Homework #0

Due Time: 2021/02/24 (Wed.) 23:59
Contact TAs: `vegetable@csie.ntu.edu.tw`

Instructions and Announcements

- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**
- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.
- Announcement will be updated on https://hackmd.io/@jimpei8989/BJUzDlvg_. Please visit the page at least once a day.

Submission

- Put all answers **in one single PDF file**, in the same order as the problem sheet. Do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Submit through this google form: https://forms.gle/cembz4kNjm3YokXe6.
- If you need to update your submission, please create another submission. We'll use your latest submission as your final submission.

Grading

- NA accounts for 100 points while SA accounts for 112 points. The final score is the average between them.
- It's possible you don't get full credits even if you have the correct answer. You should show how you get the answers step by step and list the references.
- There's a *10% early-bird bonus* points in HW0. It decays linearly since *2021/02/04 00:00*.
- In this semester, we'll introduce a *tidiness score*. As a trial period, you only need to follow the three criteria to get all the credits.
  - Please list your answers in the same order as the problem set. You should type your answers and use a proper typesetting.
  - Please use `monospace fonts` when writing commands and codes in your answer sheet.
  - Screenshots of your terminal outputs are allowed. Please crop the screenshots and zoom them to a proper size that we can easily read your terminal outputs.

  As a sweet note, we recommend you to try out *hackmd*, *typora* and other markdown applications if you don't know how to make a proper typesetting. They should be pretty easy to the beginners.
- You can get at most $\frac{100+112}{2} + 10 + 3 = 119$ points. However, we cannot guarantee the minimum score to take the class.

Network Administration

1. True/False (40 points)

In each of the following question, please specify if the statement is true or false and **briefly explain why**. Please avoid just repeating the question. Each question is worth 4 points.

1. 4G and 5G (4Th and 5Th Generation of Mobile Networks) are often heard in the news now, which refer to the speed of network connection.
2. Following the previous question, the "5G" mentioned in question 1 is the same as the "5G" of csie-5G, which is a Wi-Fi network in CSIE department.
3. A NAT server may have different NAT entries for processes run on different ports of the same end device.
4. Each IP will be associated with only one device, and each device only has one **IP address**.
5. VPN can fake source IP in a packet by directly rewriting the bits of source IP in the packet.
6. In an **intranet**, all packets must transmit through the gateway.
7. When you send a request to DNS server 8.8.8.8, it will respond that there is no corresponding domain if the server doesn't store the answer of the request.
8. Without DHCP, DNS and NAT, we can't connect to a server in the Internet whose IP is known.
9. If we send packets through HTTP protocol, anyone who capture the packets can easily get the information, such as source IP, target IP, and content.
10. If an end device get an IP address from a DHCP server, all packets sent to that IP address will pass through the DHCP server first.

2. Short answer (35 points)

Answer the questions. Each question is worth 7 points.

1. Briefly explain the following terms and their usages.
   (a) MAC address
   (b) Router
   (c) Switch
2. Briefly explain what is subnet mask and pick up **valid** IP addresses which are in the same subnet with 192.168.0.1/23.
   (a) 192.167.0.1
   (b) 192.168.0.0
   (c) 192.168.1.0
   (d) 193.168.0.1
3. Network attacks are becoming more and more common. Please briefly explain the networks attacks below, how they work and what we can do to avoid them?

(a) DoS

(b) DDoS

(c) Man in the middle attacks

4. The **five-layer internet protocol stack** is essential for understanding the internet. List the five layers (2%), briefly explain what each layer does (3%), and give one example of service provided for each layer (2%).

5. Briefly explain TCP and UDP. (3%) What are their advantages and disadvantages relative to each other? (2%) Give one example situation/application for both TCP and UDP when we will choose one rather than the other. (2%)

3. Command Line Utilities (25 points)

For the following questions, please **provide the commands you used** along with the result.

1. Find out the IP addresses corresponding to the following URLs. Each address is worth 3 points.

   (a) www.ntu.edu.tw

   (b) csie.ntu.edu.tw

   (c) linux1.csie.ntu.edu.tw

   (d) ceiba.ntu.edu.tw

2. **NTU VPN**

   The following questions should be done under the NTU SSL VPN environment.

   Usage of NTU SSL VPN: `https://ccnet.ntu.edu.tw/vpn/`
   For Windows: `https://ccnet.ntu.edu.tw/vpn/for-windows.html`
   For Linux: `https://ccnet.ntu.edu.tw/vpn/for-ubuntu.html`
   For Mac OS: `https://ccnet.ntu.edu.tw/vpn/for-macosx.html`

   Please use the VPN client to get an IP from NTU VPN server and then answer the following questions.

   (a) What IP did you get from the VPN server? (3%)

   (b) What is the DNS server IP you asked when you query `csie.ntu.edu.tw`? In addition, show the delegation path from the root name servers for the query. (3%)

   (c) Now disconnect from the VPN, what is the DNS server IP you asked now when you query `csie.ntu.edu.tw`? Explain the difference. (3%)

   (d) Following question c, show the routing path from your device to the DNS server you asked without connecting to the VPN. (4%)

System Administration

1. Capture The Flag (100 points + 12 bonus points)

Before you start this part, there are something you should notice.

- For each problem, you need to provide your approach to retrieve the flag. Otherwise, we might not give you the credits.
- Unless explicitly instructed, avoid using nasty hacks (for example, parse the executable file to get the flag). You may get no or partial credit if you do so.
- You may manipulate the VM (for example, boot the VM into rescue mode and get root permission to look around) to inspire youself to get the flag. However, **your final method must work in an unmodified VM**, or you will get no points for the problem.
  - Exception: You can modify the VM port forwarding settings so that you can SSH into the machine (if you don't like that dirty black window of VirtualBox). The SSH server will start running once the VM boots. For further details about VM port forwarding, please refer to https://www.kjnotes.com/devtools/77.

About the VM

- Download the image from google drive: https://drive.google.com/file/d/17ZV6xHLb5dlsBiy5HPwRqwGYkjILOrpQ/view?usp=sharing
- SHA256 checksum : `2db53dee595020b93e870f1a9b7739f15728b4d5251eea2d2492903c1f915f93`
- Account:
  - Username : `antivirus`
  - Password : `nasa2021`
- We recommend you to to open the `.ova` file with **VirtualBox**.
- You may want to take a **snapshot** of the VM (google it if you don't know how to do it) before working on the problems, so that you can easily recover (without re-downloading the whole image) if you messed it up.
- Please change `"Setting of the VM > Network > Adapter 1 > Attached to"` of the VM to **NAT** as the following figure does. As a NASA student candidate, it's encouraged that you figure out their meanings on your own :)

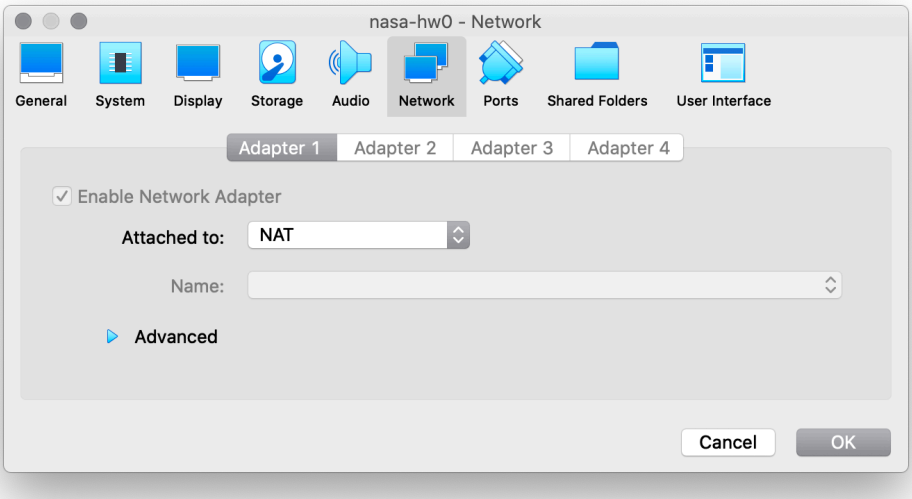

Figure 1: An example of NAT network setting

Good Luck and Have Fun

There are **15** problems in total. Anyway, good luck and have fun!

In 3019, there is a computer virus called **"covid-19"**. The virus infected over 96 million computers and killed about 2 million of them. As an antivirus, you have got a few missions from NASA. Though it is a difficult trip, we believe that you can complete all missions and defeat the virus.

During the missions, you need to collect flags in a virus world. That is, you have to find strings like `NASA{xxx}` or fill the content of flags. Notice that not all flags are correct and there are no spaces or square brackets in flags. The world will shutdown in 30 minutes once you log in. How much you complete will decide your priority to take the course. Please write down the flags (e.g. `NASA{I_am_a_sample}`) and include all the Linux commands you used step by step in detail.

For the problems marked with a asterisk (*), you can earn 2 bonus points by providing another solution. The new solution must be different enough from the original one. For example, you cannot change the editor from `vi` to `vim` and claim for the bonus points. This part will be judged by the TA, just do your best :)

1. *** Welcome to the virus world (5 points)**

   Suddenly, you were delivered into a world. You may be familiar with the world. We called the phenomenon "déjà vu". As Cobb in Inception said, "You never remember the beginning of your dreams, do you?" However, you forgot not only the beginning of the world, but also your name! Can you find who you are with a Linux command?

   The content of this flag is the command. (`NASA{[command]}`). For example, if you find the flag with the command `"ls -al"`, write the flag as `NASA{ls_-al}`.

2. **Whistleblower (5 points)**

   Once you found the name, all memories flashed back and reminded you the mission about the origin of the virus. At the beginning of the disease, there were some whistleblowers in a website,

`ptt.cc`. In this mission, you have to connect to the remote server with secure shell. (Due to Chinese encoding, it is okay if the terminal cannot show Chinese word)

The content of this flag is the whole command, including some parameters. (`NASA{[command]}`) Please replace spaces with underscores.

3. **A man (5 points)**

   After collecting information, you noticed a repeated word `man`. As Harry Hart in Kingsman said, "Manners maketh man." What is `man`? How could you find the manual page of the word?

   The content of this flag is the whole command, including some parameters. (`NASA{[command]}`) Please replace spaces with underscores.

4. **Toilet (5 points)**

   During reading the manual page, you had some snack from De-Tian. After 5 minutes, your stomach hurt and need to find yourself a toilet! It took you some strength to get into the toilet. You may find a piece of article in the toilet. There may be a shattered flag about the line counts and word counts of the article. Could you find the lost numbers?

   This flag contains two numbers, which are separated by an underscore. (`NASA{[line counts]_[word counts]}`)

5. *** Goose the Flerken (5 points)**

   Back from the toilet, you found a Flerken called Goose in `carton`. Wait a minute, the cattish Flerken sliced the content of a flag into pieces! Goose slipped away and left pieces of flag in the carton. Could you put the pieces together and catch the flag?

   This flag contains two word, which are separated by an underscore. (`NASA{[word]_[word]}`)

6. **Inside box, inside vote (5 points)**

   After Goose's left, you heard the footsteps of the virus! The place is not safe anymore. You have to find some place to hide. It is safe inside `box`, which is inside `vote`, which is inside `CSIE`, which is inside `TW`. However, there is only `hide.sh` in `TW`. Could you make yourself a safe place?

   You could test if the place is safe with `hide` in `TW`. Remember to move `hide` with you whenever you enter another directories and make sure **no one except you** could enter the box. Use command `./hide` in the safe place to get the **proper** flag.

7. *** Grep the virus! (5 points)**

   It is told that the virus is very sly, which may hide inside the content of a flag. You took a look at `flags` and find a string `_virus_` in the content of all flags. However, the only proper flag contains the string `_virus_` between alphabets, which means the proper flag looks like "`NASA{[alphabets]_virus_[alphabets]}`" . Could you find the flag?

8. *** nasa or NASA (5 points)**

   As a virus, covid-19 also surveyed NASA. You could find the report of NASA in `nanasasa`. However, the virus always misspell `NASA` to `nasa`. Could you replace every `nasa` with `NASA` in `nasa_report`?

   Use the command `./test [file name]` in `nanasasa` after completing the mission to get the **proper** flag.

9. **Maze Runner (10 points)**

   After catch the flag of NASA report, the virus fled to a maze! It is said that the virus left a flag in the maze. Your next mission is to find the flag in a maze. Could you enter the `maze` and find the `flag`?

10. **Don't just see, observe! (10 points)**

    Congratulations! You have done well to come so far. Here we found an `url` in `image`. As Sherlock Holmes said, "Don't just see, observe!" We believe that you can find the flag from it. Can you download the image and find the flag?

11. *** I'm inevitable (10 points)**

    It seemed that the virus also kept some pets! You entered `puipui` and found a `guineaPig`. It was so cute! You started the `guineaPig` and found the `guineaPig` unstoppable. Could you stop the `guineaPig`?

    The content of this flag is the whole command, including some parameters but not the pid. (`NASA{[command]}`) Please replace spaces with underscores.

12. **Dormammu, I've come to bargin (10 points)**

    As you noticed, there were something **strange** in this world. The virus mock you every minute! Could you find the way to stop the mocking words?

    This mission has no flag.

13. *** Sand glass (10 points)**

    As you noticed, there were another **strange** in this world. How could a virus stay in a world that can only exist 30 minutes? Could you find the way to stop the countdown?

    This mission has no flag.

14. **Permission Denied (5 points)**

    During those missions, you may notice the first 10 bits of rows while using `ls -l`. For example,

    ```
    -rwxr-xr-x 1 antivirus antivirus 1000000 Feb 3 23:59 nasa_report
    ```

    What is the meaning of `r`, `w`, `x` and what could you do with them?

    This mission has no flag.

15. **I'm Groot (5 points)**

    Do you know how to get into the root of the file system? You could find several subdirectories in the root. In order to prevent getting lost, you memorized the names of the subdirectories. However, others may get lost if they don't know what the directories contain! Could you write down what kind of files that the directories below may contain?

    - `/bin`
    - `/dev`
    - `/etc`
    - `/tmp`
    - `/usr`

    This mission has no flag.