Homework #6

Due Time: 2018/5/27 (Sun.) 22:00
Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Compress all your files into a file named **HW6_[studentID].zip** (e.g. `HW6_bxx902xxx.zip`), which contains two folders named **[studentID]_NA** and **[studentID]_SA**.
- There should be a **na.pdf** in **Folder [studentID]_NA** containing all your answers in *Network Administration*.
- There should be a **sa.pdf** in **Folder [studentID]_SA** containing all your answers in *System Administration*.
- Submit your zip file to Ceiba.

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 OR PLAGIARISM IS ALLOWED.**

Network Administration

Wi-Fi Authentication (15%)

1. WPA-Personal and WPA-Enterprise are two main method for authenticating users. What are the differences between them? (10%)
2. What authentication method is used by "csie" and "csie-5g"? (Please provide the evidence.) (5%)

Wi-Fi Encryption (15%)

1. WEP, WPA and WPA2 are three security protocols designed by the Wi-Fi Alliance (in that order). What cipher does they use, respectively? (10%)
2. What encryption method is used by "csie" and "csie-5g"? (Please provide the evidence.) (5%)

WPA3 (10%)

Earlier this year, the Wi-Fi Alliance announced the release of WPA3. Although it may take some time for the vendors to implement it and for us to upgrade our infrastructure, it doesn't hurt to get familiar with it now. Please list at least three new features or improvements that WPA3 introduces.

Seeing is Believing (10%)

There are actually many stages involved when connecting to Wi-Fi (under the CSIE wireless networks). Let's see it for ourselves.

1. Start Wireshark and capture the packages when connecting to "csie" or "csie-5G".
2. Apply the filter `eapol` to select relevant packages.
3. Provide a screenshot of the filtered packages.
4. Find the package where the client response to the AP with identity info (it should be student ID in this case). Provide the screenshot of the data field where the identity should be shown in plain-text.
5. Classify the packages filtered out into 5 stages specified below with the package number. (2% per stage)
    - Stage 1: EAP type proposal (outer authentication). Your identity is requested in this stage and the EAP type is determined.
    - Stage 2: TLS tunnel setup. You negotiate with the AP about the details of setting up a TLS tunnel.
    - Stage 3: TLS encrypted EAP inner authentication. Use the established TLS tunnel to finish authentication.
    - Stage 4: EAP success.
    - Stage 5: WPA2 4-way handshake.

- **If you didn't fulfill step 3. and 4., you won't get any point for this section**.
- For those whose machine can't capture 802.11 packages, you can download the pcapng file here.

System Administration

Short Answer Questions (16%)

Please write down your answers as pdf format, and separate them well.

1. What happens when we boot a Linux computer? (5%)
   Hint keywords: BIOS/UEFI, GRUB, kernel, init
2. What is the difference between traditional BIOS and UEFI? (3%)
3. What is the difference between NFSv2, NFSv3 and NFSv4? (3%)
4. In tradition, we build Preboot Execution Environment (PXE) with DHCP and TFTP services. Please explain how it works in detail. (5%)

Network Ninja (9%)

Imagine that you are one of the workstation managers. One day another manager told you that there is a suspicious user sending lots of weird packets from our workstations. It seems like he/she is trying to attack other servers online, and now you decide to log the messages to get more information about him/her.

Requirement: install an Arch Linux VM, set up `nftables` / `iptables` and other needed services (like... `ulogd` xD) to **log all packets sent from the VM**.

Please write down what you do step by step, and explain them in detail to get full credit.

PXE & NFS (25%)

In this part, you're going to build a system with PXE and NFS services.

Here are some basic requirements:

1. You can do this part on Virtualbox or libvirt-based virtualization platform; **you have to mention which platform you use in your report**.
2. The enviroment of virtual machines should be Arch Linux; please download the latest released image from official website.
3. You have to write down what you do step by step, and explain them in details to get full credit.
4. Please write down your answer in order, and separate them well.

3.1 (5%)

Install first VM (just call it `VM1`) of which the operating system is Arch Linux. `VM1` will be the PXE server and NFS server.

Since that `VM1` will be NFS server, please create a partition mounted on `/nfs`, which will be used as a shared partition with clients (call them `VM2` and `VM3`) later.

3.2 (10%)

Use `VM1` as PXE server, and install other two VMs (`VM2`, `VM3`) using PXE. Of course, the operating system should be Arch Linux :).

Hint 1: If you're using Virtualbox, you might have to install the extension pack to enable PXE support of Intel interface card.

Hint 2: I recommend you to use NFS method. That is, let PXE clients mount the installation media from VM1 using NFS protocol.

3.3 (10%)

Create an NFS system, in which `VM1` is NFS server, and `VM2`, `VM3` are NFS clients. The shared partition is `/nfs`, you can mount it anywhere on `VM2` and `VM3`, e.g. `/mnt/nfs` is ok.

Bonus: 3.4 (at most 10%)

As you can see, this system is a simple one, and there are lots of features you can add to it, like auto installation, automount, LDAP, Kerboros, etc. If you have time, please feel free to try them! I'll give you up to 10 points bonus according to what you done.