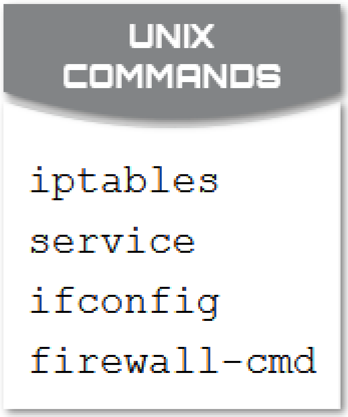
## UNIX Commands

Some common UNIX commands to research and become proficient with are:



UNIX COMMANDS

```
iptables
service
ifconfig
firewall-cmd
```

## Tables in iptables

| Table | Used for | Chains |
|---|---|---|
| filter | Accepting or rejecting packets | INPUT, FORWARD, OUTPUT |
| nat | Implementing network address translation | PREROUTING, OUTPUT, POSTROUTING |
| mangle | Implementing specialized packet rewriting rules | PREROUTING, INPUT, OUTPUT, FORWARD, POSTROUTING |
| raw | Circumventing the kernel's connection tracking mechanism (rarely used) | PREROUTING, OUTPUT |

## Options for iptables

| Option | Used for | Tables |
|---|---|---|
| -A *chain* | Append, or add, a rule to the end of a chain | All |
| -D *chain* [*line-number*] | Delete a rule from a chain; defaults to match | All |
| -I *chain* [*line-number*] | Insert a rule into a chain; defaults to first | All |
| -R *chain* [*line-number*] | Replace a rule in a chain; defaults to first | All |
| -L [*chain*] | List rules in a chain; defaults to all chains | All |
| -F [*chain*] | Flush rules in a chain; defaults to all chains | All |
| -P *chain target* | Sets default policy for a chain | filter |

## Frequently-used Match Criteria

Note: All of these criteria can be negated with **!**. Multiple criteria are combined with a logical **and**.

| Option | Used for | Legal values |
|---|---|---|
| -p | IP protocol | icmp, tcp, udp,all, number 0-255 |
| -s | Source of packet | Single IP address or network in CIDR |
| -d | Destination of packet | Single IP address or network in CIDR |
| -i | Interface packet arrived on | Interface specification from system |
| -o | Interface packet is departing on | Interface specification from system |
| -m | Loading additional matching rules, such as *state* | Loaded matchers |
| --sport | Source port | 0-65535, requires –p tcp or –p udp |
| --dport | Destination port | 0-65535, requires –p tcp or –p udp |

## Recommended Readings

- Linux iptables Pocket Reference

## Recommended Internet Sites

- HowTo for iptables: https://web.archive.org/web/20160801110428/https://wiki.centos.org/HowTos/Network/IPTables
- Man page for iptables: https://web.archive.org/web/20160801111314/http://ipset.netfilter.org/iptables.man.html
- Stateful rules with iptables: https://web.archive.org/web/20160801111413/https://wiki.archlinux.org/index.php/simple_stateful_firewall
- Port forwarding with iptables: https://www.systutorials.com/port-forwarding-using-iptables/
- Snort rules tutorial: https://web.archive.org/web/20150627004707/http://www.cse.sc.edu/~okeefe/tutorials/cert/i042.14.html
- Snort Users Manual: https://web.archive.org/web/20160801111652/http://manual-snort-org.s3-website-us-east-1.amazonaws.com/snort_manual.html

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.