Homework #0

Due Time: 2018/2/24 (Sat.) 23:59
Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Compress all your files into a file named **HW0_[studentID].zip** (e.g. `HW0_bxx902xxx.zip`), which contains two folders named **[studentID]_NA** and **[studentID]_SA** respectively.
- **Folder [studentID]_NA** should contain a pdf file of all your answers in *Network Administration Part*.
- **Folder [studentID]_SA** should contain your `hero.sh` to do the tasks in *System Administration Part*.
- Submit your zip file to Dropbox.

Instructions and Announcements

- 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.
- **NO LATE SUBMISSION IS ALLOWED.**

Network Administration

True/False

In each of the following question, please specify if the statement is **true or false** and **briefly explain why**. (2 points per question)

1. One public IP address corresponds to exactly one device.
2. Theoretically, a single NAT server can host an arbitrary number of NAT entries if equipped with unlimited memory.
3. A device can only have one IP address at the same time.
4. The DHCP server will always assign the same IP address to the same device.
5. All the traffics from the end devices will definitely pass the gateway.
6. In general, an end device judges whether itself is the recipient of a packet by the value in the MAC address field.
7. If the DNS server that we are directly querying has no record of our requested URL, then this query will fail immediately.
8. Some variants of VPN do not encrypt the traffic.
9. WEP, WPA, WPA2 are security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. These protocals have no vulnerabilities and we can choose which to use according to our needs and not worry about any security issues.
10. TCP reset attack can be used to perform DoS attack.

Select All that Apply

For this section, you may provide the reason why you think an option is right or wrong, and we may give you points if your answer is different from ours but the explanation makes sense. (0.4 point per option)

1. Which of the following protocols are **not** in the Network Layer?
   (a) IPv6
   (b) FTP
   (c) IPsec
   (d) ICMP
   (e) IEEE 802.11ac
2. Which **valid** IPs are in the same subnet with 12.34.56.78/20?
   (a) 12.34.56.123
   (b) 12.34.63.78
   (c) 12.34.48.0
   (d) 12.35.56.78

(e) 13.34.56.78

3. Which of the following are valid IPv4 private subnet?

   (a) 10.4.8.0/21
   (b) 192.160.32.0/25
   (c) 172.64.0.0/16
   (d) 192.168.16.0/20
   (e) 172.20.15.0/24

Short Answer Questions

For this section, each question is worth 3 points.

1. What are the differences between 2.4G and 5G wireless band. List at least 3 differences.
2. Please list 3 functionalities that VPN can provide?
3. When you open a browser and enter an URL in the address bar, what happens until the webpage is displayed? (What application/transport layer protocals are used and what services do they provide?)
4. Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). Commom key lengths are 128, 192, and 256 bits. Now let's calculate AES-128 (most commonly used) security against brute force attack. Current world fastest supercomputer (as per wikipedia) has a peek speed of 93.01 Petaflops (Flops = Floating point operations per second). Suppose you have a suuuuuupercomputer with the computing power of 100000 Petaflops, which is probably more than the world's total computing power. The number of Flops required per combination check is 1000 (very optimistic but just assume for now). Then how many years will it take for you to brute force an AES-128 key?

Basic Command Line Utilities

For the following questions, please provide the commands you used along with the result. (3 points per question)

1. Find out the IP addresses corresponding to the following urls.

   (a) www.ntu.edu.tw
   (b) csie.ntu.edu.tw
   (c) linux1.csie.ntu.edu.tw

2. Show the routing path from linux1 workstation to google.com.
3. What is the gateway to the following destinations on linux1 workstation?

   (a) 8.8.8.8
   (b) 10.217.44.3
   (c) linux2.csie.ntu.edu.tw

4. List all Internet interfaces and their corresponding IPv4 addresses on linux1 workstation.

System Administration

Let's catch the flag!

You will be frequently using virtual machines and Linux in the NASA course and various future CSIE courses. Knowing how to navigate and control the system is essential to your success in this course. Why not get your hands dirty on some basic commands in this lovely winter vocation?

The purpose of this homework is to familiarize you with the usage of basic UNIX commands. You're expected to understand how to use "`cut`", "`echo`", "`sed`", etc and the concept of "shell piping", "shell redirecting", etc. The following tutorials can equip you with enough knowledge to solve the challenges presented in this homework:

- https://www.tjhsst.edu/đhyatt/superap/unixcmd.html
- https://ryanstutorials.net/linuxtutorial/piping.php

An ova file (username: `nasa2018`, password: `nasa2018`) is provided. Please import it into VirtualBox and boot it.

We will be entering a fantasy world, which looks like this:

```
challenge
├── nasa_land
│   ├── cave
│   │   └── ...
│   ├── village
│   │   └── ...
│   ├── shop
│   │   └── ...
│   ├── castle
│   │   └── ...
│   └── worm_hole
├── sanpei
└── hero.sh
```

`sanpei` is an old warrior who had already finished all the missions in this world. He knows that one day he will be gone, like tears in rain, and wants to make sure that there will still be some talent young heroes who can solve these tasks.

The missions are as followed: (you will get different secret codes after finishing each of them. And you can get 12.5 points for each completed mission.)

1. Get the secret inside the chest in Goblin's cave
2. Solve the quest from the wisdom in the village
3. Fix the problem of the merchant in the shop
4. Defeat the boss in the castle

`sanpei` will tell you the secret code but not the methods. Please complete the shell script `hero.sh` such that its output is exactly the same as that of `sanpei`'s. How much you complete will decide your priority to take the course. You only need to submit `hero.sh`.

Please don't just echo the answer in `hero.sh`. Make sure `hero.sh` will still output the correct answers after you jump into `worm_hole`! `worm_hole` will disturb some of the factors in these missions.

Oh, and don't invoke `sanpei` in `hero.sh`. Although we will test your script in the same environment (run `sh hero.sh` in the same location), he might not be there when we test your script :)

Hints:

1. If you set your VM's network to NAT, you can try port forwarding and use `ssh, sshfs, scp` to have better experience.
2. Besides googling, `man` is always your good friend.
3. If you really don't know how to start, bash history might give you some idea.
4. You can use `diff` to compare your answers with `sanpei`'s.