LAB F QUESTIONS

1.3.1 iptables

**Chains** The rules in iptables are always parts of a chain. Chains can either be user-created or one of the built-in chains. In this lab, we will use three standard chains: INPUT, FORWARD, and OUTPUT. Explain which packets will pass through each of these chains:

* Input
  + This chain is used to control the behavior for incoming connections. For example, if a user attempts to SSH into your PC/server, iptables will attempt to match the IP address and port to a rule in the input chain.
* Forward
  + This chain is used for incoming connections that aren’t actually being delivered locally. Think of a router – data is always being sent to it but rarely actually destined for the router itself; the data is just forwarded to its target. Unless you’re doing some kind of routing, NATing, or something else on your system that requires forwarding, you won’t even use this chain.
* Output
  + This chain is used for outgoing connections. For example, if you try to ping howtogeek.com, iptables will check its output chain to see what the rules are regarding ping and howtogeek.com before making a decision to allow or deny the connection attempt.

**Operators** To change a chain, you need to use an operator. Look up the short form command for the following operators and explain what they do:

* Append
  + Appends the iptables rule to the end of the specified chain. This is the command used to add a rule when rule order in the chain does not matter.
* Insert
  + Inserts a rule in a chain at a point specified by a user-defined integer value. If no number is specified, iptables places the command at the top of the chain
* Delete
  + Deletes a rule in a particular chain by number (such as 5 for the fifth rule in a chain). You can also type the entire rule, and iptables deletes the rule in the chain that matches it
* List
  + Lists all of the rules in the chain specified after the command. To list all rules in all chains in the default filter table, do not specify a chain or table.
* Flush
  + Flushes the selected chain, which effectively deletes every rule in the the chain. If no chain is specified, this command flushes every rule from every chain.
* Policy
  + Sets the default policy for the specified chain, so that when packets traverse an entire chain without matching a rule, they are sent on to the specified target, such as ACCEPT or DROP.

**Filters** Filters are used to choose which packets match a rule. Each filter is used to create matches. Some matches requires modules to be loaded with -m MODULENAME to be available. Explain the following matches and how they can be used:

* -p
  + specify protocol,
* -s
  + specify source address
* -d
  + Specify destination port
* -i
  + specify the name of an interface to match. An interface is the physical device the packet came in on (`-i') or is going out on (`-o'). You can use the ifconfig command to list the interfaces which are `up' (i.e., working at the moment).
* -o
  + specify the name of an interface to match. An interface is the physical device the packet came in on (`-i') or is going out on (`-o'). You can use the ifconfig command to list the interfaces which are `up' (i.e., working at the moment).
* --sport
  + followed by an optional `!', then either a single TCP port, or a range of ports. Ports can be port names, as listed in /etc/services, or numeric. Ranges are either two port names separated by a `:', or (to specify greater than or equal to a given port) a port with a `:' appended, or (to specify less than or equal to a given port), a port preceded by a `:'.
* --dport
  + they specify the destination, rather than source, port to match.

**Jump Targets** We use jump targets to decide what to do with a packet once it has matched a rule.