 00 01 00  |..csman.........|
00000050  01 51 80 00 08 05 6e 74  75 6e 73 c0 15 c0 10 00  |.Q....ntuns.....|
00000060  02 00 01 00 01 51 80 00  09 06 63 73 6d 61 6e 32  |.....Q....csman2|
00000070  c0 10 c0 41 00 01 00 01  00 00 02 58 00 04 8c 70  |...A.......X...p|
00000080  1e 15 c0 55 00 01 00 01  00 00 03 88 00 04 8c 70  |...U...........p|
00000090  fe 06 c0 69 00 01 00 01  00 00 02 58 00 04 8c 70  |...i.......X...p|
000000a0  1e 0c                                            |..|
000000a2
```

2.3 (15%)

Entire domain names or the end of a domain name is replaced with a pointer to a prior occurrence of the same name. Pointers are two bytes long, with highest two bits set to 1, and following bits is an offset from the start of the message.

For example, "csman" follows by binary value `1100000000010000`. It is a pointer to offset `10000`, which is `16` in decimal format. We can find out that the pointer points to `.csie.ntu.edu.tw`, and the entire domain name is `csman.csie.ntu.edu.tw`.
With IPv4 standard, only packets with length equal or less than 576 bytes are guaranteed to be reassembled if fragmented in transit. Also, fragmented packets have higher chance to be dropped while transmitting using UDP. Thus, larger responses may be truncated or transmitted using TCP, which requires three way handshake and is slower than UDP. Therefore, we can conclude that it is better to reduce length of responses and keep them transmitted using UDP.

2.4 (15%)

DNS Amplification Attack. People may send DNS requests with spoofed IP and use the responses which have much larger length to attack other hosts. Restricting query clients to NTU network reduce the possibility the DNS server being abused.

2.5 (15%)

Read DNS server setting from the file `/etc/resolv.conf`, cut out the IP address part, and save it in a variable.
Replace `140.112.30.21 53` in `cat dig.tmp - | ncat -u -i 1 140.112.30.21 53 2>/dev/null | hexdump -C` with the variable.
There is script on class website for reference.

2.6 (Bonus 10%)

According to RFC1035, MX type has type value 15, which is `0F` in hex format. If the 2nd argument pass to the script is `MX` then set the value in line 21 of dig.sh to `0x0F`, else set it to `0x01`(type A).
There is script on class website for reference.

System Administration

1

```
$ ifconfig eth0 192.168.217.1 netmask 255.255.255.0
$ route add default gw 192.168.217.254 eth0
```

沒有設定 gateway 扣一半，其它錯誤全題不給分。其它錯誤包括但不限於：ip 打錯、interface 打錯

2

```
$ tracepath www.google.com
```

題目要求 from linux1，但只要給出能在 linux1 上執行的指令會給對 (linux1 上沒有 traceroute)

3

```
$ printf "HEAD / HTTP/1.0\n\n" | nc www.csie.ntu.edu.tw 80
```

(某些平台會是 ncat 而非 nc，linux1 上即是 ncat)
或

```
$ curl -I www.csie.ntu.edu.tw
```

得到的結果包含 html 內文的話不給分

4

```
$ dig -t MX csie.ntu.edu.tw
```

非使用 dig 不給分

5

`$ lsof -i :80` (需要 root 權限)
能找出 pid 或 process name 即可。只找出 tcp 或 udp 其一扣一半，其餘不給分。