Homework #1 Solutions

Due Time: 2015/3/16 (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*, and a file named "⟨*studentID*⟩ *.pcapng*".
- **Folder StudentID_SA** should contain all files 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

Part 1

While configuring the settings of Internet in a PC, we often encounter a keyword "TDP/IP", which is actually a combination of two protocol, "TCP" and "IP". Known that Internet is often classified into 5 layers in networking industry, the ISO/OSI model, however, tries to standardize the communication model, making it a 7-layer model, from the lowest layer, "Physical layer", to the highest layer, "Application Layer". In either model, a wellness of upper layer relys on stable connection of lower layer during communication, just like construction of upper floor relies on stability of lower floor while constructing a building.

a) According to the regulation of ISO/OSI model, to which layers TCP and IP respectively belong? Please write down the English name of the layers they belong. (10%)

「TCP」 屬於 「transport layer」,第四層
「IP」屬於「network layer」,第三層

b) UDP is at the same layer as TCP, but most of the servers that require stable connections over the Internet would adopt TCP, rather than UDP, as their transport layer protocol. Is this a reasonable choice, why or why not? (20%)

(答案僅供參考,只要說出道理即可給分)
合理,因為TCP是connectionoriented,也就是TCP運作的機制提供了雙邊穩定的連線,來回溝通確認,確保資料是否從一端送達另一端,而UDP只負責將資料傳出去,並不會確認對方是否收到資料。

c) Assume that you are using a browser. Whenever you try to fetch a web page, TCP and IP would both be working on your system to achieve your request. Besides those two protocols, what protocols are also used during the whole process of fetching a web page from remote. Please name one protocol which belongs to application layer, and describe what role it plays in the whole process. (20%)

DNS: 用來查詢網址(url)所對應的IP address。
HTTP / HTTPS : 用來傳送網頁訊息,HTTPS是較安全的版本。

Part 2

As an identification on the Internet, IP address is a critical information for two host to communicate. To send packet to the correct destination host, a sender needs to know the IP address of the reciever. IPv4, representing an IP address with 32 bits, is still the most general version of IP address. The total number of avaible address of Ipv4 is no larger than $2\hat{3}2$ and today we are running out of them. IPv6, with 128-bit long per address, is being promoted and claiming to let any sand on Earth to have a single IP address.

a) There are tools available online to translate URL to respective IP address. The IP address of NTU web server (www.ntu.edu.tw) is 140.112.8.116, which is apparently an IPv4 address. In fact, the web server of NTU-CSIE (www.csie.ntu.edu.tw) also uses IPv4 address. What is the IP address of the web server of NTU-CSIE? (15%)

在linux系統上可用nslookup指令查詢網頁的IP address,正確答案是140.112.30.28

b) Due to the limit amount of IP address, allocation of IP addresses is strictly managed by IANA(Internet Assigned Numbers Authority) and it is visible online. We can easily look up IP segments and countries or organizatinos that own them. However, you can't find the owner of some centain IP addresses, such as 192.168.0.1. Why is that? (15%)
(Hint: Distinguish the differences between Public IP and Private IP)

並非所有IP都會分配到世界上,有些IP address被保留為Private IP,供私人網路中使用,不屬於任何國家。這些IP address不用來對外連線,因此,所有想要架設私人網路的公司、政府、學校、社團組織,都可以在自己的私人網路內使用這些IP,讓自己的電腦設備互連。若要對外連線,才需要Public IP。根據IETF的RFC1918規範中,10.0.0.0/8、192.168.0.0/16、172.16.0.0/16都屬於Private IP網段。因此題目中,192.168.0.1在192.168.0.0/16的網段中,屬於Private IP,它不屬於任何國家。

Part 3

Please execute WireShark in any of the computer platform you can access. Try to connect to linux1.csie.ntu.edu.tw(140.112.30.32) and record all the packet flow until you login successfully. Then utilize the built-in filter to get the pakcets that the destination IP is 140.112.30.32 and the protocol being TCP. Write down the conditions you designed for filtering, and save the results as a file named "⟨*studentID*⟩ *.pcapng*", which must also be uploaded as a part of your homework. (20%)

過濾條件可如下表示
ip.proto == TCP && ip.dst == 140.112.30.32
(答案僅供參考,只要能過濾出正確結果,即可給分)

Part 4 (Bonus 30%)

NTUCC (Computer & Information Networking Center, NTU) is the primary network uplink of our whole campus. They would monitor the network traffic and take actions to ensure network security if needed. For example, blocking an IP address, of which the host is suspected of sending harmful packets or behaving abnormally. That host would not be able to connect to the Internet until the security issue is identified and solved. Like NTUCC, we, the network administration team of NTU-CSIE have our way to block a harmful host in our building. Rather than blocking the IP address, we block its MAC address to cause the similar effect.

a) What is MAC address? (15%)

Mac address 是網卡的編號,每一台電腦通常都配有二張網卡,一張有線網卡,處理有線網路連線;一張無線網卡,處理無線網路連線。而一張網卡在製造過程中,會被賦予一個編號,這編號就是Mac address,其中包含著製造商的資訊,因此可由Mac address反查網卡的製造商,每張網卡的Mac address都是全球唯一的。

b) Compared to IP address blocking, give an advantage of MAC address blocking. (15%)

鎖Mac address的優點:可以直接擋住從可疑電腦的網卡發出的封包,即使他更換IP也無法避免被封住,除非他改用另一張網卡、或使用虛擬網卡。鎖Mac address一般適合用於動態IP分配的網路之中,管理同網段底下的電腦。
鎖Mac address的缺點:Mac address屬於link layer,封包一經過router,Mac address就會變,反而IP address(Public IP)較可能保留下來。因此鎖Mac address不適合用於對付其它網段來的惡意封包。

System Administration

Shell Scripts

1. Find queue IDs of junk messages

```
#!/bin/sh

grep -v ’^ ’ | \
    grep ’b12345678@csie.ntu.edu.tw’ | \
    cut -f 1 -d ’ ’ | \
    sed -e ’s/\*//’ -e ’s/!//’
```

2. A compiler wrapper to workaround some broken build systems

```
#!/bin/sh

compiling_args=’-isystem /usr/local/include’
linking_args=’-Wl,-Y/usr/local/lib’
script_mode="‘basename $0‘"

for i; do
    case "$i" in
        -c|-S|-E)
            unset linking_args
            break
        ;;
    esac
done

if [ "${script_mode}" = "cpp" ]; then
    unset linking_args
fi

exec /usr/bin/${script_mode} ${compiling_args} "$@" ${linking_args}
```

3. Print the most recent login time and desktop session of an user

```
#!/bin/sh

as_get_login_time () {
    dbus-send --system --print-reply --dest=org.freedesktop.Accounts \
        --type=method_call /org/freedesktop/Accounts/User"$1" \
        org.freedesktop.DBus.Properties.Get \
        string:org.freedesktop.Accounts.User string:LoginTime | \
        tail -n 1 | { read variant int64 value; echo "${value}"; }
}

as_get_xsession () {
    dbus-send --system --print-reply --dest=org.freedesktop.Accounts \
        --type=method_call /org/freedesktop/Accounts/User"$1" \
        org.freedesktop.DBus.Properties.Get \
        string:org.freedesktop.Accounts.User string:XSession | \
        tail -n 1 | sed -e ’s/.*string "\(.*\)"$/\1/g’
}

date_format () {
    if date --version 2>/dev/null | grep ’GNU coreutils’ >/dev/null; then
        # We are using GNU coreutils
        date --date="@$1" ’+%Y-%m-%d %H:%M:%S’
    else
        # We are using BSD date command
        date -r "$1" ’+%Y-%m-%d %H:%M:%S’
    fi
}

if [ -z "$1" ]; then
    echo "Usage: $0 user" 1>&2
    exit 1
fi

while [ "$1" ]; do
    user="$1"
    uid=$(id -u "${user}")
    login_time="$(as_get_login_time ${uid})"
    xsession="$(as_get_xsession ${uid})"
    echo "${user} ${xsession} $(date_format ${login_time})"
    shift
done
```

Shared Folders and Files

```
# file: project_shared_folder
# owner: student1
# group: student
user::rwx
user:student1:rwx
user:student2:rwx
user:student3:rwx
user:ta1:r-x
user:ta2:r-x
user:prof1:r-x
group::---
mask::rwx
other::---
```