Basic Iptables Options

Here are explanations for some of the iptables options you will see in this tutorial. Don't worry about understanding everything here now, but remember to come back and look at this list as you encounter new options later on.

* -A - Append this rule to a rule chain. Valid chains for what we're doing are INPUT, FORWARD and OUTPUT, but we mostly deal with INPUT in this tutorial, which affects only incoming traffic.
* -L - List the current filter rules.
* -m conntrack - Allow filter rules to match based on connection state. Permits the use of the --ctstate option.
* --ctstate - Define the list of states for the rule to match on. Valid states are:
  + NEW - The connection has not yet been seen.
  + RELATED - The connection is new, but is related to another connection already permitted.
  + ESTABLISHED - The connection is already established.
  + INVALID - The traffic couldn't be identified for some reason.
* -m limit - Require the rule to match only a limited number of times. Allows the use of the --limit option. Useful for limiting logging rules.
  + --limit - The maximum matching rate, given as a number followed by "/second", "/minute", "/hour", or "/day" depending on how often you want the rule to match. If this option is not used and -m limit is used, the default is "3/hour".
* -p - The connection protocol used.
* --dport - The destination port(s) required for this rule. A single port may be given, or a range may be given as start:end, which will match all ports from start to end, inclusive.
* -j - Jump to the specified target. By default, iptables allows four targets:
  + ACCEPT - Accept the packet and stop processing rules in this chain.
  + REJECT - Reject the packet and notify the sender that we did so, and stop processing rules in this chain.
  + DROP - Silently ignore the packet, and stop processing rules in this chain.
  + LOG - Log the packet, and continue processing more rules in this chain. Allows the use of the --log-prefix and --log-level options.
* --log-prefix - When logging, put this text before the log message. Use double quotes around the text to use.
* --log-level - Log using the specified syslog level. 7 is a good choice unless you specifically need something else.
* -i - Only match if the packet is coming in on the specified interface.
* -I - Inserts a rule. Takes two options, the chain to insert the rule into, and the rule number it should be.
  + -I INPUT 5 would insert the rule into the INPUT chain and make it the 5th rule in the list.
* -v - Display more information in the output. Useful for if you have rules that look similar without using -v.
* -s --source - address[/mask] source specification
* -d --destination - address[/mask] destination specification
* -o --out-interface - output name[+] network interface name ([+] for wildcard)