Homework #6

Due Time: 2019/6/2 (Sun.) 22:00
Contact TAs: vegetable@csie.ntu.edu.tw

Submission

- Put all answers **in one single PDF file** named **[studentID].pdf**, in the same order as the problem sheet. Do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Submit on NTU COOL (https://cool.ntu.edu.tw).

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

Short Answers (50%)

1. Sometimes a domain name is associated with several IPs. Explain why we might want to do so (10%).
2. Cache is important in the DNS world. Explain when cach is used (5%) and why they are needed from the perspective of recursive servers and authoritative servers, respectively (5%).
3. Explain *DNS propagation time* (5%) and its relationship with the TTL field in a DNS record. In what circumstances are higher (or lower) TTL beneficial? Explain the two cases each with an example (5%).
4. *DNSSEC* is introduced to mitigate certain attacks on the DNS system. Explain the threat model (10%) as well as how *DNSSEC* mitigates it (10%).

DnsDoOmSday (50%)

Arvin is a diligent schoolboy and is always eager to test out his skills. He recently learned about DNS and decided to setup his own recursive DNS server!! Everything went smoothly: his new DNS server is working and he is very much content with it until one day he was accused of launching an attack against some public servers. Though sometimes mischievous, Arvin is a good boy and would not purposely participate in such attacks; thus, we suspect there must be something wrong with the DNS server that he recently set up. To prove Arvin's innocence, we obtain Arvin's DNS server configuration files and query logs for further investigation. Now, could you figure out what really happened in the attack? What's the role of Arvin's DNS server in this plot? How should Arvin prevent such things in the future?

Note that Arvin's DNS server is not compromised in any way

1. (5%) State your observations (points would be awarded for worthy findings)
2. (10%) Come up with a reasonable attack scenario and explain the attack in details. (point would be awarded depending on how convincing the scenario is)
3. (10%) Why would this attack work? Provide full details on what you have discovered about the attack from the log. You can start with the questions listed below:
   - identity of victim
   - identity of culprit
   - attack vector
   - estimation of resources needed to launch attack
   - estimation of strength of attack
4. (5%) How should Arvin prevent such things from happening again?
5. (20%) Do it yourself! Set up your own VMs to replay this attack and observe the process. Provide screenshots of the process and give comments on the attack.

Warnings:

- ***Conduct your experiment strictly in your own environment.***
- ***Any attack on external servers results in severe consequences.***

System Administration

Lucky you! There is none in this homework.