# CO2508 Computer Security

## Worksheet – 06 Tinkering with the Firewall

### Homeworking Risks

I do not think there are any legal risks when completing this worksheet.

It will involve enabling and disabling a firewall on one of the virtual machines; however, as long as you have a firewall running on your host machine then you should not be increasing the risk of an attacker against your host machine.

Installing a firewall will require a small amount of data to be downloaded to your virtual machine; if you set up the virtual machine with enough hard disk space (I suggested 80gb in the installation instructions) then there will be no ‘logical’ storage problems; this will obviously also require physical storage space to be available.

**Note: I will refer to co2508kali001 as kali001; co2508kali002 as kali002.**

### Aims of this Worksheet

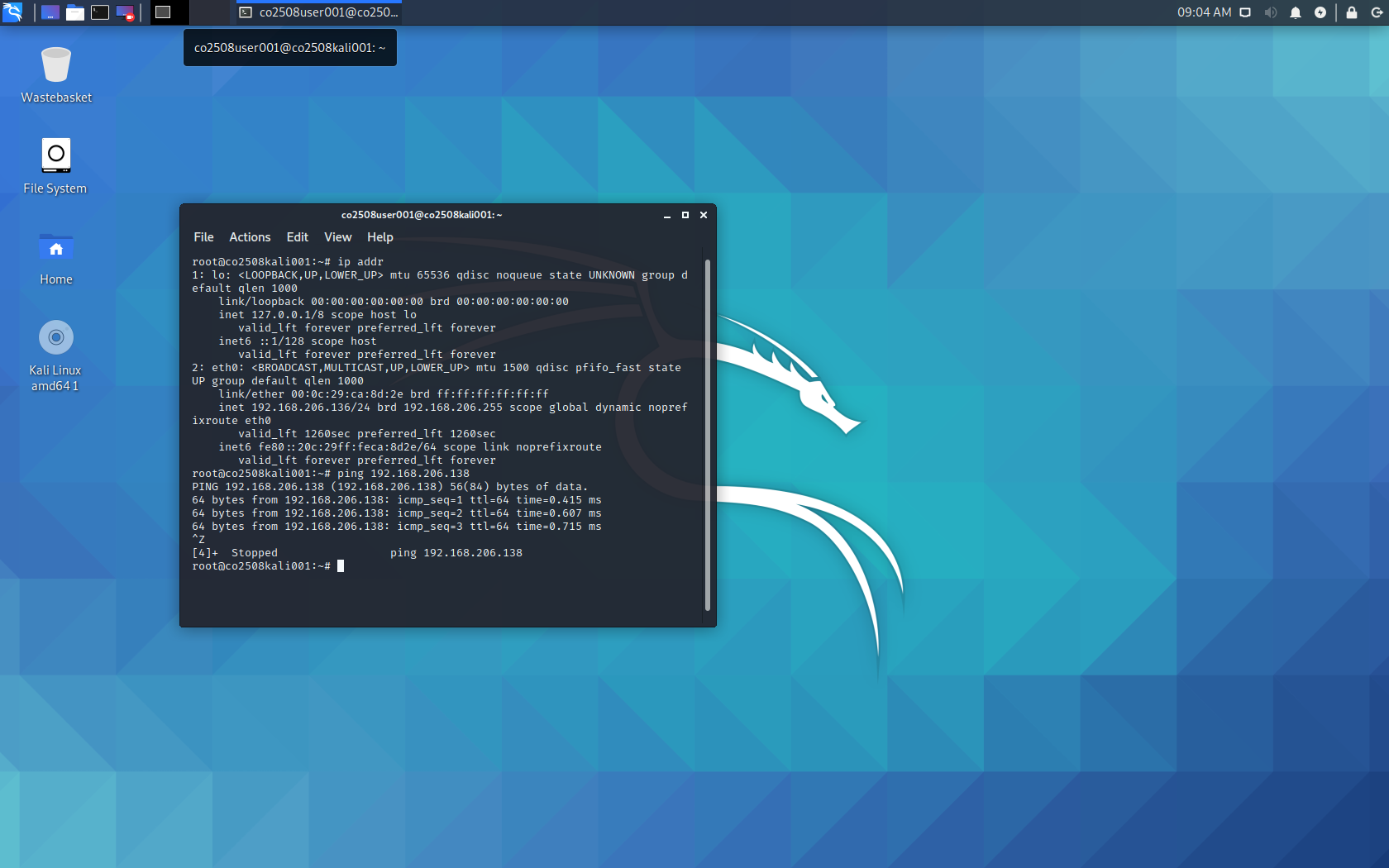
During this worksheet you will…

1. Run both virtual Kali computers
2. Make sure they can connect to each other with a PING command
3. Install the ‘uncomplicated firewall’ on Kali002
4. Set up some simple firewall rules
5. Test your firewall rules to see if they protect your host perimeter

### Part One – Running Kali

You should have done this at the end of your last worksheet – however, do it again just to make sure that nothing has changed since you last ran the virtual machines.

1. Start both of your virtual machines kali001 and kali002.
2. Log in to both machines
3. Obtain the IP address of both machines
4. Send a PING command to kali002 from kali001
5. Send a PING command to kali001 from kali002



1. Send a PING command to an IP address with a slightly wrong host address. For example, my kali002 IP address is 192.168.206.138 – so I will send the command

ping 192.168.206.139

this should fail. If it doesn’t fail then there is another host machine on this network – why?

**Note**: you can stop the PING command executing by pressing CTRL + Z

### Elevating Permissions to Super User

You probably need to be the super user to run some commands on your virtual machine.

There are different ways you can do this. The most ‘secure’ way of doing this is to precede every super user command with the ‘sudo’ command. This will force you to type sudo every time you want to elevate your permissions – and kind of acts like a circuit breaker in your brain, so that you are actively deciding the command to execute.

You can also put yourself into super user interactive mode by issuing the command

sudo -i

Which puts you as the superuser until you exit. The downside of this is that you will be executing all your commands (even the ones you type by mistake) with super user permissions.

I will leave it to your discretion whichever version you want to use. I won’t keep telling you to get super user permissions – I will expect you to know how to do it.

### Part Two – Enabling SSH

We are going to log in as a remote user from Kali001 to Kali002. We will use the SSH service to allow us to connect from Kali001 to Kali002. This is the ‘secure shell service’ and it listens to port number 22.

If you try to run this service immediately, it will fail.

Within Kali001 type the command

ssh [co2508user002@192.168.206.138](mailto:co2508user002@192.168.206.138)

you should receive a message saying the connection is refused.

In Kali002 issue the command

systemctl start ssh.service

Then go back to Kali001 and try to connect again

ssh co2508user002@192.168.206.138

It will ask you to enter a password, and might ask you if you are happy to continue connecting – you have to type in ‘yes’…once you have done this, you will be logged in to kali002 and any commands you enter will be executed on the other machine.

In Kali001 type ‘exit’ to log out of the secure shell session.

exit

### Part Three - Installing Uncomplicated Firewall

We are going to install the ‘uncomplicated firewall’ on co2508kali002.

1. The first step should be to check if the uncomplicated firewall is already installed. I don’t think it should be – but let’s check anyway.

ufw status

If the software isn’t installed then it should say “command not found”.

1. Install the software by downloading and installing the software

Modern versions of Linux have a neat little utility that will automatically download and install everything that we need – this makes installing software quite easy! To install the uncomplicated firewall issue the command…

apt-get install ufw

this will look on the Internet to download all the files necessary for the software to run; it will download these files, install them, and make the program ready to operate.

1. Check the status of ufw

Issue the command

ufw status

Note: if you get a message that the ‘command is not found’ – then you have forgotten to elevate yourself to the super user.

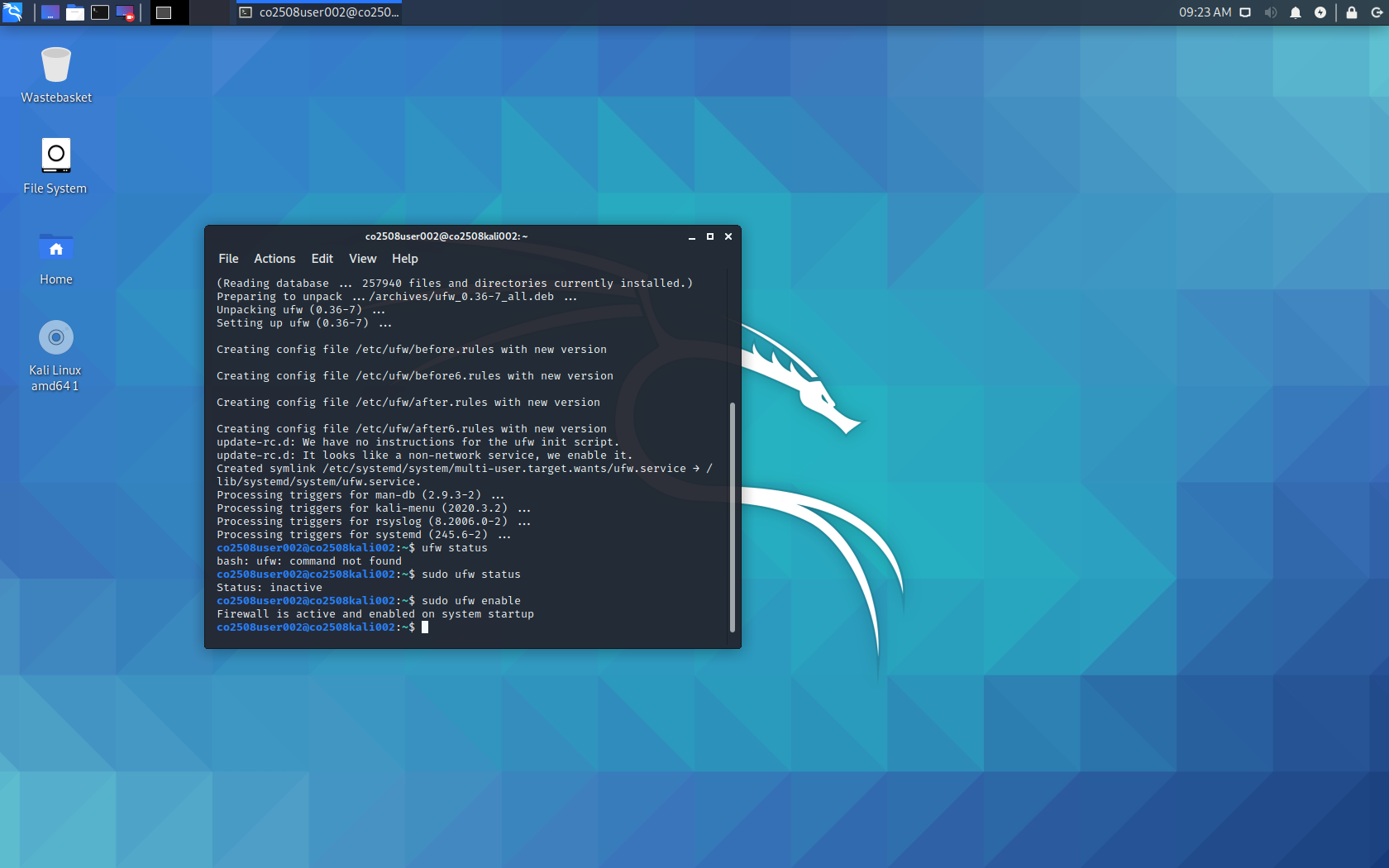
You should get a message saying that ufw is ‘inactive’.

1. Activate ufw so that it is running and protecting your host machine

Enter the command

ufw enable

the screenshot below is just the commands as I have explained in the steps above.



### Part Three – Creating Firewall Rules

We are going to set up the firewall to protect the perimeter of the co2508kali002 host machine. To do this we are going to edit some of the firewall rules.

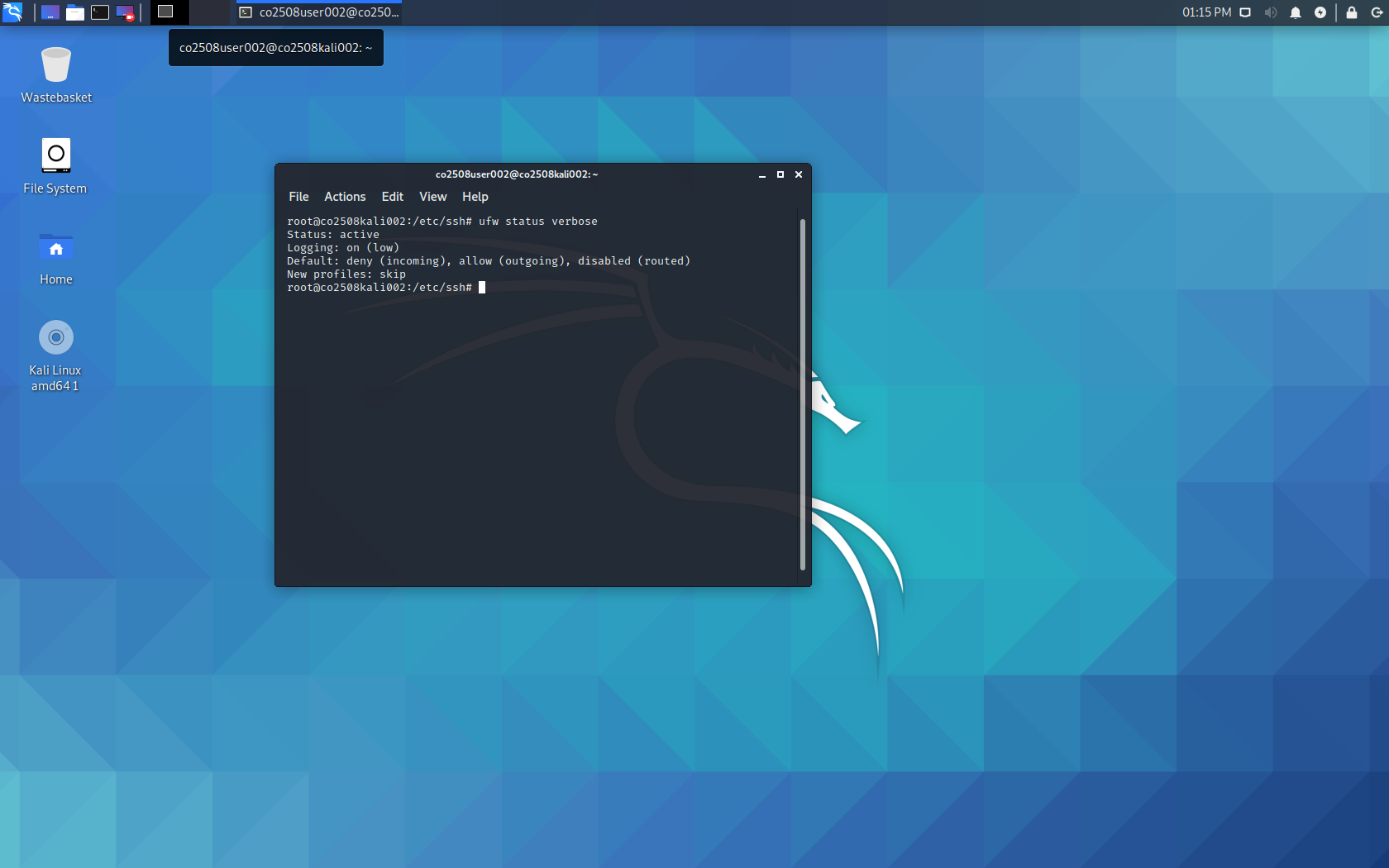
1. From Kali001 try to connect to Kali002 using the SSH command we issued previously.

ssh co2508user002@192.168.206.38

in this situation, we have the SSH service running and we have the UFW firewall running. When you issue this command, if you have everything set up correctly, it will sit doing nothing until it eventually times out. If you get bored of waiting for it to time out you can press CTRL + Z.

1. See if you can see why this is happening by entering the following command on Kali002,

ufw status verbose



We haven’t set up any rules in our firewall yet – so what is actually happening? Can you figure it out by looking at the output from the verbose output above?

1. On Kali002 type in the following command…

ufw allow ssh

Try to make a secure shell connection to Kali002 from Kali001.

1. Have a look at what has changed in the firewall rules by issuing the command,

ufw status verbose

When we issued the ‘allow’ command above, we added a rule that allowed incoming connections onto port number 22. UFW comes knows about some protocols and their default port numbers, and you can simply refer to the ‘app’ by name rather than get bogged down in port number details.

1. To see a list of apps that UFW recognises you can issue the command

ufw app list

1. You can stop this rule from working

ufw deny ssh

Try to connect from Kali001 to Kali002.

1. Let’s remove this rule entirely, enter the following commands…

ufw status numbered

Find the numbers for the rules you have added (if you haven’t added any other rules, they should be numbered 1 and 2).

ufw delete 2

ufw delete 1

Why did I delete rule 2 before deleting rule 1?

1. We can add rules manually

ufw allow 22/tcp

This requires us to know the port number and protocol; although we could also issue

ufw allow 22

which would block port 22 for TCP and UDP at the same time.

### Part Four – Advanced Tasks

If you don’t want to do these advanced tasks then jump to part five below.

Enable SSH on Kali001. Do not install or enable a firewall on Kali001.

Test it by connecting from Kali002 to Kali001.

Add an egress filter on Kali002 that stops people from connecting to SSH on other computers (e.g. block Kali002 from connecting to Kali001).

Test it by SSH from Kali001 to Kali002, and then connecting from this back to Kali001 with SSH.

Remove all rules.

Block JUST incoming connections when they come from Kali001 (the IP address of Kali001).

Find out about ‘bogons’. How might you setup a firewall to block bogons?

A useful website can be located by [clicking on this link](https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-14-04). It contains a whole range of different commands for setting up rules in UFW.

### Part Four – Making Your Computer Stable

It is important that you return your computer to a position where you understand what is enabled/disabled – so that next time you attempt to play with the security settings it is back to a stable position.

This exercise has enabled UFW and enabled the SSH service. To return to our previous position we should disable these from running. To do that, issue the following commands…

systemctl stop ssh.service

ufw disable