Sisältö

1 Exercise 5: Introduction

In this exercise, a tunnel from KONE2 to KONE1 is made. That tunnel is used for SSH and a web server. Backups VG is prepared for backups.

Meanwhile, there is the twin of `diskfiller.sh` running, called `diskkiller.sh`. This might break your VM. Worry not, there are instructions to fix it in the last section.

When presented with multiple equal options to solve a problem, some people experience decision fatigue. Then you may let the RNG (Random Number God) decide the right path for you with this short bash function: `choose() { shift $(($RANDOM%$#)); echo $1; }` (for BSD and OSX, replace $((..)) part with ‘`jot -r 1 0 $(($#-1))`‘) To use it, write something like `choose option-1 option-2 option-3` and it will choose one of the options for you.

2 Steps (all in KONE2 unless otherwise noted)

2.1 Setup nginx

- Install nginx. See that it serves the placeholder page. Include the string “hello from behind the cat… er nat” in the index for the checker. You may create a new file with the string, or edit the placeholder, or use your web designer skills.

2.2 Setup autossh

Install `autossh`. Make a SSH tunnel from KONE2 to KONE1. This tunnel forwards SSH and HTTP traffic from KONE1 ports to KONE2. Forwarding it this way allows us to access KONE2 from outside of the lonka networks (JYUnet).

1. Make a SSH key for the zero account in KONE2. Copy the public key to KONE1 to allow automatic login with autossh. Test and see that it works.

2. In `.ssh/config`, add the configuration at the end of the chapter [1]. If you try logging in to KONE1 now, you should see the forwarded ports in listen state with `ss tl` command. However, the bind address is 127.0.0.1 or ::1, which only allows connections from localhost.

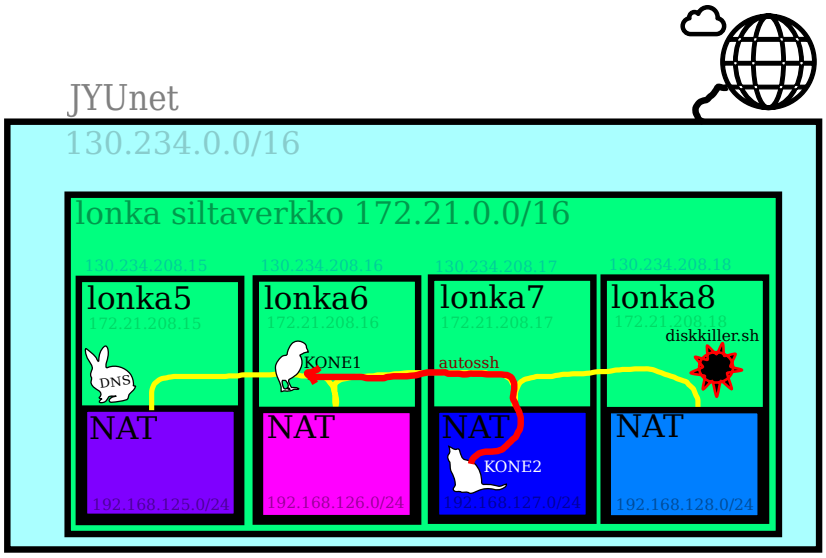
3. Edit `/etc/ssh/sshd_config` in KONE1. Add the following line: `GatewayPorts yes` [2]. Reload sshd configuration with `kill -HUP ‘pidoff sshd‘` (or restart sshd service, or restart the whole VM). Try the connection again and see if the remote forwards work properly. Tunneling can be tested by connecting to the forwarded ports from a lonka.

4. Edit crontab (`crontab -e`) and add the following line: `@reboot autossh -fN KONE1`

5. Reboot and see if it works. If it doesn't, try running autossh (or plain ssh) manually and see what happens.

[1] This will make the forwards default if we try to ssh from KONE2 to KONE1 with the zero account. This conflicts with autossh. Optionally, you can create a separate account in KONE2 just for autossh. See `ssh_config(5)` for explanation.

[2] This setting allows remote connections to connect to the forwarded ports and thus reach KONE2. See `sshd_config(5)` for explanation.



./autossh.svg
SSH Configuration:

```
Host KONE1
User TUNNUS0
PasswordAuthentication no
ExitOnForwardFailure yes
ServerAliveInterval 120
RemoteForward *:8080 localhost:80
RemoteForward *:2222 localhost:22
```

2.3 Setup reverse proxy

1. Edit `/etc/nginx/sites-available/default` (Optional: create a new config file) Add the things at the end of the chapter.

2. Since the host sNNN.vm.it.jyu.fi doesn't resolve to a local address (bridge or NAT), we need to include that record in `/etc/hosts` to make it work from NAT.

3. Restart nginx. Test that the reverse proxy works for all of the URLs. Both http://KONE1.student.it.jyu.fi:8080 and http://192.168.12N.XXX should return the same page ("hello from behind the cat"), and http://KONE1.student.it.jyu.fi:8080/kone1a should return the same page as http://KONE1.student.it.jyu.fi/. http://KONE1.student.it.jyu.fi:8080/kurssi should take you to the homepage of this course. (You can test these in a lonka with `lynx`, and KONE1 addresses work everywhere within the university network.)

4. What is the path of a HTTP request in this setup? Elaborate this in your log. Explain briefly how packets are routed between KONE1 and the new KONE2.

Reverse proxy configuration:

```
location /kone1a { proxy_pass http://KONE1.student.it.jyu.fi/; }
location /kone1b { proxy_pass http://sNNN.vm.it.jyu.fi/; }
location /kone1c { proxy_pass http://KONE1.ties478.website/; }
location /kurssi { proxy_pass http://kurssit.it.jyu.fi/TIES478/2019/; }
```

2.4 Setup backups partition

1. Make a LV inside the backups VG. Format that into xfs (`mkfs.xfs`), and make a mount point `/backups` for it. Include this is in `fstab`. Test that it works over a reboot.

2. Make a manual backup of configurations, logs, keys, and everything you see necessary. Also backup relevant things from KONE1 (using scp should be fine, later we learn about `rsync` and friends).

3 In case the VM doesn't boot anymore

./penguins-stabintheback.gif

Oh no! You have been visited by the antidiskfiller, that makes the disks disappear instead of filling them up. In this part, you will learn how to deal with an unbootable system and how to make that functional again.

3.1 Getting into GRUB

1. Reset the VM while having an open console. You will see GRUB menu as the first thing. Press `c` to open GRUB shell. Here you can insert boot commands manually. Type `linux /boot/vmlinuz^T console=ttyS0 serial` to find the kernel (press TAB at `^T` to autocomplete), and then `initrd /boot/initrd^T` for the initial ramdisk. Finally, `boot` command to boot them.

2. You should see boot messages and soon after that, a `(initramfs)` prompt (if not, reset and try again).

3. Activate LVM LVs: `lvm lvchange -ay --sysinit TUNNUS2-vg &`. Then refresh device mapper with `dmsetup mknodes`. Now you can find and mount your LVM partitions manually from `/dev/mapper`.

4. If the above two steps didn't work, try editing the Ubuntu entry (press e). Move downwards, until you find the line that starts with linux. Append `console=ttyS0 init=/bin/sh` and ctrl-X to boot. This should open a shell. Remount the root partition with `mount -o remount,rw /`

5. Mount the filesystems and find the source of the problem and fix it. Hint (rot13): Ybbx ng rgp sfgno.

6. Is the script starting up regularly, and where is it starting from? Investigate.

3.2 Finish

- Check updates for the systems.
- Run the checker script. (`sudo checker.sh 5`)

./sorry-no-fancy-gifs-in-the-pdf-version.gif