Network Administration and System Administration

Midterm Examination

Time: 2018/4/23 (Mon.) 09:10 - 12:10

Instructions and Announcements

- 考試時間共三小時，每組依照座位分配坐在一起。
- 除了第一題外，所有題目均可在 **R204 的電腦**上或**自己的筆電**上完成，**第一題只能在 R204 電腦上作答**。
- 以防發生重大意外，請自行在過程中斟酌是否需要備份 VM。若真的不幸發生悲劇，助教可以提供原始狀態的 VM，但傳輸或下載 VM 需花費一些時間，請盡量避免此一危機。
- 完成題目時可請助教過去評分，如果還未完成就偷跑先找助教，會給予 penalty 2 pts。若題目有若干小題，可分階段完成。有結果可以 demo 但 demo 失敗不在此限。助教有權判斷是否給 penalty。
- 組與組間**禁止討論**，如被發現等同作弊，**期中考 0 分**。
- 各題後面黑色星號數目代表我們估計的難度。請參考，可用來衡量解題順序。
- 滿分 200 pts。
- Good Luck!!

1 THE WALL (25%) ★★★

Network infrastructure

- Here are our bots that check if your firewall works according to the specifications. Import it to **Virtualbox** and then boot `VM-bot` and `VM-service`:
  - IMPORTANT: DO NOT try to modify, login, or read files/processes in these two VM; it's **cheating**. The only operations you can perform with these two VMs are to reinitialize MAC addresses and to turn them on/off.
  - You need to setup pfSense on the same R204 PC where the bots run.
  - You need to reinitialize MAC addresses of these two bot VM when you import them.
  - We do not guarantee these bots to work on virtualization platforms other than Virtualbox.
  - File: thewall ova
  - Bots will run every 30 seconds to check if you fulfill subtask 1 to 3. You can check the results at http://localhost:8080/. The status board will not update in real-time; refresh the webpage if you want to check the results.
- Here are some files you may need:
  - pfSense ISO
  - alpine ISO
  - Ubuntu 16.04 ova
  - It is not necessary to setup any client VM, but it may be helpful when debugging.
- Configure one bridged interface to access R204's network and to be used as WAN interface.
  - IP: Obtain from DHCP
  - Be careful with your web configurator access rule, LAN anti-lockout rule, and admin password, or some malicious party may sabotage your configuration :)
- VLAN 5 on WAN (user VLAN):
  - VLAN id: 5
  - Gateway IP: 10.0.5.254

  - Netmask: 24
  - Hosts in this subnet can connect to VLAN 8 and the Internet.

- VLAN 8 on WAN (service VLAN):
  - VLAN id: 8
  - Gateway IP: 10.0.8.254
  - Netmask: 24

- NOTE: You don't need to actually set up any host under VLAN 5/8. But if you do, do not assign IP `10.0.5.1` and `10.0.8.1` to the hosts, since TA's bots and services are using them.

Subtask 1 - Illegal (10%)

- Prerequisite: hosts in VLAN 5 can connect to the Internet.
- Objective: We have been notified that someone is downloading illegal copyrighted content. Please examine the traffic and block access to the possible sources.
- Hint:
  1. `Packet Capture` is your friend.
  2. Our bot sends a lot of packets, so increase the number of packets to capture when you use Packet Capture. Otherwise you may miss some very important packets!

Subtask 2 - All in One (10%)

- Prerequisite: hosts in VLAN 5 can connect to servers in VLAN 8.
- Objective: Our secret token `4VARTSmkwgjCwtrT` on server `10.0.8.1` is leaked. Find out which port it was leaked from, block the port and keep other services working.
- Hint: Do you know what is `port scanning`?

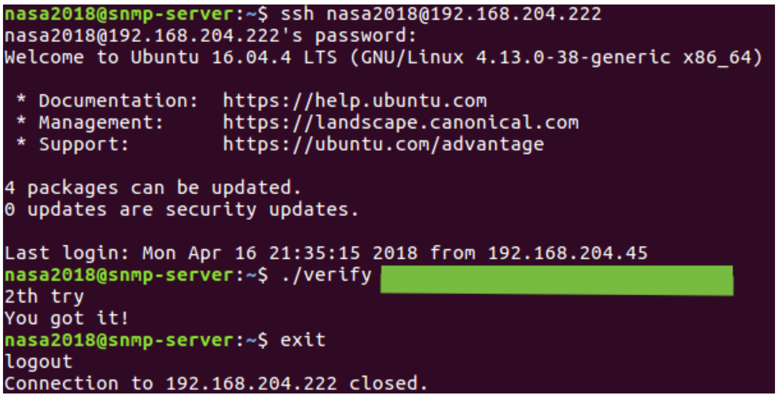
Subtask 3 - SNMP (5%)

As a network/system administrator, it is useful to collect all kind of metrics from your managed devices. Simple Network Management Protocol (SNMP) is a protocol designed to do that. Now, you are required to configure pfSense to run an SNMP agent and set up an SNMP manager from the provided pfSense MIB files and the Ubuntu 16.04 ova file (or create a VM of your favorite distribution on your own). The following requirements should be satisfied.

1. Use SNMPv2c.
2. When querying from the manager,
   a. `-v` and `-c` flags don't need to be specified,
   b. for the host argument, use alias instead of IP address.
3. These commands should be able to work:
   a. get brief system info: `snmpwalk alias:pfSense system`,
   b. get interface status: `snmptable -Cbi -Cw 80 alias:pfSense BEGEMOT-PF-MIB::pfInterfacesIfTable`.

2 SSH Leak? (20%) ★★★★★

A NA TA was doing some mysterious things at R204. I thought it was related to the midterm exam, so I sniffed his packets. I was behind him and saw him typing something like the following picture:



```
nasa2018@snmp-server:~$ ssh nasa2018@192.168.204.222
nasa2018@192.168.204.222's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

4 packages can be updated.
0 updates are security updates.

Last login: Mon Apr 16 21:35:15 2018 from 192.168.204.45
nasa2018@snmp-server:~$ ./verify [redacted]
2th try
You got it!
nasa2018@snmp-server:~$ exit
logout
Connection to 192.168.204.222 closed.
```

The green part is the password. I couldn't memorize it since it is long, but I remember that it contains only 1 and 0. Can you help me to get the password and own the midterm together? :)

Details:

- In this problem, each team is given an SSH account on the server. Your goal is to execute `./verify [password]` with the right password.
- The captured packets are in `ssh.pcapng`.
- The source code of verify is at verify.c.
- Once you successfully execute `./verify [right password]` and get the message `You got it!`, you will get the points of this problem.
- Ignore the fact that the server's host name is `snmp-server`. This problem has nothing to do with that. I used another TA's ova file to create the environment for this problem.

[**WARNING**] The maximum number of times that each team can guess is LIMITED!! This is reset every 45 minutes. As a result, be clever on your attempts!

- Don't worry about this constraint when testing the behavior of the program manually. The limit is far more than sufficient for you to test. The constraint is created to prevent you from using a brute-force attack to obtain the password ”mindlessly”.
- Hint: What is the length of the password? You may want to observe the behavior of your own SSH connection.

P.S. Attacks against the server are allowed (i.e., privilege escalation) and you'll be rewarded if you succeed. However, if other teams are affected during the process, you will receive penalty in your score. So, do it at your own risk.

3 Agent J (25%) ★★

Last week, NASA's web server (`192.168.0.254/24`) was compromised by a secret agent, Jin. He stole the secret flag in the server. What's worse, Jin even deleted all the evidence he left, including the backdoor. However, the mills of god grind slowly, and eventually a hacker will be caught. Please help the NASA team to track down Jin.

The packet dump of the web server can be downloaded here. Note that since Proxy ARP is enabled in the environment, all the clients source MAC address are identical.

Your objectives:

1. Find out Jin's source IP in LAN.
2. Determine the content of the leaked flag.
3. Jin seems to have another server to help him to steal the flag. Find out which country the server is hosted. NASA team will contact the responsible authorities.

4 Cisco packet tracer (25%) ★★

Hey new IT intern, please help us to set up our network! There are 3 switches, which contains a core switch and 2 end switches. PCs are located on VLAN 8, and servers are located on VLAN 30. Please configure the network according to the following specifications:

1. Create trunk connections with link aggregation among these switches.
   - Core: port-channel 1 (Gi0/1, Gi0/2) ↔ Switch0: port-channel 1 (Gi0/1, Gi0/2)
   - Switch0: port-channel 2 (Fa0/1, Fa0/2) ↔ Switch1: port-channel 1 (Fa0/1, Fa0/2)
2. Connect the PCs and servers to their respective VLANs.
3. PC0 is the admin of the whole network. Put it on VLAN 99.
4. Allow PC0 to telnet to Core Switch through `192.168.99.10/24`.
5. Change the hostname of Core Switch to `Core`, and use enable secret `cisco`.
6. In Core Switch, configure login username `admin` with plain-text password `nimda` on vty 0.

Cisco Packet Tracer:

- Username: `cisco.packet.tracer3@gmail.com`
- Password: `Cisco.packet.tracer3`
- Download Cisco Packet Tracer here
- Work with the pka file here.

5 Simple CSV Viewer (20%) ★★★★★

CSV (Comma-separated values) is a well-known file format. Please write a simple CSV viewer that meets the given criteria. Here are some notes:

- You can assume that the first line of CSV file is a valid header.
- You can only use the standard shell (POSIX, sh) or GNU bash.

- You may find test data here.

This problem can be divided into three continuous stages:

Stage 1 (5%)

- Output help message when this script is used in an incorrect way or with option h.

Examples:

```
$ ./csv_viewer.sh
csv_viewer.sh [ -f names | -h ] file
-f names    specify the columns names by comma separated list of names
-h          print this help message

$ ./csv_viewer.sh -h
csv_viewer.sh [ -f names | -h ] file
-f names    specify the columns names by comma separated list of names
-h          print this help message

$ ./csv_viewer.sh file
csv_viewer.sh [ -f names | -h ] file
-f names    specify the columns names by comma separated list of names
-h          print this help message

$ ./csv_viewer.sh -f FIELD file1 file2
csv_viewer.sh [ -f names | -h ] file
-f names    specify the columns names by comma separated list of names
-h          print this help message
```

Stage 2 (10%)

- Generate a columnized list according to the order specified with option f.
- Output error message to stderr when invalid column names are specified, but still output other valid columns to stdout.

Examples:

```
$ cat dataset-small.csv
URL,URL_LENGTH,Type
M0_109,16,1
B0_2314,16,0
B0_911,16,0
B0_113,17,0
B0_403,17,0
B0_2064,18,0
B0_462,18,0
B0_1128,19,0
M2_17,20,1
```

```
$ ./csv_viewer.sh -f Type,URL dataset-small.csv
Type  URL
1     M0_109
0     B0_2314
0     B0_911
0     B0_113
0     B0_403
0     B0_2064
0     B0_462
0     B0_1128
1     M2_17

$ ./csv_viewer.sh -f Type,NOT_IN_HEADER,URL dataset-small.csv
'NOT_IN_HEADER' is not a valid field
Type  URL
1     M0_109
0     B0_2314
0     B0_911
0     B0_113
0     B0_403
0     B0_2064
0     B0_462
0     B0_1128
1     M2_17
```

Stage 3 (5%)

- Your script must work with process substitution in bash.

Example:

```
$ ./csv_viewer.sh -f Type,URL <(head -n2 dataset-small.csv)
Type  URL
1     M0_109
```

6 Matryoshka Doll (20%) ★★★★

Mr.Codera is a well-known DL (Dummy Learning) and NLP (No Language Processing) researcher. One day, he received a special package; he tried to find out what is in the package, but when he opened it, there was another package inside! After repeating it for several times, he gave up and made you, a newbie of his laboratory, to do the job for him.

Objective: You have to write a shell script to remove multiple layers of compression to uncover the content of the package, satisfying the following requirements:

- Name: doll.sh
- Usage: `./doll.sh [file]`

- You can find an example of the package here.
- Follow the sample output format:

```
$ ./doll.sh package
DeepLearningLearnNothing
```

- Note:
  - `Mr.Codera` told you that there are only four types of compression might be used to compress the file: tar, rar, zip, and gz. (Don't ask why he knows that, it's Dummy Learning!)
  - Since `Mr.Codera`'s computer is weak, you can only use the commands we've taught in class, and **`file`**, **`tar`**, **`rar`**, **`unzip`** and **`gzip`**.
  - `Mr.Codera` is a perfectionist, so you have to make sure that there isn't any error during your extraction, or he won't give you any credit!
  - You can extract the example file manually first to get more information about this special package. FYI, you'll get another package to extract during testing.

7 I Get My Job! (20%) ★★★

`Mr.Codera` uses CSIE workstations to run his experiments almost everyday. Of course, he has to browse monitor.csie.ntu.edu.tw to get information about these workstations. However, sometimes the website turns dead, and `Mr.Codera` can't see the status of workstations. His best assistant, you, are asked to create a webpage like monitor.csie.ntu.edu.tw to list the status of workstations (linux[1-15], oasis[1-3], not including bsd1).

Objective: You have to write a shell script satisfying the following requirements:

- Name: monitor.sh
- Usage: ./monitor.sh
- Output: a webpage named monitor.html, in which is a table consists of the information (CPU, loading, free memory, swap (%), tmp2 free space, uptime and count of online users).
- You can find an example of the output format here.
- Note:
  - You can only use the standard shell (POSIX, sh) or GNU bash.
  - You don't need to make everything exactly same as the webpage; however, you have to make sure that you really fetch the correct information, and have to explain your code to TAs to get the credit.
  - You don't need to do it in some fancy way, and it's totally okay for you to use the code from homework 1 :)
  - It's okay for you to split your code into several functions, or several files (if you want LOL).

8 Матрёшка (20%) ★★★★

Create a virtual machine host, and create 2 virtual machines based on `libvirt` inside it (just as what you did in homework 4). Each virtual machine should have 4 containers with `sshd` running.

The two virtual machines use IP1 and IP2, respectively. The objective is to setup the containers and to allow one to run commands:

```
ssh b07902000@[IP1] -p 1022
ssh b07902000@[IP1] -p 2022
ssh b07902000@[IP1] -p 3022
ssh b07902000@[IP1] -p 4022
ssh b07902000@[IP2] -p 1022
ssh b07902000@[IP2] -p 2022
ssh b07902000@[IP2] -p 3022
ssh b07902000@[IP2] -p 4022
```

to access the containers form outside of the virtual machine host, respectively. You have to figure out how to do that :D

Objectives:

1. Create 1 virtual machines and login to it via any console. (8%)
2. Be able to ssh login to the **4** containers from outside of the VM host (e.g. 204 PC). (Only one VM is necessary.) (10%)
3. Be able to ssh login to **all** the containers from outside of the VM host (e.g. 204 PC). (Two VMs are required.) (2%)

Relevant Files

- VMWare VM Image with CentOS Installed
  - Linux 1
  - Linux 2
  - Linux 3
  - Linux 4
  - uid/password: root/nasa

  Note: We highly recommend that you use the image on R204 PC. We do not guarantee that the image will work in other environments.

- CentOS Docker image
  - Linux 1
  - Linux 2
  - Linux 3
  - Linux 4
- CentOS installation ISO file

  - Linux 1
  - Linux 2
  - Linux 3
  - Linux 4

Hints

- To import a VMWare VM, first unzip it, and load it from `File` > `Open`. You can ask a TA if you have any problem during this process.
- To save time, instead of pulling image, you can download CentOS Docker image from links provided above, then load it with command `docker load -i centos.tar`.
- The `sshd` application can be installed with `yum install -y openssh-server`.
- SSH key pairs must be generated before `sshd` can be run. You can generate them with `ssh-keygen -A` once `openssh-server` package is installed.
- To run `sshd` in Docker properly, you may need to run it as `/usr/sbin/sshd -D`. The `-D` argument tells `sshd` to run in foreground.
- Maybe you will want to check man page of `passwd`.
- If you have network problem with Docker, you can try `systemctl restart docker`.
- You can clone a VM with command `virt-clone -o [ORIGINAL_GUEST] --auto-clone`.
- `nmtui` may be your good friend.
- You may need to stop firewall in your VM with command `systemctl stop firewalld` to access ports `X022` from outside.
- матрёшка and how to pronounce it.

9 More on Storage! (25%) ★

Before you start, download `nasa-midterm.ova` from `linux1-4` under `/tmp2`. The username is `nasa` and the password is `nasa2018`.

There should be a network interface for you to SSH into as mentioned in class. Also, there is another network interface which you are allowed to use to access the Internet. You may simply use the command `sudo ifup <interface>` to enable the interface.

Part 1 (10%)

Please fulfill the following requirements.

`/dev/sdb`:

- GPT partition table
- first partition, 400 GiB in size, labeled as LVM
- second partition, use the rest of the disk, FAT32 file system

- mount the second partition somewhere you want in the system

`LVM`:

- create a volume group `storage` with the first partition of `/dev/sdb` and the entire `/dev/sdc`
- create a logical volume `bebi`, 250 Gib in size, and use ext4 file system
- create another logical volume `inm`, 150 Gib in size, and use ext4 file system
- mount them somewhere you want in the system

Note: If you encounter any difficulty, you should try to google it yourself first.

Part 2 (10%)

Shrink `/dev/centos/home` to 20 Gib and create a new logical volume `images` under volume group `centos` with the rest of the space and use xfs file system.

Note: You should be careful dealing with the file system while resizing. Under `/home` there are many folders and files belongs to user `nasa`. Any data loss is intolerable and would result in no credit. There are several ways to get around the problem.

Part 3 (5%)

There's an old disk `/dev/sdd` in the system. Please satisfy the following requirements.

- extend volume group `storage` to fill the entire disk
- create a logical volume `csie` to use all remaining space and ext4 file system
- mount it somewhere you want in the system

Note: You are not allow to partition `/dev/sdd`, which means that if you come up with something like `/dev/sdd1`, you would get no credit.