[**https://www.feistyduck.com/library/apache-security/online/apachesc-CHP-8.html**](https://www.feistyduck.com/library/apache-security/online/apachesc-CHP-8.html) **(logging)**

**CentOS DoomsDay**

**Change passwords**

Command: sudo passwd

**Create new users**

Command: sudo useradd newusername

Command: sudo passwd newusername

**Look for extra users**

#Check for active users

Command: w

#Shows all existing users

Command: cat /etc/passwd/

#Shows users with sudo privileges

Command: sudo lid -g wheel

#Deletes users

Command: userdel -r username

#Check groups

Command: cat /etc/groups

#Check hosts

Command: cat /etc/hosts

**Disable root login**

Command: sudo vi /etc/passwd

#Change

root:…/bin/bash

#To

root:…/sbin/nologin

**Chronjobs and aliases**

#List of aliases

Command: alias -p

#Removes all aliases temporarily, check bashrc later to full remove

Command: unalias -a

#Disable cron jobs

Command: sudo service crond stop

Or Command: /etc/init.d/crond stop

#Lists cron jobs

Command: crontab -l

#Removes cron jobs

Command: crontab -r

**Change wheel group name**

Command: sudo groupmod --new-name new\_groupname old\_groupname

**Wheel Group**

Command: sudo visudo

#Uncomment

# %wheel   ALL=(ALL)   ALL

Command: sudo gpasswd -a newusername wheel

**SSH**

Command: sudo vi /etc/ssh/sshd\_config

#Change lines

#LogGraceTime 2m

#PermitRootLogin yes

#UsePAM no

#MaxStartups 10:30:100

#To this (Uncomment)

LoGraceTime 30

PermitRootLogin no

AllowUser user

UsePAM yes

MaxStartups 3:50:10

ServerKeyBits 2048

Command: sudo service sshd restart

**IPtables**

#Accept localhost

Command: iptables -A INPUT -i lo -j ACCEPT

#Accept SSH connections (template for opening incoming ports)

Command: iptables -A INPUT -p tcp --dport 22 -j ACCEPT

Command: iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Command: iptables -A INPUT -p tcp --dport 443 -j ACCEPT

#Allow ping requests

Command: iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

Command: iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

Command: iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

Command: iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

#Drop all other packets

Command: iptables -P INPUT DROP

Command: iptables -P FORWARD DROP

Command: iptables -P OUTPUT ACCEPT

#Check iptables config files to see if it is set correctly

Command: vi /etc/sysconfig/iptables

Command: sudo iptables -L -n

Command: sudo iptables save

Command: sudo service iptables restart

**Static ARP**

Command: sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0

#Change to look like

DEVICE=eth0

HWaddr=00:0C:29:9B:C9:00

BOOTPROTO=static

ONBOOT=yes

NM\_CONTROLLED=no

IPADDR=172.2.240.12

NETMASK=255.255.255.0

BROADCAST=172.2.240.12

GATEWAY=172.2.240.254

Command: sudo service networking restart

**IPRoute**

#Check and edit /etc/resolv.conf

Command: sudo vi /etc/resolv.conf

#Add

nameserver 8.8.8.8

nameserver 8.8.4.4

nameserver 127.0.0.1

**ETH0 up**

Command: sudo ifup eth0

#If it doesn’t work, make sure you’re on root

**Shut off NetworkManager**

#Check to see if enabled

Command: chkconfig --list NetworkManager

#If error, it’s not installed and everything’s fine

#If enabled, will see

NetworkManagaer   0:off   1:off   2:off   3:off   4:off   5:off   6:off

#If all run levels are off, move on

#If all run levels aren’t off, turn Network Manager off

Command: sudo service NetworkManager stop

Command: sudo service network restart

Command: sudo chkconfig network on

**Yum update**

Command: /etc/redhat-release or /etc/centos-release

Command: sudo yum clean all

Command: sudo yum -y update or upgrade

Command: sudo reboot

**Service installs**

Command: yum install httpd php php-mysql mysql-server php-devel php-gd php-pecl-memcache php-pspell php-snmp php-xmlrpc php-xml mod\_ssl openssl

**HTTP**

Command: sudo vi /etc/httpd/conf/httpd.conf

#Change

Options Indexes FollowSymLinks

#To

Options -Indexes FollowSymLinks -ExecCGI

Command: sudo service httpd restart

**Get GUI (if needed)**

Command: sudo yum groupinstall “Desktop”

Command: sudo reboot

Command: startx

**Service setup**

#Follow LAMP packet

#Make sure to replace IP on URL to your own set static IP

**Check services and shut off any services that are not needed**

#List all services

Command: chkconfig --list

#Disable services

Command: chkconfig servicename off

Command: chkconfig servicename -del

#Defaults are

auditd nefts

blk network

availability postfix

crond rsyslogd

iptables&&ip6tables sshd-udev-post

lvm2-monitor

**Check running processes**

#Real time list of processes

Command: top

#Kill process

Press k

Enter PID

Will ask for signal, ignore and press enter

**Check rogue aliases for users ( ~/.bashrc)**

Command sudo vi .bashrc

**Recheck crontab**

#User crontab

Command: sudo crontab -l -u

#Remove all crontab

Command: sudo crontab -r

#Edit and remove pecific cron jobs

Command: sudo crontab -e

**? Watch logs**

? Command: sysdig etc