Course Title
Term: (Fall, Spring, Summer, Winter) 20XX

Useful Commands and Config Files Cheat Sheet

Part 1

Examining/Working with Networking (from your server):

```
ip address show          # show configured IP addresses (the new way)
ifconfig                 # show configured IP addresses (the old way)
hostname -I              # show all public IP addresses
iptables -L              # list human readable listing of iptables ACLs chains
iptables -F              # flush all iptables rules
iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
             # chain   interface proto  dest port  ^the state of the packet^       target
iptables -t filter -A INPUT -j LOG   # Log packets that make it this far (good for watching)
iptables -t filter -A INPUT -j REJECT  # Reject packets that make it this far (common last
rule)
nmap -sS {target}        # stealth port scan
nmap -sP 10.1.1.1/24     # ping scan the IPs of the 10.1.1.x octet
netstat -ant             # local IP/port bindings: see [a]ll [n]umerical [t]cp
netstant -antp           # same as above + show process names bound to ports
```

Working with Files & Services:

```
vim                      # requisite editor (or vi) on most all unix systems
nano                     # popular editor, but not as ubiquitous as vi/vim
apt-get                  # working with configured OS package repositories
aptitude                 # working with configured OS package repositories
service <service name> start|stop|restart|status  # running service control

update-rc.d <service> enable|disable
                         # older, systemV init based service config control

systemctl start|stop|restart|status <servicename>.service
                         # newer, systemd based service config control

mv <file1> <path/file2> # move or rename file1 to file2
cp -a <file> <path/>     # archive copy w/preserving attributes/modes
ps auxw | grep xxx       # list all processes and grep (filter) for “xxx”
/etc/firewall.sh         # our distro-agnostic iptables firewall Network ACLs
/etc/apache2/ports.conf # the apache2 IP/port bindings (needs a restart)
/etc/mysql/my.cnf        # The main MySQL daemon config file (needs a restart)
/etc/services            # The human readable service names into port numbers
```

Part 2

Examining/Working with Networking (from your server):

```
service <name> restart  # restart a service or daemon (mysql, postfix, etc)
service <name> --status-all   # show all services and if configured to run
ip address show               # show configured IP addresses (the new way)
hostname -I                   # show all public IP addresses
netstant -antp|grep -e ^Proto -e :25
      # lists the header ^^ + process names with port binding of :25

aptitude -y -q full-upgrade   # full upgrade, yes-prompts quiet mode
cp -a <source> <dest>         # copies file and its mode and attributes
chmod 711 <folder>      # makes directory only readable/writable by its owner
                        # but allows those who know the internal structure to
                        # still enter (or execute entering) the directory
tail -f <logfile>       # great way of watching a log file in real time
```

Important Configuration Files:

```
/etc/ssh/sshd_config    # the main ssh daemon config file
                        # sshd must be restarted after changing
/etc/apache2/apache.config    # the main apache2 config file
/etc/postfix/main.cf    # The main postfix mail server config file
/etc/fail2ban/jail.conf # the main fail2ban (default) config file
```