**Practical 5**

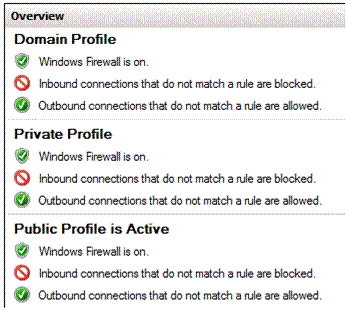
**Objectives: To explore Windows firewall, fwbuilder for Linux firewalls**

We will use the Windows Firewall with Advanced Security, and Firewall Builder to manage the iptables firewall on a Linux system.

**Exercise Exploring Windows Firewall with Advanced Security**

In Win10 VM:

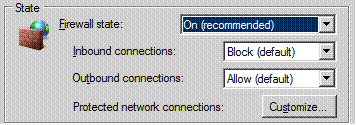
1. In the Cortana search textbox, type “firewall”. Click on “Windows Firewall with Advanced Security”.
2. You will see the configuration of the three possible profiles for the Windows Firewall (see following diagram).



This profile is currently active

Question : Which profile is currently active on your system?

1. In the right-hand frame, click on Properties.
2. Click on the tabs to see the different configuration for Domain Profile, Private Profile and Public Profile.
3. Take note of the default policies for Inbound and Outbound connections for the different profiles (see following diagram).



The action to take when connections do not match any of the firewall rules

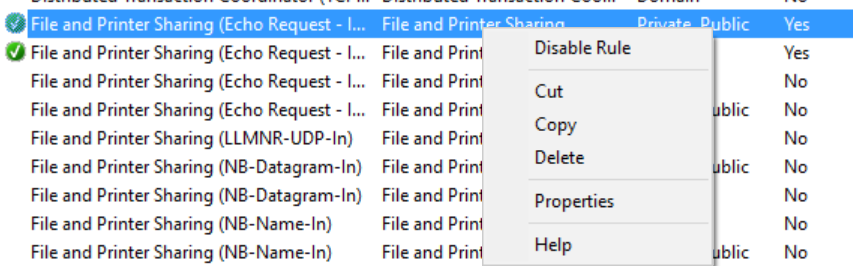
1. Click Cancel.
2. Close the Windows Firewall Management console.

**Exercise Restricting incoming ICMP packets to certain computers only**

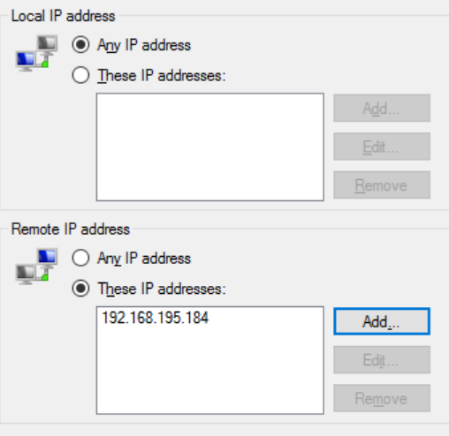
In a previous practical, you had configured the Windows Firewall to allow incoming ICMP packets, so all systems can ping to your Win10 VM. You will now modify the rule to allow only certain systems to ping your Win10 VM.

In Win10 VM:

1. In the Windows Firewall with Advanced Security, in the left hand pane, click on Inbound Rules.
2. Look for the rule “File and Printer Sharing (Echo Request - ICMPv4-In)” for the Public profile. You had enabled this rule in a previous practical.
3. Test that both your Host PC and Kali VM (or web-server2 VM) can ping your Win10 VM.
4. Right-click on the rule (Public profile) and choose Properties. (see following diagram)

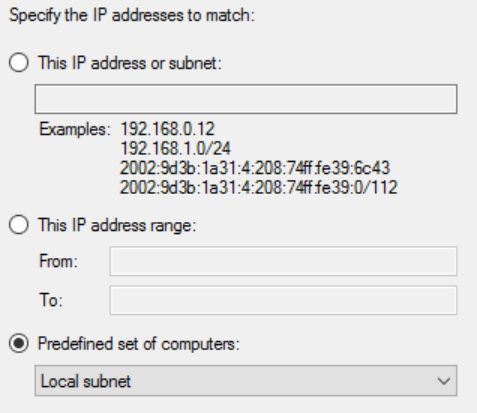


1. Click on Scope tab.
2. Under Remote IP Address, remove “Local subnet”. Add the IP address of your Kali VM (or web-server2 VM)



Change to the IP of your Kali VM

1. Click OK.
2. Test that your Kali VM (or web-server2 VM) can ping to your Win10 VM, but your Host PC now can not ping to the Win10 VM.



To reset back

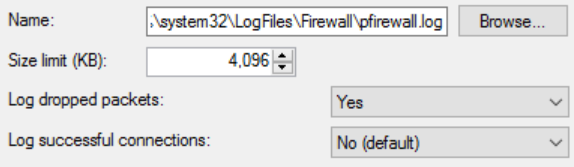
1. Right-click on the rule again and choose Properties.
2. Click on Scope tab.
3. Under Remote IP Address, remove your Kali IP. Click Add. Select “Predefined set of computers” and choose “Local subnet”.
4. Click OK.

**Exercise Configure logging for Windows Firewall**

In Win10 VM:

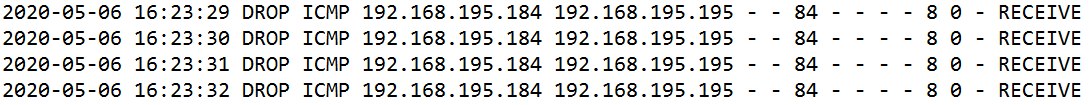
1. In the Windows Firewall with Advanced Security, in the left hand pane, click on “Windows Firewall with Advanced Security”.
2. In the right hand pane, click on Properties.
3. Click on the Public Profile tab.
4. Under Logging, click Customize.
5. Set “Log dropped packets” to “Yes”.

Location of Log File



Check this to start logging packets that are blocked by the firewall

1. Take note of the location of the Windows Firewall log file.
2. Click OK. Click OK.
3. Disable the rule (Public profile) that allows incoming ICMP packets.
4. From your Host PC or Kali VM, try to ping the Win10 VM. The ping packets should be blocked as you have disabled the rule in the last step.
5. As the Windows Firewall log file is locked by the Windows Firewall process, copy the Windows Firewall log file to another folder. Open the copy with a text editor like Notepad. The packets that have been dropped will be listed.



If the date and time of the logged packets are wrong, check the timezone of your Win10 VM.

1. Enable the rule (Public profile) to allow incoming ICMP packets again.
2. Disable the logging for your Windows Firewall (in case the logs created take up too much space)

**Optional Task**

What happens for Windows Firewall with Advanced Security, if there is a rule allowing a type of network traffic and another rule blocking the same type of network traffic?

Try it out! There is already a rule enabled to allow incoming ICMPv4 packets. In Inbound rules, create New Rule -> Custom Rule to block ICMPv4 traffic.

Remember to delete or disable the rule that you have created to block ICMP.

Conclusion : For firewalls with rules that are not numbered, usually the Deny or Block rules take precedence.

**Exercise Using fwbuilder to manage Linux iptables**

Description:

Iptables is used to implement packet filtering on many Linux systems. System administrators can configure the iptables directly on the Linux command line.

Firewall Builder (fwbuilder) is a GUI application that can be used to configure and manage different types of firewalls, including iptables.

Kali Linux with fwbuilder

Red Hat Linux running iptables

We will be installing fwbuilder on our Kali Linux and use it to configure the iptables firewall on a Red Hat Linux system.

**Set up Red Hat Linux image with a running Web Server**

1. Go to C:\BaseImages and extract the Red Hat Enterprise Linux 6 (RHEL6) virtual machine rhel6.7z to your D:\EHD folder. You can also download rhel6.7z (about 700MB) from the download links.
2. Check that the Red Hat Linux VM is in NAT networking and power it on.

In RedHat Linux:

1. Login as user “root” with password “redhat”.
2. Go to Applications->System Tools->Terminal to start a terminal.
3. View the IP address of your Red Hat Linux system by running the following command. Check the name of network interface (eth0, eth1, etc)

ip addr

1. The Apache Web Server has already been installed in this image. Start the Web Server by running the following command.

service httpd start

1. Create a default home page for the Apache Web Server by using a text editor to create the file /var/www/html/index.html and enter the following contents.

Or you can change to any contents you like

This is my Web site!

1. Open a Web Browser and browse to http://*ip\_address* where *ip\_address* is the IP address of your Red Hat Linux image. You should see your web page.
2. Create a new directory to store the Firewall Builder configuration files by running the following command

mkdir /etc/fw

**Test that Kali can SSH to RHEL6**

After using Kali to configure the firewall rules for RHEL6, Kali will use SSH to push the firewall rules to RHEL6. Test that Kali is able to establish a SSH connection with RHEL6.

In Kali

1. Start a SSH connection to RHEL6.

Change to your rhel6 IP

ssh root@*rhel6-IP*

1. As this is the first time, you are doing a SSH connection to the RHEL6 from your Kali, you will see a message about the key fingerprint of the host. Type “yes” to continue connecting.
2. Type “redhat” for the password. You should be logged in successfully to the RHEL6.
3. Type “exit” to close the connection.

**Install fwbuilder on Kali Linux**

In Kali

1. Download the fwbuilder packages from Brightspace or from the same Dropbox link, under Topic 5 Firewalls. You can also use “apt install fwbuilder” to download and install the packages.
2. To install the packages, run the following command.

sudo dpkg -i fwbuilder-common\_*NNNN*\_all.deb where NNNN is the version number

sudo dpkg -i fwbuilder\_*NNNN*\_amd64.deb

1. Start Firewall Builder by running “fwbuilder” in a terminal.
2. Close the Quick Start Guide if it starts.

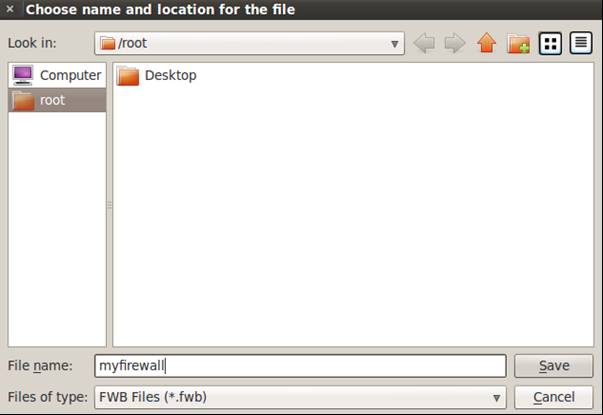
**Use fwbuilder to set up a firewall configuration**

In Kali

1. In a terminal, check that you can ping to your Red Hat Linux by running “ping *ip\_address*” where *ip\_address* is the IP address of your Red Hat Linux.
2. Open a Web Browser and browse to http://*ip\_address* where *ip\_address* is the IP address of your Red Hat Linux image. Check that you are not able to view the web site of your Red Hat Linux. This is because the default iptables setting of your Red Hat Linux is not allowing anyone to connect to the Apache Web Server.
3. In Firewall Builder, click on Create New Firewall.
4. Give a name for your new firewall object, eg myfirewall.
5. For firewall software, choose “iptables”.
6. For OS, choose “Linux 2.4/2.6”. (see following diagram)



1. Click Next.
2. Select “Configure interfaces manually”. Click Next.
3. You do not need to specify any network interfaces. Click Finish.
4. From the File menu, choose Save As. Save your new firewall setting. You can call the file “myfirewall”. (see following diagram)



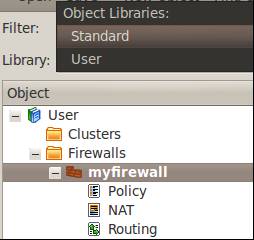
Give a name for your firewall config file

Save in a directory on Kali

**Add a rule to allow SSH connections**

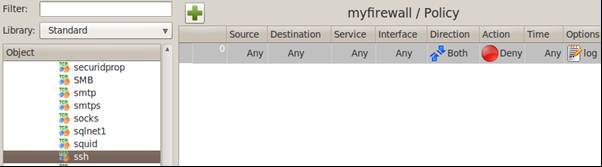
In Kali

1. Right-click in the empty rules panel and choose Insert New Rule.
2. From the Library drop-down box, select Standard. (see following diagram).



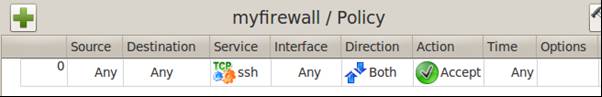
Click on Library and choose Standard

1. Expand Services. Expand TCP. Look for “ssh”. Click on “ssh” and drag it to the Service column of the new rule. (see following diagram).



Drag “ssh” to the Service box

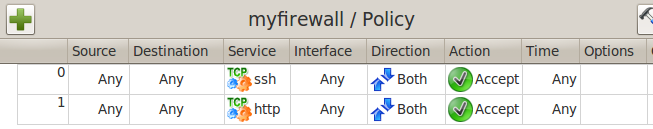
1. In the new rule, right-click on the Deny Action and change it to Accept.
2. In the new rule, right-click on the log option and change it to Logging Off. The rule would look like the following.



**Add a rule to allow HTTP connections**

In Kali

1. Right-click in the empty portion of the rules panel and choose Insert New Rule at the Bottom.
2. From the left-hand Objects panel, expand Services. Expand TCP. Look for “http”. Click on “http” and drag it to the Service column of the new rule.
3. In the new rule, right-click on the Deny Action and change it to Accept.
4. In the new rule, right-click on the log option and change it to Logging Off. The rule would look like the following.



**Add a rule to deny all other traffic**

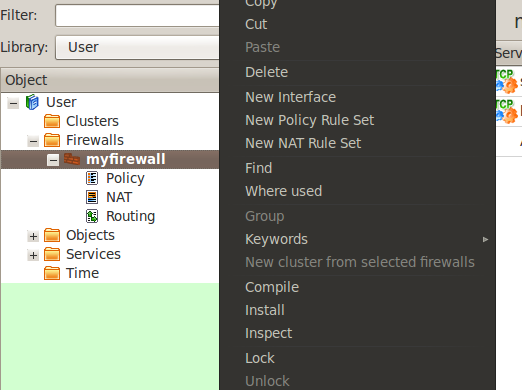
In Kali

1. Right-click in the empty portion of the rules panel and choose Insert New Rule at the Bottom. By default, the new rule added will deny all other traffic.

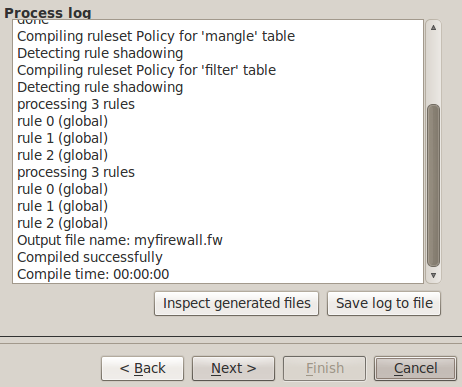
**Compile and install the rules to your Red Hat Linux**

In Kali

1. From the Library drop-down box, select User.
2. Right-click on myfirewall and choose Install. (see following diagram)



1. Click Next to start compiling the firewall.



1. If you see the “Compiled successfully” message like the above diagram, click Next.
2. Enter the login credentials for your Red Hat Linux – “root” for user name, “redhat” for password. Enter your Red Hat Linux IP address for the address. Select Verbose. (see following diagram.



1. Click Install.
2. If you see a message about the “authenticity of the host can’t be verified” like the following :



This will happen if the Kali user account running Firewall Builder is doing a SSH connection to the target system for the first time, and Firewall Builder is unable to find the target’s SSH host key.

Return to the part of the practical where, from Kali, you do a SSH to RHEL6. Once the SSH connection is successful, exit the connection, and try to Install the Firewall Builder rules again.

1. If you see a “Firewall policy successfully installed” message, click Finish.

**Test the rules**

In Kali

1. Open a Web Browser and browse to http://*ip\_address* where *ip\_address* is the IP address of your Red Hat Linux image. Check that you can view the web site of your Red Hat Linux.
2. Test if you can ping your Red Hat Linux image. You should not be successful because you have not added any rules to allow ping packets.

**Task**

Add a rule to allow anyone to ping your Red Hat Linux (ICMP protocol). You will need to compile and install your firewall rules to your Red Hat Linux again.

After adding the rule to allow anyone to ping your Red Hat Linux, your firewall rules may look like the following :

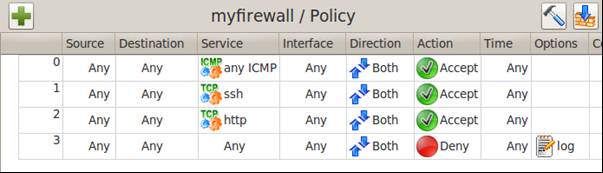
Rule 0 : Allow ICMP traffic (both directions)

Rules 0 to 2 can be in any order

Rule 1 : Allow SSH service

Rule 2 : Allow HTTP service

Rule 3 : Deny all other traffic

****

**Exercise Setting the Direction for firewall rules**

Description:

Currently the ICMP rule applies for both directions. This means the rule allows both your Red Hat and Kali images to ping each other.

ICMP traffic

Kali Linux with fwbuilder

Red Hat Linux running iptables

ICMP traffic

In Kali

1. Using Firewall Builder, change the Direction of the ICMP rule to Inbound. (see following diagram)



1. Install the modified rules to your Red Hat Linux image.

**Test the rules**

In Kali

1. Test if you can ping your Red Hat Linux image. You should be successful.

In Red Hat Linux

1. Test if you can ping your Kali image. You should not be successful as the ICMP rule now only accepts incoming ICMP packets. Outgoing ICMP packets are blocked.

Inbound ICMP traffic

Kali Linux with fwbuilder

Red Hat Linux running iptables

Outbound ICMP traffic

**Task**

Modify the Direction of the HTTP rule so that other systems can access the Web Server on your Red Hat Linux image but your Red Hat Linux can’t access web sites on other systems. (for eg, on Red Hat, try to browse to your webserver virtual machine)

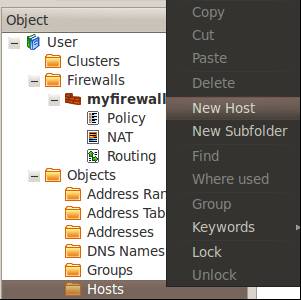
**Exercise Setting the Source or Destination for firewall rules**

Description

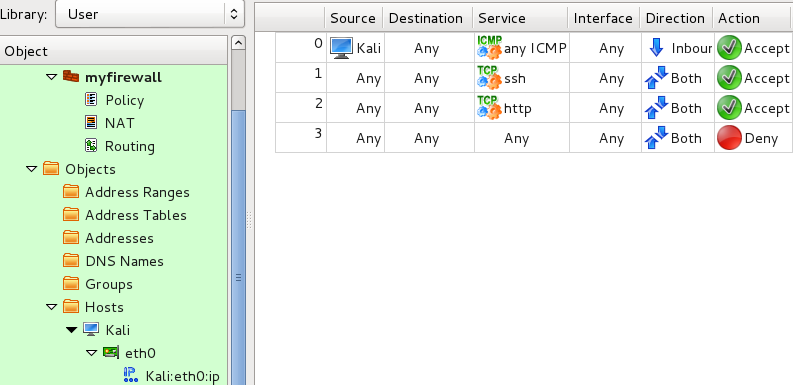
You will now specify that only your Kali system can ping to the Red Hat Linux. You will need to create an Object to represent your Kali system.

In Kali

1. Run “ifconfig” or “ip addr” to check the IP address and Netmask of your Kali. Also note the name of your network interface, eg “eth0”.
2. Using Firewall Builder, in the left-hand Object panel, expand Objects.
3. Right-click on Hosts and choose New Host (see following diagram)



1. For Name of New Host Object, type “Kali”. Click Next.
2. Select “Configure interfaces manually” and click Next.
3. For Interface Name, type the name of your network interface, eg eth0
4. Click on Add Address.
5. Enter the IP address and Netmask of your Kali. Click Finish.
6. From the Objects panel, drag the Kali icon to the Source column of your ICMP rule. (see following diagram)



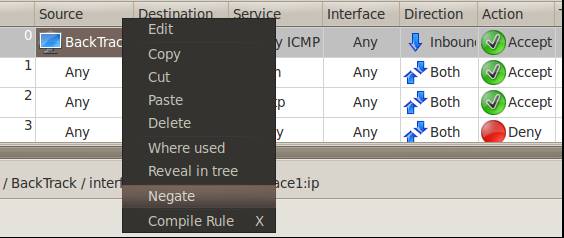
1. Install the new rules to your Red Hat Linux.
2. Test that your Kali can ping your Red Hat Linux. Other systems like your Host PC or webserver are not able to ping the Red Hat Linux.

**Exercise Using the Negate option**

Description

You will now specify that only your Kali system can NOT ping to the Red Hat Linux.

1. In the Rules panel, in your ICMP rule, right-click on Kali and choose Negate. (see following diagram)



1. Your ICMP Rule now means : Any IP except for your Kali can ping the Red Hat Linux system.



1. Install the new rules to your Red Hat Linux.
2. Test that your Kali can NOT ping your Red Hat Linux now. Other systems like your Host PC or webserver can ping the Red Hat Linux.

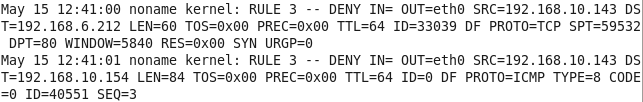
**Exercise Viewing Firewall Logs on Red Hat Linux**

Description : By default, iptables on Red Hat Enterprise Linux 6 will log into the file /var/log/messages

In Red Hat

1. Run “tail -30 /var/log/messages” to view the last 30 lines of /var/log/messages.

The log entries will appear like the following.



Packets that have been denied by the firewall are logged down

**Exercise Setting rules for firewalls with more than one network interface**

Description:

Firewalls that are connected to several subnets will have more than one network interface. Rules can be set for specific network interfaces of the firewall, or for specific subnets.

The following firewall has 3 network interfaces :

eth0 with a dynamic IP address that will be assigned by the Internet Service Provider (ISP), connected to the Internet

eth1 with IP address 192.168.1.1, connected to the company’s internal network

eth2 with IP address 192.168.41.1, connected to the DMZ subnet

Internet

eth0



eth2

DMZ Subnet

192.168.41.0/24

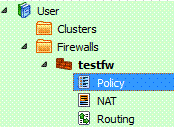
eth1

Internal Network

Subnet 192.168.1.0/24

In Kali

1. Download the fwbuilder file testfw.fwb from Brightspace. Open it with Firewall Builder. Expand User->Firewalls->testfw and double-click on Policy to view the rules.



Answer the following questions :

1. Does Rule 0 or Rule 1 allow traffic on the loopback interface? **Rule 1 allows.**
2. What is the IP address range for the subnet specified in net-192.168.1.0? **192.168.1.0**/24 with subnet mask 255.255.255.0
3. Can the system at 192.142.9.2 do a SSH connection to the firewall?  **NO**
4. Rule 5 allows a Mail Server in the DMZ to connect to a Mail Server in the internal network.
5. What is the IP address of the Mail Server in the DMZ?

**192.168.41.10**

1. What is the IP address of the Mail Server in the internal network?

**192.168.1.10**

1. Which rule will allow users in the internal network to browse Internet web sites? **Rule 8**

*(answers found on Brightspace)*

**Exercise Firewall Builder User Guide**

1. Go through the Firewall Builder User Guide (found on Brightspace) and do the Online Quiz for fwbuilder for General Performance marks.

*End of Practical*