# Purpose of lab

The purpose of this lab is to note the effect on internet communications when using a firewall to restrict connections. The lab will use a virtual machine (VM) installed on one of the lab computers. A Linksys router will inserted between the lab computer and the lab network. After establishing connection through the router, the student will then restrict communication by setting up rules to block certain traffic. Traffic affected will be HTTP (port 80) and ssh (you must look up the port).

The *New Linux Tricks* part for this lab will give more insight into the use of groups and permissions.

***Note: Items marked with a \*\* must be documented in your lab report.***

# Equipment

* Workstation with VM
* Linksys Router
* Cables

# Pre-Lab Investigation

#### Research *ssh*

* What is ssh?
* Why it is used?
* What port does it use?

Q1: Answer the above questions in your report. A short paragraph at a high level will do.

# Lab Procedures

## Part 1 - New Linux Tricks - Groups

The first part is to familiarize you with a new aspect of Linux. This segment will be creating new groups for your Debian VM. If you still have the new users you created in Lab 4 use them. If not create 2 new users before proceeding.

Files of interest:

* /home
	+ directory for users’ home directories (default location)
* /etc/passwd
	+ file with user ids and attributes definitions
* /etc/shadow
	+ file with “secure” password and attributes definitions
* /etc/group
	+ file with the group ids and attributes
* /etc/gshadow
	+ file with security info for groups

Before creating the new group ids check the contents of the above directory and files. Find your ID and the root ID in each of them. Note the group ID has group ids to match the user ids you created. Get a copy of the file and directory contents.\*\*

DO NOT use screen captures to document text data!

**Hint:** for getting a listing of the contents of the /home directory into a file try:
 ls /home > home1.txt
This will redirect the listing of the /home directory to a file named home1.txt. You can then copy that file to a thumb drive to include the data in your lab report.

**Hint:** for putting data into your report you can copy the files to your USB and then in the report copy the lines of interest from the file to your report.

### Create a new group using the GUI:

Gnome 3 no longer installs Users and Group as part of the base programs. To install Users and Groups:

1. Under *Applications* 🡪 *Administration* select *Synaptic Package Manager*
2. Enter the root password for your VM
3. In *Quick Filter* enter *gnome-system-tools*
4. Click the box for  *gnome-system-tools* then select *Mark for Installation*
5. Click on the green *Apply* check mark
6. Click on the *Apply* button
7. When the software has installed click the *Close* button
8. Close Synaptic

You can now use the newly installed *Users and Groups*. Be sure to have your users created before creating your group.

1. Select Users and Groups (In Applications 🡪 System Tools 🡪 Administration 🡪 Users and Groups
2. Enter the root password when prompted
3. Click on the Manage Groups button
4. Click on Add
5. Enter a Group name
	1. Enter root pw if asked
6. Enter the Group Name
	1. Add members from the list at this point
7. Click OK, then Close
	1. You can check if it worked by clicking Manage Groups again and see if your group is listed
8. Look at and get a copy of the relevant file(s) and directory contents (especially the group file) again.

### Create a new groups and associate users using the CLI:

In the commands below change the newGroup, existingGroup and newID to names unique for yourself

1. Start a terminal
2. Switch to root access
3. Create a new group
	1. addgroup newgroup
4. Set an existing user to a group
	1. usermod –a –G group userID
5. Look at and get a copy of the file and directory contents again.
6. Create a new user and put it in an existing group
	1. useradd –G existingGroup newID
	2. passwd newID
7. Look at and get a copy of the file and directory contents again.

**Q2:** Discuss what files and directories were changed as the new groups and users were added in the above steps.

## Part 2 -Firewalls

### Preparation

#### Reset the router to factory defaults

There are two ways to **reset** the **Router's factory defaults**:

1. Press the **Reset Button** for approximately **10 seconds ~ 30 seconds.** On some routers you may need to hold the Reset Button while repowering.
2. [Restore the Factory Defaults](http://www.linksysdata.com/ui/WRT54G/v5/1.00.2/Factory-Defaults.htm) from the **Administration tab** in the **Router's Web-Based Utility**.
	* The WRT54G may ask permission to reset

After resetting the user name and password are also reset. To access: leave the user name blank, the password is ***admin***.

#### Familiarize with the router UI (on-line or in the Lab)

The following website (on the internet) has emulations of the routers used in the lab:

* LinkSys WRT54G:[**http://www.linksysdata.com/ui/WRT54G/v5/1.00.2/Setup.htm**](http://www.linksysdata.com/ui/WRT54G/v5/1.00.2/Setup.htm)

In this lab you will connect the router between the pc and the lab network. After the router has been inserted the VM must be restarted establish connection via DHCP in the router. You will use your Debian VM for this lab.

* **Note:** For Debian, see Lab 3 and Lab 4 Addenda on how to change to modify the interfaces file.
	1. Make sure that DHCP is enabled and if a static address is defined comment out appropriate lines
* Move the Ethernet cable from the back of the Lab workstation to the router’s *WAN* port (may also be labeled *Internet*). This connects the wall port to the routers WAN port.
* Add a cable from the Lab Computer to one of the switched ports (1-3) of the router (connect the pc to the router)
* Restart the router by unplugging and re-plugging the power
* Optional if having major problems:
	1. Restart the Lab computer and then start the VM
* Check for a default gateway to your route table for your VM using the route command
	1. It should be 192.168.1.1
	2. If it does not exist add default gateway for 192.168.1.1
		1. route add default gw 192.168.1.1

Q3: What does the gateway do? Look it up and give a brief answer. This concept will be important for next week’s lab!

##### Check the IP addresses assigned to the VM and to the WAN side of the router

* \*\* Check the IP address assigned to your VM by the Linksys router. It should be 192.168.1.nn where nn is typically between 100 and 150 for the Linksys routers.
	+ From your VM do an ***ifconfig*** and note the VMs IP configuration
* Open a browser (Ice Weasel) and browse 192.168.1.1, to check the router configuration. You will need to log into the router to do this:
	+ You will first see a security logon prompt
	+ Leave *user id* blank
	+ Default password for the router is***admin***
* Check what IP address was assigned to the WAN port by DHCP server on *hades.lab*
	+ *\*\** Capture the information for your report

##### Check to see if the hades servers can be browsed:

* Open a browser (Ice Weasel) and this time browse (try both the domain name and the IP addresses):
	+ lab302-web.hades.lab (172.16.1.250)
	+ lab302-repo.hades.lab (172.16.1.251)
* A small web page should show for each should appear indicating the browser can connect to the web servers
	+ \*\* Capture one of the browsers to include in your lab report. (Screen capture allowed)

##### Ensure the hades server can be pinged:

* Open a command line terminal
* Ping both172.16.1.250 and 172.16.1.251
* Break the ping after a reasonable number of pings
	+ \*\* Capture the ping activity to include in your report, use file redirection, do NOT use screen capture!

#### Block HTTP service

In this step the student will double-check to make sure the browser still can browse the data on the **hades servers** (hades.lab). The student will then configure the Linksys router to block traffic on port 80, and then notice the server can no longer be browsed. Finally the restriction will be removed and the server will be browsable again. Ping will be used throughout the lab to show that a connection is kept throughout the entire lab, only the HTTP service is blocked.

**Goal:** block the HTTP service from lab302-web.hades.lab (172.16.1.250) and lab302-repo.hades.lab (172.16.1.251) from the local VM

##### Setup the environment

Note: The following instructions are for the WRT54G, steps are similar for the WRTG54L, BEFSX41 and some others. Also, the steps may vary slightly depending on the vintage Linksys router you get.

* If needed, boot and login to the VM, then use ***ifconfig*** to check the IP for VM.
	+ It still should be 192.168.1.nn as seen in the Preparation step.
* Open a web browser input the router’s IP: 192.168.1.1. You may need to re-log into the router.
* Open a web browser input browse the *hades* servers (see above) (not 192.168.1.1), and check that the *hades* servers can still be browsed
* On the browser open to the Linksys router go to the “Access Restrictions” tab, create a new policy to block “HTTP” service
* Make sure the following is set:
	+ Status: Enable
	+ Enter policy name: for example “blockHTTP”
	+ Click “Edit List of PCs”, you will edit the PCs affected by this policy
	+ Enter the IP of your VM (use ***ifconfig*** if you have forgotten the address) in “Enter the IP Address of the PCs” field, and then check “Save Settings”
	+ In “Blocked Services”, choose the “HTTP” option
	+ Select “Save Settings” to enter the policy
	+ \*\* Document the changes with a screenshot
* This blocks your VM from using port 80

Test the networ**k**

* On the VM, open a terminal window and ping both IP addresses 172.16.1.251 and 172.16.1.250 (You may also try the fully qualified domain name). Both pings should still work
* Use the Ice Weasel browser to try to view the web serves on both servers again.
	+ Nothing should happen, except perhaps for a timeout.
* \*\* Document the above two steps above for your report. A screen capture is not required, you may describe what happened.

***Important: After testing that blocking port 80 worked remove the rule***.

##### Create a rule to only block lab302-web.hades.lab

* Create a new rule and label it “block lab302-web.hades.lab
* This time set a range of PCs to be blocked (e.g. 1-254)
* In Website Blocking by URL address add 172.16.1.250
* Save the settings
* Try to browse 172.16.1.250, 172.16.1.251, lab302-web.hades.lab and lab302-repo.hades.lab
* Next, change the Website Blocking by URL address to lab302-web.hades.lab
* Again, try to browse 172.16.1.250, 172.16.1.251, lab302-web.hades.lab and lab302-repo.hades.lab
* \*\* Document what happened. Which addresses were blocked and which worked? Why?

#### Block *ssh*

Using the experience from blocking http above the student will now block a login using ***ssh***. For this exercise the student will only need to attempt an ***ssh*** login. After ***ssh*** is blocked the student will not see a response from an attempt to log in the**hades server**. The command to login using ***ssh*** is:

***ssh*** 172.16.1.250

You should see a response from**hades server** after asking to log in. That shows you have tried to access the ssh port. You don’t need to continue, use <ctrl>+C to quit. \*\* Document for your report

Set up the router to block ssh using its port. For this step of the lab it is your responsibility to find and document the port used by ***ssh***. After ***ssh*** is blocked retry the previous command to login using ***ssh***. You should get no response. Do a ping before and after the ***ssh*** block is done to show there is a valid connection. \*\* Document for your report

**Optional:** try a block of ssh while also blocking HTTP.

##### Note the effect of NAT when accessing hades.lab (this is the lab network)

\*\* Comment on how NAT allows the local network to access the “global” network. Does the workstation act differently? If so how? Hint: compare the IP address assigned when connected to the router instead of directly to the lab network.

### Tips:

* You will need know which port ssh uses before starting the lab. **Investigate before the lab!**
* In "Blocked Services", you may need to define a new service. Click "Add/Edit Services" button.
* With this new service you can do something just like HTTP block.
* Note that some browsers will cache (that is keep a local copy) of a web page. If that occurs, try reloading, or stop and restart the browser to get the latest copy of the web file. lab302-web.hades.lab default page will show a new “lucky number” for every time it is accessed. If the page is cached the numbert will not change

Items noted with a \*\* are the key concepts for this lab. Pay special attention to what is done at these steps and why.