Homework #0 Solution

Contact TAs: vegetable@csie.ntu.edu.tw

Network Administration Preliminary

True/False

1. False. The Internet is provided on a "best-effort" basis and 100Mbps is the best possible value. "Oversubscription" is often the case. If everyone "has" 100Mbps network connection, and then we "have" more network connection than the actual amount. Therefore, congestion can happen. However, people seldom utilize network 24/7, so it's often not a problem.

2. False. Ideally, one IP address corresponds to one host, but NAT breaks this rule. NAT enables many people to share one public IP address and thus sharing the same IP address doesn't imply they are the same person.

3. True. Without DHCP, one can still configure network manually. However, a gateway is required to connect to hosts outside local network.

4. True. MAC addresses are designed to be unique in the same broadcast domain (although an end device is able to be explicitly assigned a custom MAC address).

5. False. Upon receiving a packet, a hub broadcasts the packet to all ports except the incoming one, while a switch maintains a MAC-port lookup table and forwards packets only to corresponding ports, which eliminates redundant traffic.

6. False. When you connect to a domain name, DNS is required to translate that to an IP address so that your computer can recognize that host.

7. False. Many devices only support 802.11b/g/n wifi, so turning it off is not a wise move.

8. True. That's how firewall works.

9. False. Each DNS server only caches or stores part of them. If a DNS server is asked an unknown domain name, it will ask the DNS server which controls that domain name. (For detailed explanation, see "authoritative DNS server" and "DNS resolver")

10. True. As an example, windows have the option of "Obtain DNS server address automatically."

11. True. Though, one may be able to decrypt other people's data which is also under the same wifi network. If you are typing some confidential data, use VPN or https.

12. True. For the latter part, VPN helps achieve better download speed through bypassing congested network or utilizing a better network route.

13. True. With proper routing.

14. True. IPv4 header(20) + TCP header(20) = 40bytes. Payload is almost empty.

Select All That Apply

1. (b)(c)(d)(e)
2. (a)(c) are public ones.
3. (a)(d) (a) IPv6 provides much more usable IP addresses. (d) CGNAT is a special case of NAT. NAT let many hosts share a public IP address, so we don't have to assign a public ip address to each host.

System Administration Preliminary

1.1

In the welcom screen text
`NASA{HW0_1S_YOUR_T1CKET_TO_NASA_COUR5E!!}`

1.2

Type `pwd` and then the flag is in part of the returned path
`NASA{YOU_ARE_@_YOUR_HOME!!}`

1.3

```
$ ls -al
```
Then the flag is there
`NASA{1s_-al_2_5EE_WH4T_YOU_H4VE:D}`

1.4

First make `engine` executable
```
$ chmod +x engine
```

Then execute it
```
$ ./engine
```
It will print out the flag
`NASA{chmod_4ND_./_ON_THE_FLY}`

1.5

Use `cat` to see password of the zip file
```
$ cat toolbox-key
```

Then unzip it
```
$ unzip -P WOW_IT_SEEMS_THAT_YOU_CAN_SEE_ME toolbox.zip
```

Or simply
```
$ unzip -P $(cat toolbox-key) toolbox.zip
```

Then use `tar` to untar the tar file
```
$ tar zxvf toolbox.tar.gz
```

`flag5.txt` is in `toolbox`, to see it
```
$ cat toolbox/flag5.txt
```

1.6

To get into the toolbox
`$ cd toolbox`

To remove the obstacle
`$ rm obstacle`

To rename the crisis to chance
`$ mv crisis chance`

Then execute magic
`$ ./magic`
The flag is there
`NASA{Cant_you_believe_that_you_built_up_my_wing}`

1.7

To see home directory of user `NASA`, command
`$ getent passwd`
can be used.
Or check `/etc/passwd`, user `NASA`'s data happens to be there, though not necessarily all users's data will be there.

Or simply
`$ echo ~NASA`

Then
`$ ls -la ~NASA`
`etago` can be found there.

Execute it with the absolute path
`$ ~NASA/etago`
Find that it dumps lots of garbage
So `pipe` is needed
`$ ~NASA/etago | less`
Then use `/` in `less` to find the flag (or use your eye):
`NASA{|_AM_A|||||||||||||||||||||||||}`

Or simply use `grep`
`$ ~NASA/etago | grep 'NASA'`

1.8

Execute throttle
`$ /plane/throttle`

Then press
`$ Ctrl + C`
`$ Ctrl + Z`
`$ Ctrl + \`

Then get the flag
`NASA{ctrl_z_ctrl_c_ctrl_\}`

1.9

`$ man man`
Then the flag is in the description section:
`NASA{M4N_15_THE_4BBREV1AT10N_OF_M4NUA1}`

1.10

To find out something suspicious, first observe top.

Then you can find that a process `periodic` appears every 1 minute with differet PIDs running as user `nobody`, so check `/var/spool/cron/nobody` and then you can find `/opt/wrapper.sh`.

Check `/opt/wrapper.sh`, and then you can find that the program `periodic` is also there.

Run `/opt/periodic`, you can see an error message "sh: te1net: command not found".
Use `ltrace` and `strings` to inspect `periodic`, and then you can find it issues a command `te1net nasa-hw0.csie.ntu.edu.tw 9487`.

Then `grep -r 250F /proc/1/net/tcp` to see who is listening on the port, and then you can find it is user `65694`. (`250F` is the hex of `9487`)

Check `getent`, find out that it is user `b03902072`.

Use `ps -u b03902072` to see that he is (I am) running the program `throttle`.

Apparently, the real `throttle` does not listen on the port 9487. Therefore, this `throttle` is not the `throttle` you know before. Check the permission of `~b03902072`, you will find that `x` is on. Try to execute `~b03902072/throttle`, it will print out an error message `sh:1s:command not found`.

So, again, use `strings` to see what the hell there is. Then find it issues a command `1s -al ./top-secret-base64-encoded-sha1sum-1413d9ae974b265cae3a8575128658ee4901b53f`.

Use `base64 -d` to decode
`~b03902072/top-secret-base64-encoded-sha1sum-1413d9ae974b265cae3a8575128658ee4901b53f`

and you can use command `file` to know that it is a gzip file.

Use `gunzip` to unzip it, and use command `file` again. Then you can find that it is a LVM image.

Then you can use command `losetup -f` and `mount` to mount partition `secret-flag` on it.

Check the partion, and find a file `F14GIO`. Again use `file` to know that it is a `bzip` file.

Use `bzip -d` to unzip it and get the file containing the flag.