Homework #3

Due Time: 2017/4/16 (Sun.) 22:00
Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Compress all your files into a file named **HW3_[studentID].zip** (e.g. `HW3_bxx902xxx.zip`), which contains one folder named **[studentID]_NA1**.
- **Folder [studentID]_NA1** should contain a pdf file named **na1.pdf** of your answers to problem 1 and 3 in *Network Administration 1 Part* and a pka file named **[studentID].pka** for problem 2.
- Submit your zip file to ceiba.
- You should demo your *Network Administration 2 Part* to a TA. Please fill in the demo timetable.
- You will get 5 points if you follow the assignment format specified above. Failure to follow any of the above requirements will result in deductions from your assignment mark.

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.
- Problems below will be related to the materials taught in the class and may be far beyond that. Try to search for additional information on the Internet and give a reasonable answer.
- 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 1

1. (10%)

Suppose that you are the manager of one Cisco switch whose network consists of a core switch and a number of edge switches, forming a tree topology. You received a report from the server monitor that there were some malicious packets from IP 140.112.31.254, and you are responsible for finding the source of this issue. Describe the necessary steps to trace the location of the end user (the port they used on the edge switch) and the commands used during the process. Assume the gateway of 140.112.31.254 is 140.112.31.252, which is the core switch, and please propose the solution with as less effort as possible. (E.g. looking up the MAC address tables on all edge switches on the network at the same time is not a feasible solution.)

2. (30%)

Download "hw3.pka" from the course website and complete the following tasks on Switch0: (Points for each question will show up in the pka result.)

- set the hostname of the switch to "CiscoLab"
- disable domain name lookup in CLI
- set enable password to "CISCO" (should be encryted)
- create VLANs 10, 20, 99
- assign PC0 and PC1 to VLAN 10 and assign PC2 and PC3 to VLAN 20 so that PCs in different VLANs cannot ping each other
- assign Admin to VLAN 99 and Admin should be able to access the switch by telneting 192.168.99.1
- set the telnet login password to "cisco" on VTY 0 to 4

Use "Check results" on the "PT Activity" window to check your points, and save your work to **[studentID]_NA1/[studentID].pka**.

3. (10%)

Please refer to the Problem 2.

(a) Is PC2 able to ping PC3? If not, what can we do? (2%)

(b) Briefly describe the method to build the connection between different VLANs so that they can ping each other. (4%)

(c) You have learned the encryption feature of Cisco password, but the encryption is actually vulnerable to attacks since it's merely a kind of encoding instead of a one-way hash function. Decrypt the password "022B054222030E35694F1D46" that the applications should apply the function with the keyword "secret", making use of hash functions such as MD5. (4%)

Network Administration 2

Set up and configure a pfsense machine with 3 vlans: 5, 8, 99. Then,

1. (10%) Run DHCP server in all vlans with pfsense as their gateway.
2. (10%) Only machines in vlan 99 can access management interface of pfsense (ssh or web).
3. (10%) Machines in vlan 99 can only `ssh` to linux1 $\sim$ 3 and pfsense, and access the web interface of pfsense.
4. (5%) DNS should be available to machines in vlan 99.
5. (10%) Machines in vlan 5 and 8 can not create connections to machines in vlan 99, but the opposite direction is allowed.
6. (10%) IP addresses won't be modified in connections between vlan 5 and 8.

Show your work by demo.