First Step

Check physical machines (random USBs, other devices).
(SANS TOP 20)
Log in
Change Password -- passwd
Check /etc/passwd for strange accounts or accounts that should not have login shells

Create new administrator account

/var/log/messages or syslog
tail -f < any error file, **SQL injection would show up here**

```
su -                        #Change to root
passwd                      #Change root password
nano /etc/ssh/sshd_config   #Disable root login
                            #Disable password authentication if SSH keys are set up
```

BE CAREFUL WITH THIS. DO NOT LOCK YOURSELF OUT OF AWS

```
rm -rf ~/.ssh/* OR  mv /home/$USER/.ssh /home/$USER/nosshlogin
```

```
ssh-keygen                  #Create new keys if needed
ssh-copy-id                 #Copy public ssh key to a server
                            #Check Repos for sketch stuff - /etc/apt/sources or w.e
apt-get update (debian/ubuntu) | yum update (centos)
apt-get upgrade -y (debian/ubuntu) | yum upgrade -y (centos)
tail -f ~/.bash_history
tail -f /
```

Check Crontab for all jobs and all users

```
vi /etc/crontab
```

```
     for user in $(cut -f1 -d: /etc/passwd); do echo $user;
crontab -u $user -l; done
```

^ this is a one liner ^

FOR CURRENT USER: `crontab -e`

Check for start up programs

```
     cat ~/.bashrc
     cat /etc/rc.local
     ls -la /etc/init.d/
```

Check Mirrors & Repos

Debian based

/etc/apt/sources
/etc/apt/sources.list.d/

CentOS7:

```
yum repolist all #lists repos
```

1. `rpm -Uvh --force \`
   `http://mirror.centos.org/centos-7/7/os/x86_64/Packages/centos-release-7-3.1611.el7.centos.x86_64.rpm`
2. `yum clean all`
3. `yum update`

1. `yum reinstall \*`

Install TMUX

```
wget https://github.com/tmux/tmux/archive/master.zip
```

Extract /install
Run TMUX

Goals: Always have a window looking for root activity / netstat

```
tail -f /var/log/auth.log
```

Basic System Information:

View Operating system version

`lsb_release -a` (debian/ubuntu)

```
cat /proc/version OR cat /etc/centos-release
```

Check Open Ports and Services

`netstat -tupln` (check open ports and services)

Processes

`ps aux` (check running processes)
`lsof -p [pid]` (lists files associated with specific process)
`kill -9 [pid]` (kill unwanted/suspicious processes)

Aliases

alias

Passwords and Users:

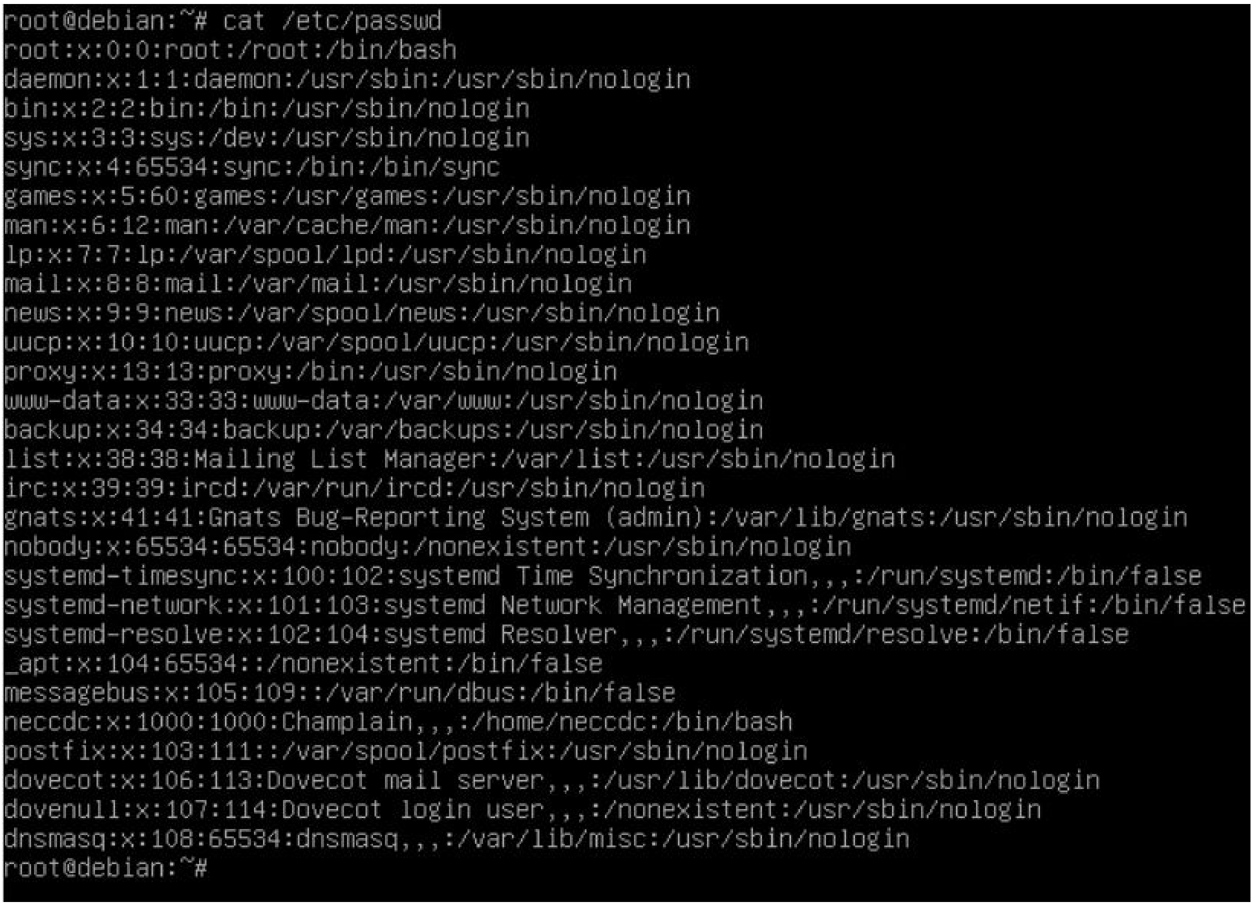
Check who is logged in

```
who
```

Lock account or delete user

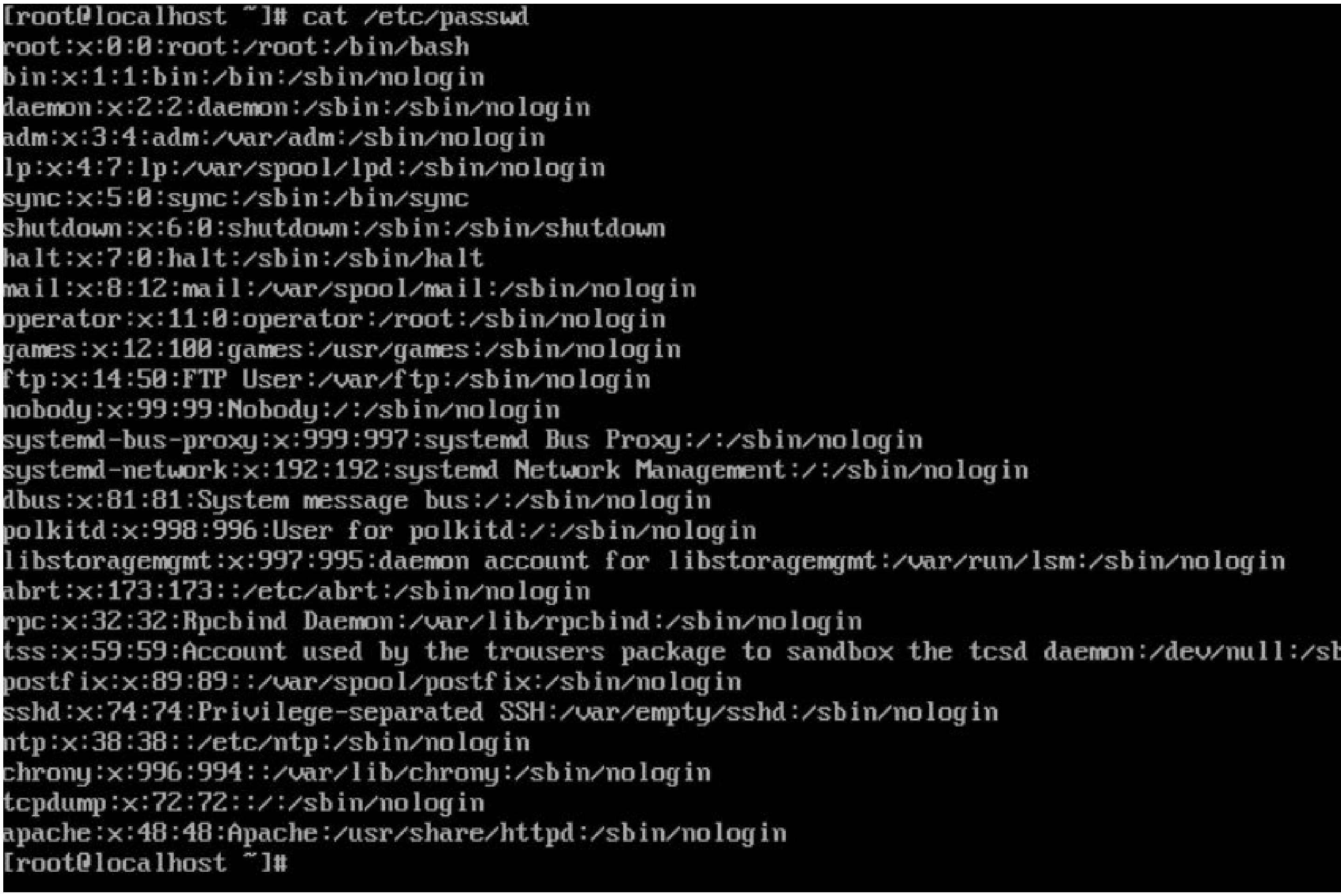
```
passwd -l <USERNAME>      (Linux Lock Account)
pw lock <USERNAME>        (FreeBSD Lock)
deluser <USERNAME>        (delete unwanted users)
```

Debian default accounts:



```
root@debian:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
messagebus:x:105:109::/var/run/dbus:/bin/false
neccdc:x:1000:1000:Champlain,,,:/home/neccdc:/bin/bash
postfix:x:103:111::/var/spool/postfix:/usr/sbin/nologin
dovecot:x:106:113:Dovecot mail server,,,:/usr/lib/dovecot:/usr/sbin/nologin
dovenull:x:107:114:Dovecot login user,,,:/nonexistent:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
root@debian:~#
```

CentOS Default accounts:



```
[root@localhost ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-bus-proxy:x:999:997:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:997:995:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sb
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:996:994::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
[root@localhost ~]#
```

Account info

finger root last (show last logins)

nano /etc/sudoers (check for unwanted users/permissions in sudo)

--*Ensure root is the only account with highest access*

```
    cat /etc/passwd (awk -F:’($3==”0”){print}’/etc/passwd)
    cat /etc/shadow
    awk -F:’($2==””){print}’/etc/shadow
```

Check for empty password

```
    awk -F: ‘( $2 == “” ) {print $1 }’ /etc/shadow
```

Services

Remove telnet and other services:

```
    /etc/inetd.conf
    apt-get purge remove <PACKAGE_NAME>
    yum remove <PACKAGE_NAME>
```

Config files and locations

```
    /etc/apache/config.file
    /etc/ssh/config.file
    /etc/mysql/mysql.cnf
    /var/lib/mysql
```

Find files/configs

```
find / -iname <FILE_NAME>     # -iname is case insensitive
```

locate firefox
whereis bash -- this will only locate binaries

Disable unneeded services (Cent OS)

/sbin/chkconfig $(SERVICE) off

Disable unneeded services (Linux)

service $SERVICE stop
chkconfig --level 12345 $SERVICE off

UNIX hardening using hosts.allow hosts.deny

Checks hosts allow
Checks hosts deny
if not in either it allows

One rule per service
immediate effect
ALWAYS NEED A NEW LINE CHAR at end

EXAMPLES
#in hosts.allow
sshd: .xyz.com
#in hosts.deny
sshd: ALL

echo “ALL: ALL” >> /etc/hosts.deny
echo “ALL: localhost” >> /etc/hosts.allow

```
for I in `/sbin/ifconfig | grep “inet addr” | cut -f2 -d: | cut -f1-3 -d”.” | grep -v ^127 | sort -n`; do printf “, $I.” >> /etc/allow; done;
```

File Permissions

Search for bad Permission files

```
    sudo find / -xdev -type d \( -perm -0002 -a ! -perm -1000 \) –print
```

Find files that have no owners

```
    sudo find / sdev \(-nouser -o -nogroup \) --print
```

/etc/fstab root:root 0644
/etc/shadow root:root 400
/etc/group root:root 644
/etc/passwd root:root 644
allows only root to access cron

```
    cd /etc/
    /bin/rm -f cron.deny at.deny
    echo root > cron.allow
    echo root > at.allow
    /bin/chown root:root cron.allow at.allow
    /bin/chmod 400 cron.allow at.allow
```

Crontab:

```
crontab -e
crontab -u root -e
for user in $(cut -f1 -d: /etc/passwd); do echo $user; crontab -u $user -l; done
```

PAM

Check /etc/pam.d/ for PAM config files

Remove any suspicious authorizations

https://goo.gl/2hACAx > PAM

SSH:

change port to anything other than 22 AND NOT 6969 or 1337 or 31337

/etc/ssh/sshd_config

```
Protocol 2
LogLevel VERBOSE
PermitRootLogin no
RhostsRSAAuthentication no
```

```
HostbasedAuthentication no
IgnoreRhosts yes
PasswordAuthentication no
PermitEmptyPasswords no
LoginGraceTime 1m
SyslogFacility AUTH

chown root:root /etc/ssh/sshd_config

Disable ipv6:
nano /etc/sysctl.conf
      net.ipv6.conf.all.disable_ipv6 = 1
      net.ipv6.conf.default.disable_ipv6 = 1
      net.ipv6.conf.lo.disable_ipv6 = 1
sysctl -p (reloads)
```

Regen SSH keys:

mv ~/.ssh/id_rsa ~/.ssh/id_rsa.old
mv ~/.ssh/id_rsa.pub ~/.ssh/id_rsa.pub.old

Ssh-keygen

scp -i ~/.ssh/id_rsa.old ~/.ssh/id_rsa.pub user@host:/home/user/id_rsa.pub.new

Ssh -i ~/.ssh/id_rsa.old

mv -f id_rsa.pub.new ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys

Check for heart bleed:

`openssl version -v` (1.0.1 is vulnerable)

Check for shellshock

Bash --version (anything before bash43-025 is vulnerable)

Useful CMDs bruh

```
rkhunter -c
watch -n 5 $cmdHere
tail -f /var/log/messages | grep --color “INBOUND:” # with proper rules
```

SCRIPTS

```
#!/bin/bash
#@author JaminB
#Will report any process started after the script is iniciated.
ps -A | cut -d ':' -f3 | cut -d ' ' -f2 | sort -k2 > snapshot
while true;
do
        current_proc=`ps -A | cut -d ':' -f3 | cut -d ' ' -f2 | sort -k2`
        snapshot_proc=`cat snapshot`
        echo NEW PROCESSES:
        diff -w <(echo "$current_proc") <(echo "$snapshot_proc") > possiblyBad
        i=1
        cat possiblyBad | while read line
        do
                if [ $(( $i%2 )) == 0 ]; then
                        echo $line | cut -d '<' -f2
                fi
                (( i=i+1 ))
        done
        sleep 3
        clear
done
```

Lynis

```
wget https://github.com/CISOfy/lynis/archive/master.zip
wget http://bit.ly/2isDC5U
Unzip master.zip
cd lynis-master
./lynis -Q  # Quick
./lynis -c  # Check-all
```

Once done `less /var/log/lynis.log`

FIREWALLS

iptables

List rules: `iptables -L`

Add:

- -i [NIC] to block connection on a specific NIC
- -p [tcp/udp] --dport [Number]
- -s [IP] to block from specific IP/ range
- -s ! [IP] to block all from IP address/range

Examples:

`iptables -A INPUT -s 11.22.33.44 -j DROP` | Adds a rule to block connections from IP 11.22.33.44

FirewallD

```
firewall-cmd --list-all # Lists rules
firewall-cmd --get-zones
```

UFW

```
sudo ufw deny from 15.15.15.51
sudo ufw allow [SERVICE]
sudo ufw allow [PORT]
sudo ufw deny [SERVICE OR PORT]
```

CentOS E-Commerce

HTML AND PHP SANITIZATION > no sql inject/xss for you

https://goo.gl/SGXKCZ > SQL
https://goo.gl/BE1tLs > XSS

LAMP

https://goo.gl/J9wnEf

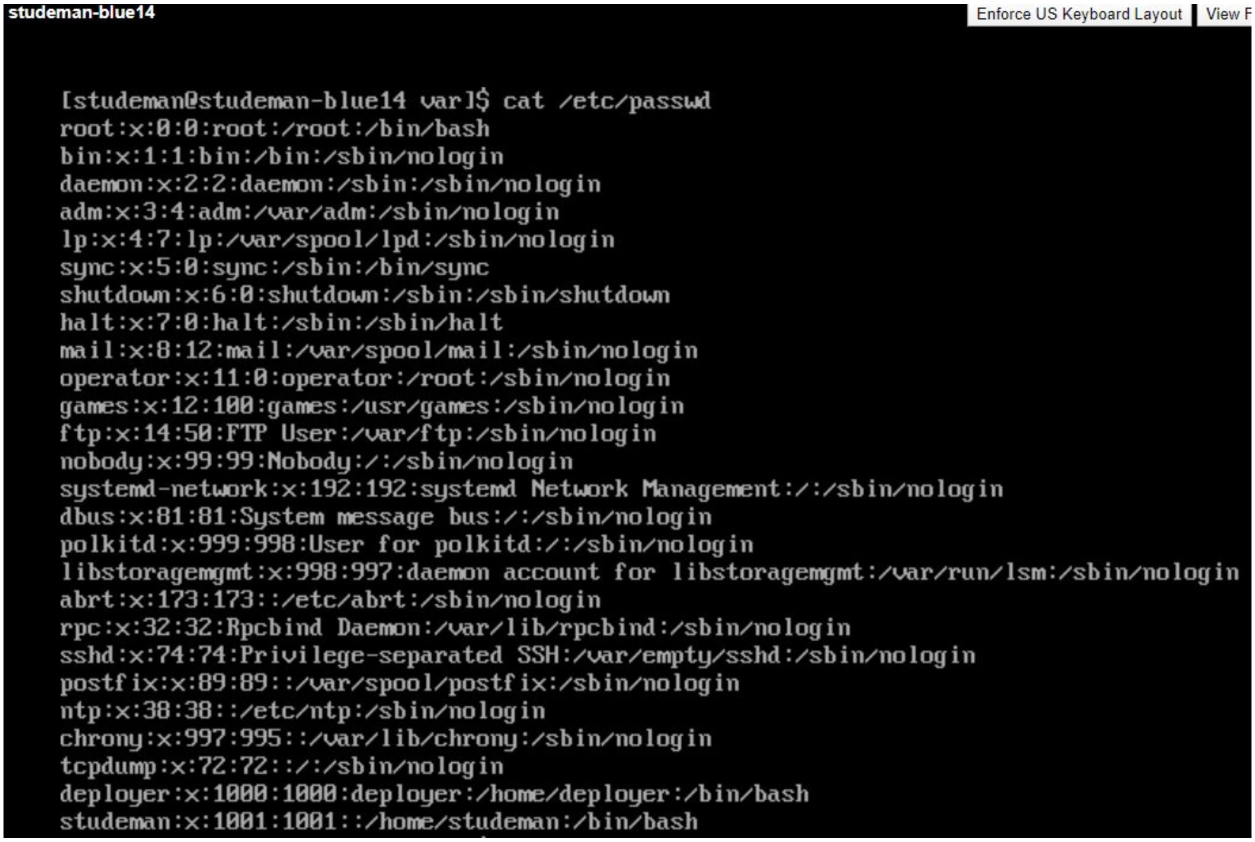
Apache

Hardening: https://goo.gl/SX2jaq

Check for any odd PHP files in /var/www/html
Check apache.conf (/etc/httpd.conf) for random file paths, filenames, reverse proxies
Check /etc/nginx/nginx.conf, /etc/nginx/sites-available, /etc/nginx/sites-enabled

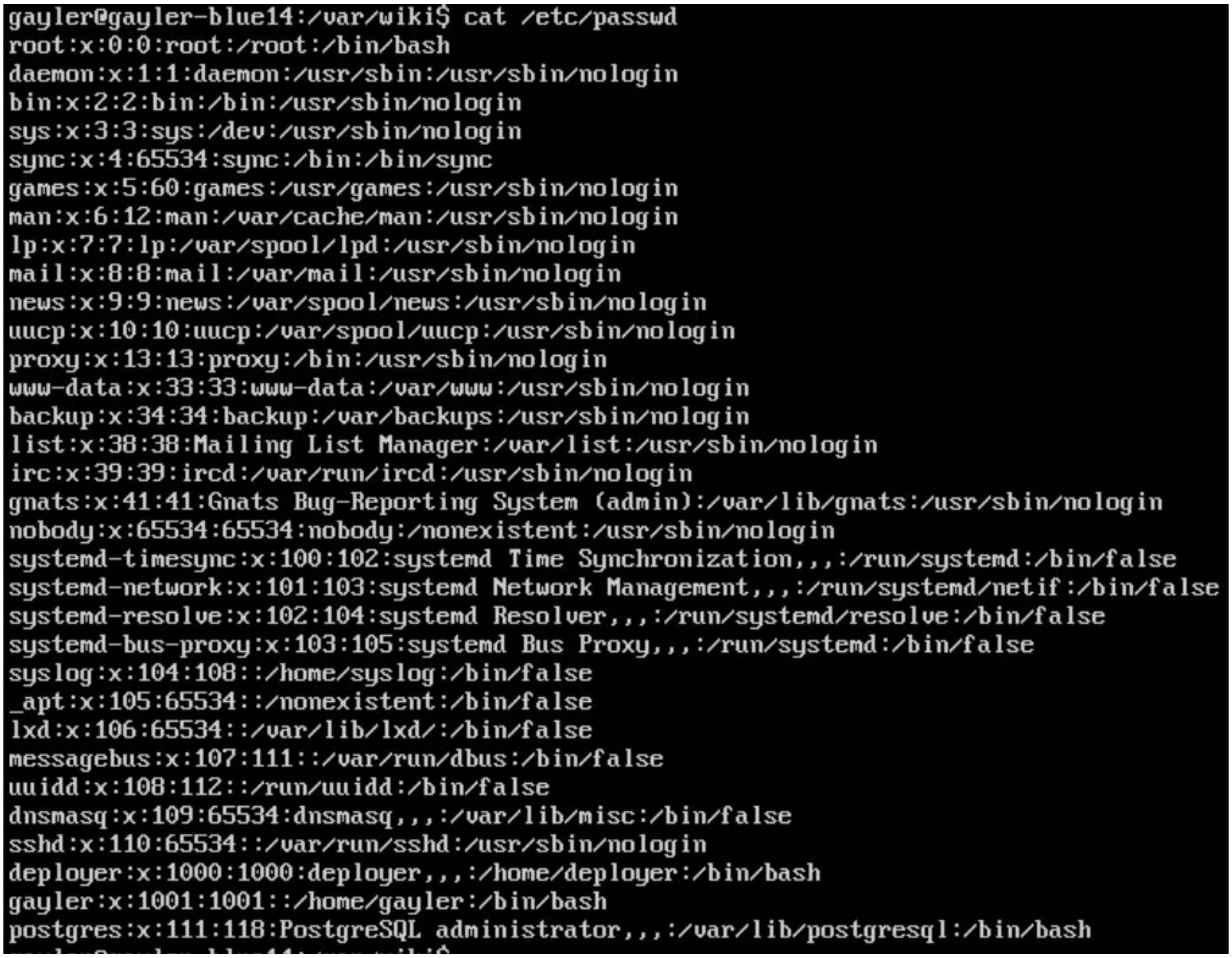
To import a database

```
mysql -u root -p
mysql> CREATE DATABASE new_database;
$ mysql -u username -p database < data-dump.sql
```



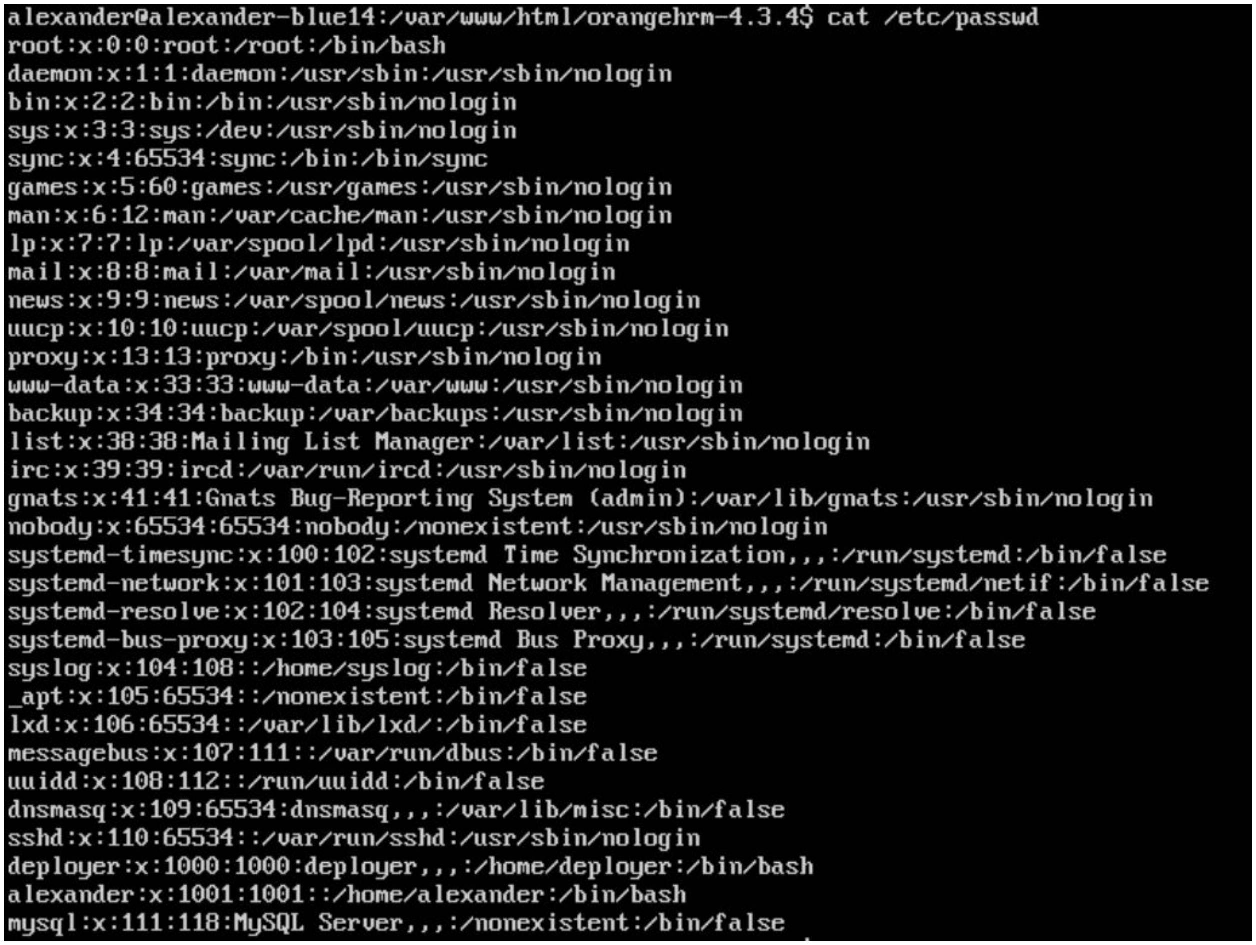
```
[studeman@studeman-blue14 var]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
deployer:x:1000:1000:deployer:/home/deployer:/bin/bash
studeman:x:1001:1001::/home/studeman:/bin/bash
```

Wiki.js:



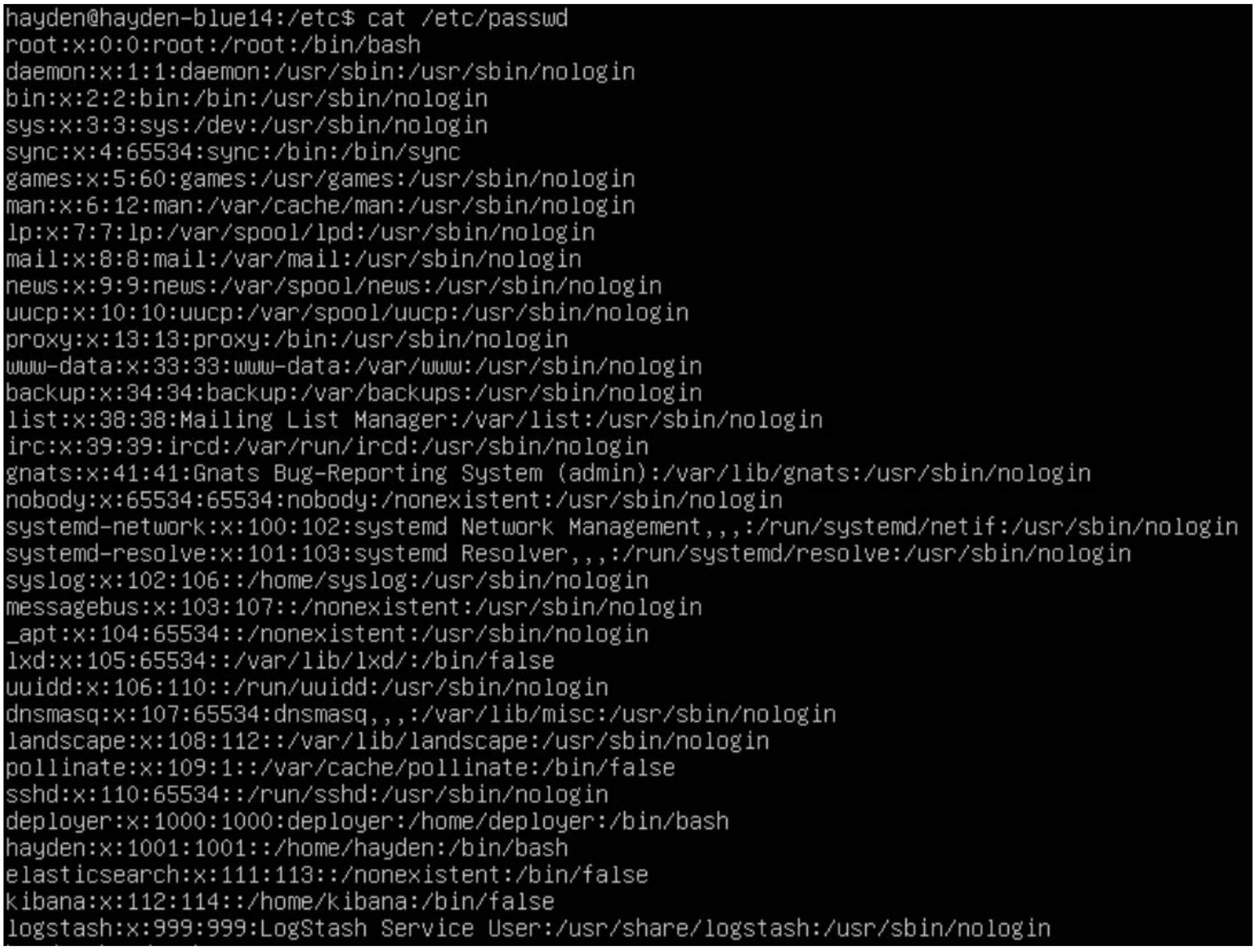
```
gayler@gayler-blue14:/var/wiki$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
deployer:x:1000:1000:deployer,,,:/home/deployer:/bin/bash
gayler:x:1001:1001::/home/gayler:/bin/bash
postgres:x:111:118:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
gayler@gayler-blue14:/var/wiki$
```

Orange HRM:



```
alexander@alexander-blue14:/var/www/html/orangehrm-4.3.4$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
deployer:x:1000:1000:deployer,,,:/home/deployer:/bin/bash
alexander:x:1001:1001::/home/alexander:/bin/bash
mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false
```

ELK:



```
hayden@hayden-blue14:/etc$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
deployer:x:1000:1000:deployer:/home/deployer:/bin/bash
hayden:x:1001:1001::/home/hayden:/bin/bash
elasticsearch:x:111:113::/nonexistent:/bin/false
kibana:x:112:114::/home/kibana:/bin/false
logstash:x:999:999:LogStash Service User:/usr/share/logstash:/usr/sbin/nologin
```