NASA 2016 HW4 NA Part

B03902086 李鈺昇

1. DHCP

References:

http://helpdeskgeek.com/networking/release-and-renew-an-ip-address/

https://community.spiceworks.com/topic/227268-how-to-get-differenct-ip-address-from-dhcp

1.1

ipconfig /release && ipconfig /renew

1.2

That may be due to DHCP reservation.

2. DNS

References:

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

http://www-inf.int-evry.fr/~hennequi/CoursDNS/NOTES-COURS_eng/syst.html

https://www.cs.uic.edu/pub/CS450fall10/WebHome/lecture7.pdf

https://github.com/rancher/rancher/issues/2928

2.1

The loading would be too heavy and thus leading to slow speed.

More faults are likely to happen.

Requires a large database.

2.2

The response:

```
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 6e 74 75 6e 73 c0  15 c0 10 00 02 00 01 00  |..ntuns.........|
00000050  01 51 80 00 09 06 63 73  6d 61 6e 32 c0 10 c0 10  |.Q....csman2....|
00000060  00 02 00 01 00 01 51 80  00 08 05 63 73 6d 61 6e  |......Q....csman|
00000070  c0 10 c0 6a 00 01 00 01  00 00 02 58 00 04 8c 70  |...j.......X...p|
00000080  1e 15 c0 41 00 01 00 01  00 00 eb e9 00 04 8c 70  |...A...........p|
00000090  fe 06 c0 55 00 01 00 01  00 00 02 58 00 04 8c 70  |...U.......X...p|
000000a0  1e 0c                                            |..|
000000a2
```

Since the last 8 hex characters are “8c 70 1e 0c”, translating to decimals we get the IP 140.112.30.12. (The last “.” is the period.)

2.3

As highlighted in red in the responsea above, the hex c010 points to the offset of “.csie.ntu.edu.tw,” and c015 points to the offset of “.ntu.edu.tw.” So we got the following:

ntuns.ntu.edu.tw

csman2.csie.ntu.edu.tw

csman.csie.ntu.edu.tw

Without such compression, the 512-byte packet size limit of UDP may be exceeded.

2.4

DNS spoofing.