Homework #2 Solution

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

Network Administration

1. Flamestrike (15%)

(a) A broadcast storm is the accumulation of broadcast traffic. Those traffic will keep broadcasting through the network, which leads to consume computational resources of switches. It's usually due to a switch loop in the network topology.

(b) The first thing is to find out the source. By monitoring to the traffic, we can find out some dominant source IPs or MAC addresses. Additionally, we can check the broadcast packet of each switch, to identify the possible loop one. Finally, trace down the source and manually shut down the interface.

(c) STP is intended to prevent possible switch loops in the network. Basically, STP utilizes an algorithm to ensure there is only one path between two different nodes. For each path, it selects the preferred path based on bandwidth. The other path will be put in blocking state. Thus, it can prevent loops.

2. MAC Pro (20%)

(a)
- ARP, 10.0.0.1 -> 10.0.0.2, fa:ce:b0:00:00:0c -> ff:ff:ff:ff:ff:ff
- ARP, 10.0.0.2 -> 10.0.0.1, de:ad:be:ee:ee:ef -> fa:ce:b0:00:00:0c
- ICMP, 10.0.0.1 -> 10.0.0.2, fa:ce:b0:00:00:0c -> de:ad:be:ee:ee:ef

Note that ARP is a layer 2 protocol. Actually it does not contain a layer 3 IP address.

(b)
- fa:ce:b0:00:00:0c: Interface 1
- de:ad:be:ee:ee:ef: Interface 2

(c)
- ARP, 10.0.0.1 -> 10.0.0.254, fa:ce:b0:00:00:0c -> ff:ff:ff:ff:ff:ff
- ICMP 10.0.0.1 -> 140.112.30.28, fa:ce:b0:00:00:0c -> ba:aa:aa:ad:c0:de

(d)
1. Spoof Gateway's ARP reply to Mario: When Mario is asking the Gateway's MAC address, we can spoof the reply to pretend we are the Gateway. Thus, Mario's upstream traffic will redirect to us.
2. Spoof Mario's ARP reply to Gateway: When Gateway is asking Mario's MAC address, we can spoof the reply. Thus, Mario's downstream traffic will redirect to us.
3. Man-in-the-middle eavesdrop: Now we have become a man in the middle successfully. Since Mario uses 'telnet', which is a plain text protocol, by simply eavesdropping the traffic, we can get his password.

3. Let's IPv6 (15%)

(a) ICMPv6

(b) ff02::2

(c) The following is a sample working code.

```
$ ssh STUDENT_ID@oasis2.csie.ntu.edu.tw
$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
    default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: net0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    group default qlen 1000
    link/ether 52:54:00:73:17:dc brd ff:ff:ff:ff:ff:ff
    inet 140.112.30.52/24 brd 140.112.30.255 scope global net0
       valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe73:17dc/64 scope link
       valid_lft forever preferred_lft forever
3: net1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    group default qlen 1000
    link/ether 52:54:00:f2:8c:2d brd ff:ff:ff:ff:ff:ff
    inet 10.217.44.52/24 brd 10.217.44.255 scope global net1
       valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fef2:8c2d/64 scope link
       valid_lft forever preferred_lft forever
$ ncat fe80::5054:ff:fe73:17dc%net0 9453
You have successfully connect me using IPv6!
Please write the follow message in your homework:
2e19fd12+af779a7258cc59b4291f848ec9a87211
```

- ”When connecting to an IPv6 link-local address, you need to specify through which link to reach it.” Refer to https://unix.stackexchange.com/a/136473
- The IPv6 server in oasis2 doesn’t listen on the localhost `::1`.
- Since `oasis2.csie.ntu.edu.tw` doesn’t contain IPv6 AAAA address, `ncat oasis2.csie.ntu.edu.tw 9453` will connect to IPv4 address of oasis2. You will see a cute cat (specifically, Pusheen) saying that ”Why are you still using IPv4?”. However this is the incorrect answer.
- An unintended solution: Execute `ps aux` in oasis2 and you are able to see the parameters of my server, `ncat -6 -lk fe80::5054:ff:fe73:17dc%net0 9453 --exec ./server.py`. (Thanks to @B04902083)

- The IPv6 server will response a message based on a nonce and HMAC signature.

```python
#!/usr/bin/env python3
import hmac
import secrets
h = hmac.new(key='N@5@_2018_5pRing'.encode())
s = secrets.token_hex(4)
h.update(s.encode())
print(f'''You have successfully connect me using IPv6!
Please write the follow message in your homework:
{s}+{h.hexdigest()}''')
```

System Administration

1 Playing With LVM

1.1 Storage For NASA Course (15%)

```
pvcreate /dev/sd{b,c}
vgcreate storage-vg /dev/sd{b,c}
lvcreate -L 150G -n student storage-vg
lvcreate -L 350G -n ta storage-vg
lvcreate -l 100%FREE -n hsinmu storage-vg
mkfs.ext4 /dev/storage-vg/student
mkfs.ext4 /dev/storage-vg/ta
mkfs.ext4 /dev/storage-vg/hsinmu
```

1.2 Need More Space (20%)

```
pvcreate /dev/sdd
vgextend storage-vg /dev/sdd
lvresize --resizefs -L -150G /dev/storage-vg/ta
lvresize --resizefs -l +100%FREE /dev/storage-vg/hsinmu
```

2 PTT Alert (15%)

硬碟損壞的機率非理想中的獨立事件。通常一整批購買時，這些硬碟就有很大的機率在相近的期限就故障損壞。因此雖然使用RAID可以增加儲存資料的可靠度(Reliability)，但是也應該謹慎使用且做好備份工作。

- RAID5 upgrade to RAID6 (increase reliability)
- replace old disks periodically (reduce failure probability)
- routine backups on different machines or offsite