Homework #3

Due Time: 2016/4/6 (Wed.) 17:00
Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Compress all your files into a file named **HW3__[studentID]__[version].tar.gz**, which contains one folder named **[studentID]__NA1** respectively.
- **Folder [studentID]__NA1** should contain a pdf file of all your answers in *Network Administration 1 Part.*
- Submit your tar file to **sftp://140.112.30.58:7000** with your workstation account and password.
- You should demo your *Network Administration 2 Part* to TA. Please fill the demo timetable.

Instructions and Announcements

- Discussions with others are encouraged. However, you should write down your solutions `in your own words`. In addition, for each problem you have to specify the references (the Internet URL you consulted with or the people you discussed with) on the first page of your solution to that problem.
- Problems below would be related to the material taught in the class and might be far beyond that. Try to search for additional information on the Internet and give a reasonable answer.
- Some problem below might not have standard solutions. We would give you the point if your answer is followed by reasonable explanations.
- **NO LATE SUBMISSION IS ALLOWED.**

Network Administration 1

1. Assume that you are the network administrator of the CSIE department. You have admin access to a Cisco switch network consisting of a core switch and a number of edge switches, forming a tree topology. One day you receive a report from NTUCC on malicious packets from 140.112.31.252, and you are responsible for notifying its user of the issue. Describe the necessary steps to trace the location of the end user (the port they use on the edge switch). Assume the gateway of 140.112.31.252 is 140.112.31.254, which is the core switch.

2. *Playing with Cisco Packet Tracer.* Download "hw3.pka" from the course website and complete the following tasks on Switch0:

   - set the hostname of the switch to "CiscoLab" (10%)
   - disable domain name lookup in CLI (5%)
   - set enable password to "CISCO" (should be encrypted) (10%)
   - create VLANs 10, 20 and 99 (15%)
   - make PC0 and PC1 be under VLAN 10 and make PC2 and PC3 be under VLAN 20 such that PCs in different VLANs cannot ping each other (35%)
   - make Admin be under VLAN 99 and Admin should be able to access the switch by telneting 192.168.99.1 (10%)
   - set telnet login password to "cisco" on VTYs 0 to 4 (15%)

   Use "Check results" on the "PT Activity" window to check your points, and save your work to **[studentID]__NA1/[studentID].pka**.

3. We learned about the Cisco password encryption feature in class and applied it in Problem 2, but the encryption is actually vulnerable to attacks since it's merely some sort of encoding instead of a one-way hash function. Decrypt the following encrypted password "04102E3E1F2D1C1B58492B5C". Real-world applications should apply the "secret" feature that makes use of hash functions such as MD5.

Network Administration 2

1. 設定 pfsense 並切 vlan2 與 vlan99 使得

   a) vlan2 的使用者 ping 不到 vlan99 的使用者

   b) vlan2 的使用者碰不到 pfSense

   c) vlan99 的使用者可以 ssh 到 linux1 ∼ linux3

   d) vlan99 的使用者可以不必背 ip

   e) vlan99 的使用者可以從 Web GUI 對 pfSense 做設定

   f) vlan99 的使用者不該可以連到其他的地方