Homework #5 Solutions

Due Time: 2015/5/25 (Mon.) 17:00
Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Compress all your files into a file named "⟨**studentID**⟩ .**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 a pdf file of all your answers in *System Administration Part*.
- **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 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 informaition on the Internet and give an reasonable anwser.
- Some problems below might not have standard solution. We would give you the point if your answer is followed by reasonable explainations.
- If you get stuck in problems below, feel free to contact TAs.
- **NO LATE SUBMISSION IS ALLOWED**.

Network Administration

1. 請解釋什麼是NAT(Network Address Translation)，以及他是如何運作的。

   略

2. 請敘述使用NAT有什麼優點與缺點。

   略

3. 假設現在有一台機器在某個NAT下，請問你該如何處理，才能使得即使你人在外面的網路也能ssh至該台機器工作?

   Method 1: 建立reverse tunnel至外面某個你碰的到的機器。
   Method 2: 架設VPN server，若要操作NAT裡面的機器，便先連VPN即可。

4. 根據Fig. 1，試著寫下封包是如何傳遞的，其中必須包含過程中封包的位置與source IP address & destination IP。

   a) Source：機器D
   Destination：機器A

位置	Source IP	Destination IP
D	192.168.1.2	128.199.58.41
C	192.168.1.2	128.199.58.41
C	128.199.74.25	128.199.58.41
B	128.199.74.25	128.199.58.41
A	128.199.74.25	128.199.58.41

   b) Source：機器D
   Destination：機器E

位置	Source IP	Destination IP
D	192.168.1.2	128.199.58.41
C	192.168.1.2	128.199.58.41
E	192.168.1.2	128.199.58.41

5. 承上題，今天你是機器A，透過VPN獲得IP 192.168.1.4，試著寫下封包是如何傳遞的，其中必須包含過程中封包的位置與source IP address & destination IP。

   a) Destination: 機器B

位置	Source IP	Destination IP
A	128.199.58.41	128.199.74.25
B	128.199.58.41	128.199.74.25
C	128.199.58.41	128.199.74.25
C	128.199.74.25	128.199.58.34
B	128.199.74.25	128.199.58.34

   b) Destination: 機器E

位置	Source IP	Destination IP
A	128.199.58.41	128.199.74.25
B	128.199.58.41	128.199.74.25
C	128.199.58.41	128.199.74.25
C	192.168.1.4	192.168.1.3
E	192.168.1.4	192.168.1.3

System Administration

System Configuration & log

1. Systemd has its logging system called the journal. Try to write down at least two other log management implementations (packages). (HINT: RFC 5424 The syslog Protocol).

   ANS: For example, rsyslog and syslog-ng.

2. On Debian GNU/Linux testing distribution, imagine you are a SA, having the root permission. Suppose you get a message from other SAs that this IP (or this machine) is trying to "attack their machine" by sending lots of HTTP requests (making lots of TCP connection). How would you do to find the rogue and reply to the message? There are dozens of users (like CSIE workstation) logging on this machine in the provided time interval. Let's try to config the system and log enough message to find out who the rogue is. In other words, you should know which process sends packets at the given time interval to the specific destination IP after looking into the log, so next time you can figure out what's going on as soon as possible if the rogue is trying to do the same thing on the system. With the log, you can further ban this user from accessing the system again.

   (a) When it comes to Linux firewall, a user-space application program is usually used to configure the rules and tables about the firewall. What's the name of the program?

   ANS: `iptables`. NOTE: `nftables` is intended to replace existing `iptables`, `ip6tables`, `arptables`, `ebtables` frameworks.

   (b) What kind of information is necessary to log? Can this program log the information you need?

   i. If your answer is `yes`, please output the rules in the tables. How to add or modify the rules in the tables in order to get the rules in the tables? Write down the commandes, and briefly explain why these rules you set can log what you have mentioned in the first question.

   ii. If your answer is `no`, write down what you have tried to solve this problem and fail to log enough information when you just use this package/command.

   Sample Answer: No. AFAIK, iptables can't log UID or PID. NOTE: This is only one possible answer. You may configure your system by using other set of commands and programs, or the modules in `iptables` can do this job. If this is the case, you should answer yes. Any possible solution will be accepted.

   (c) If you answer no in the previous question, give a set of instructions on how to setup the logging system in order to achieve the target you set in the first question. (HINT: take a look at another package which is also developed by netfilter[1])

   Sample Answer: Take a look at `ulogd` project. Install it by the command `apt-get install ulogd2`. A sample configuration will be created under `/etc/ulogd.conf`. After slightly modification to the configuration file, you can log what you want with the aid of ulogd. A sample setup of the iptables is provided as follow:

```
sudo iptables -N LOGGING
sudo iptables -A OUTPUT -j LOGGING
sudo iptables -I LOGGING -d ip_to_the_machine -m limit --limit 40/minute
--limit-burst 3 -j NFLOG --nflog-group 1 --nflog-prefix "example_log"
```

[1] http://www.netfilter.org/index.html

A sample record is provided as follow:

```
Feb 19 16:26:39 linux5 example_log IN= OUT=eth0 MAC= SRC=140.112.30.36
DST=140.98.193.112 LEN=84 TOS=00 PREC=0x00 TTL=64 ID=4504 DF PROTO=ICMP TYPE=8
CODE=0 ID=24494 SEQ=1 UID=0 GID=0 MARK=0
```

As you can see, there is a field called UID. This may help you to find out who the rogue is.

NOTE: This is only one possible answer. Any possible solution will be accepted.