### Preamble

You must read the sections before Parts 1 – 4 before turning on your computers. Failure to start properly will result in running incorrect software and being unable to complete the lab.

Do not start your machine until you have read the ***Procedure*** section below.

### Environment

We are again using the virtual environment provided by VMware Workstation to set up a virtual network of computers. The Ubuntu machine UbuntuServer hosts the server for DHCP(isc-dhcp-server), DNS (bind9) and HTTPD (Apache2). The two Windows PE machines will be used to test the firewall.

### Aims

LAN Segment 1

WINPE2

UbuntuServer

UbuntuServer communicates with outside world on eth0 interface via NAT on the host PC

Internet

Host PC

VMWare environment

WINPE1

### Using IPTables we have one aim in mind, to protect the servers that we have configured in previous labs.

### Tools

Sudo will give you elevated privileges to run commands. On Ubuntu, these privileges are highly restricted. You may need to invoke elevated privileges by typing sudo ifconfig, this will allow access to sudo for a short while. You will probably need to do this every few minutes during the lab. A painful work-around, but it does work.

Ipconfig (on Windows) and ifconfig (on Linux) will show us the network configuration on our VMs. On the Windows machines we can also control the acquisition and renewal of IP addresses and display other network information.

Checking Syslog is very useful to help you understand why things are not working. Print out the last part of the syslog file with the following to see why something is not working…

**sudo tail /var/log/syslog**

Check out the tail command on the man pages. The man pages are a useful source of information on how things work, for instance.

Debugging tips…

* Make sure that every virtual machine is on the virtual LAN, **Lan Segment 1**
* Make sure that DHCP is supplying the address of the DNS server to its clients, use ipconfig /all on the WinPE1 and WinPE2 machines.
* Check that bind9 is loading and operating correctly. Check /var/log/syslog, use ping and nslookup.
* Make sure that the Webserver is operating correctly. Check the URLs on both Windows machines.

To run a fresh copy of the QTWeb browser on WinPE1 and WinPE2, shut them down and re launch them from the terminal invoking \qtweb\qtweb.

### Web pages for help

For IPTables, there is lots of help all over the Internet. IPTables is one of the best tools in the system manager’s toolbox and is utilised very widely.

<http://www.help.ubuntu.com> as always has lots of help on how to do simple things to establish a firewall.

Ping can be used to try to reach a host. Either an IP address can be used or the FQDN can be used. If the FQDN is used, then the resolver of the DNS is utilised to translate the FQDN into an IP address.

nslookup can be used to test the DNS server from one of the PCs or from the Ubuntu server. You will get helpful messages I either case.

dig is another DNS testing utility which can tell you if your DNS server is working.

**Check out the *help.ubuntu.com* web pages for more information.**

### Procedure

1. Power on your computer and boot into the **Windows** tab.
2. Log onto the machine as usual with your student login/password.
3. Launch VMWare Workstation from the start menu.
4. There are three virtual machines to work with on this exercise, the UbuntuServer (a Linux VM) and the Windows PCs, named WINPE1 and WINPE2. Power up each of these machines in turn.
   1. If you are asked if you moved or copied any of the VMs, say “**I moved it**”.
   2. Cancel any other messages as they come by.
5. The UbuntuServer has an account set up on it with (all lower case)
   1. Username: student
   2. Password: **computing**
6. Make sure that your DHCP, DNS and Apache servers are working correctly, that the PCs are getting IP addresses and the address of the DNS server. Make sure that nslookup is resolving the IP addresses for UbuntuServer.computing.org, [www.computing.org](http://www.ca304.org) and ns.computing.org. If not then copy down the appropriate configuration files from loop.dcu.ie and install them. This should all be done before this lab commences.
7. **WARNING; Do not cut and paste into your firewall rules, there are hidden characters in some documents which will cause your firewall to fail and you will not be able to see these characters.**

### Marking

* 1 mark for establishing the basic firewall (as detailed below)
* 3 Marks: Establish a firewall with the following…
  + DHCP is enabled
  + DNS is enabled
  + Ping is enabled from WINPE1 only.
  + HTTP enabled from WINPE1 only
* 1 Mark: Error logging.

Subnet addressing (like 192.160.10.0\24 for example) must be used throughout the firewall, no individual IP addresses allowed for source machines and no specified ranges allowed either e.g. --src-range 192.168.1.100-192.168.1.200

Destination of 192.168.10.1 is allowed.

The following rule will cause IP Tables to generate a log record (do not cut’n’paste this line!): **Make sure that you can explain it! Check it out on the Ubuntu help site.**

**-A INPUT -m limit --limit 5/min -j LOG --log-prefix “iptables denied: “ --log-level 7**

Place this line at the correct point within your firewall rules file, so that a log record is generated only when a packet is blocked by your firewall rules. Log records are generated in the file /var/log/syslog.

Test your log rules by trying to access blocked services:

* HTTP traffic from WINPE1 only
* Ping from WINPE1 only
* Find the correct log record generated in the syslog file using gedit on WINPE1 (You may have to turn off line wrapping in gedit:
  + Edit > Preferences > Uncheck ‘Enable text wrapping’)

sudo gedit /var/log/syslog

Syslog Legend: SRC = source IP address

DST = destination IP address

SPT = source port

DPT = destination port

PROTO = protocol

Cut’n’paste the appropriate log entries that were generated trying to access blocked services:

* HTTP traffic from WINPE1 only (WINPE2 blocked)
* Ping from WINPE1 only (blocked from WINPE2)
* DNS blocked from WINPE2
* Allow DHCP from both machines

### Demo

* Have your myfirewall.rules file open
* Confirm these network services are or are not available by re-running ping and the browser.
* Logfiles

Part 0: Establish the basic Firewall

On the WINPE1 and WINPE2 machines, ensure that they can see the UbuntuServer machine.

**ping UbuntuServer.computing.org**

This ensures that it is reachable and that the DNS is working. Now start a browser on WINPE1 and WINPE2:

* + Point both browsers at: [www.computing.org](http://www.ca249.org/) (username/password: )

Confirm these network services are available by re-running ping and nslookup .

Lets create a file on the user home directory for the firewall rules and allow us to load them as needed.

**sudo touch myfw.rules**

Make it executable…

**sudo chmod 755 myfw.rules**

Now lets edit it (make sure that sudo has been run recently before doing the following).

**sudo gedit myfw.rules &**

Add the following iptables rules that will implement the default firewall policy.

iptables -F

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT

iptables -A INPUT –j DROP

The first rule flushes any existing iptables rules (good for when you edit them again)

The second rule allows the loopback interface

The third rule allows any already established connections (see netstat command for details)

The fourth rule drops all other incoming packets to our server.

Save and then run your iptables rules file:

**sudo ./myfw.rules**

Now the firewall is established, have a look at the rules as they are installed.

**sudo iptables –L –n -v**

Check out the switches “–L –N –v” using

**man iptables**

Confirm these network services are no longer available by re-running ping and nslookup and refreshing your browser page on WINPE2.

Part 1: Extended Firewall

Add ACCEPT rules to your firewall configuration script to re-enable access to

* DHCP (UDP and TCP ports 67 and possibly 68?) Be able to explain which ports you blocked.
* DNS (UDP port 53)
* HTTPD (TCP port 80)
* Ping (ICMP not UDP or TCP!) services **from our network only**! **Use CIDR mask notation.**

Use the iptables man page as a reference for writing your new rules

Save and re-apply your rules.

Confirm the network services are now available again by re-running ping and refreshing your QTWeb browser page on WINPE2.

Check that you have now access the [www.computing.org](http://www.ca304.org) website from any of the Windows VMs

Part 2: Extended Firewall – Fine Tuned

Adapt/Add your ACCEPT firewall rules to do the following:

* Only allow HTTPD traffic from WINPE1
* Allow Ping traffic from WINPE1 only
* The DNS should still work (test it with nslookup) from WINPE2 but not the browser.

Re-apply these changes.

Verify these new rules with **ping and nslookup** from WINPE1 and WINPE2

Confirm that you can still access the [www.computing.org](http://www.ca304.org) home page from WINPE1 but not from WINPE2.

Note: Ping uses the ICMP protocol and is routinely blocked on many Internet machines. Search the Web for help on allowing/blocking ping traffic on a network. You must enable echo-request type packets arriving at the server. Confirm that Ping now works from WINPE1 but not from WINPE2.

Part 3: Logging

The following rule will cause IP Tables to generate a log record **(do not cut’n’paste this line**! There are hidden characters here which you cannot see):

-A INPUT -m limit --limit 5/min -j LOG --log-prefix “your message here - iptables denied: “ --log-level 7

Place this line at the correct point within your firewall rules file, so that a log record is generated only when a packet is blocked by your firewall rules. Log records are generated in the file

/var/log/syslog

Test your log rules by trying to access blocked services:

* HTTP traffic only from WINPE1
* Ping only from WINPE1

Find the correct log record generated in the syslog file using gedit on WINPE1 (You may have to turn off line wrapping in gedit:

* + Edit > Preferences > Uncheck ‘Enable text wrapping’)

sudo gedit /var/log/syslog

Syslog Legend: SRC = source IP address

DST = destination IP address

SPT = source port

DPT = destination port

PROTO = protocol

Cut’n’paste the appropriate your log rules that were generated trying to access blocked services:

* HTTP traffic from WINPE2
* Ping from WINPE2

**Have your myfirewall.rules file open**

**and the last ping/nslookups**

**from WINPE1 and WINPE2**

[THE END]