

User Auditing

week of 10/5/2020

Announcements

1. Create your teams by Oct. 15!
 - a. Practice Round: Oct. 22 weekend
 - i. Ubuntu 16/Debian 9 *NEW*
 - b. Find/Make friends for teams; email people (spreadsheet)
 - c. 3 Windows, 2 Linux, 1 Cisco
 - d. Cyber Dating Session
2. Troy Cyber Discord
 - a. cyber.jmal.xyz
 - b. join I guess if you wanna be a cool kid

wish I used this post-it

Users? They exist? no way

Users: people that exist on the system and can use varying features of the system

- standard: users that have normal privileges
 - User ID > 1000
- administrator: users that have elevated privileges
 - UID = 0
- system/service: "users" that run services
 - UID = btwn. 0 & 1000

Today, we're going to learn how about users, groups, and much more! :))



Adding/Deleting Users

- **adduser** [user_name]
 - adds a user to the system (where?)
 - prompts for password & personal information
 - creates corresponding group named [user_name]
- **deluser** [user_name]
 - deletes an existing user from the system


must have sudo privileges (standard user can't make accounts)

useradd, userdel (same thing but more bare bones)



/etc/passwd file (not password)

- file that contains information about all users (admin, standard, system)
- How do we get here? (to read/write the file)
- If you have permissions to write on this file, you can edit the lines directly and configure users



```
oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash
```

↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7

/etc/passwd in detail

oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash

The diagram shows the entry 'oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash' with arrows pointing from each field to a number below it. The fields are: 'oracle' (1), 'x' (2), '1021' (3), '1020' (4), 'Oracle user' (5), '/data/network/oracle' (6), and '/bin/bash' (7).

1. Name of user
2. Encrypted Password
3. User ID (UID)
4. Group ID (GID)
5. GECOS/Comments (Extra Info)
6. Home directory (absolute path)
7. Shell directory
 - a. make sure users have functioning shells (/bin/bash)
 - b. Remember the difference between shell and terminal?


```
user@ubuntu: ~  
GNU nano 2.5.3 File: /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
toor: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:Mail 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  
messagebus:x:106:110:./var/run/dbus:/bin/false  
uidd:x:107:111:./run/uidd:/bin/false  
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false  
whoopsie:x:109:117:./nonexistent:/bin/false  
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false  
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false  
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false  
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false  
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false  
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false  
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false  
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false  
Read 46 lines  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page  
^X Exit ^R Read File ^_ Replace ^U Uncut Text ^T To Spell ^_ Go To Line ^V Next Page
```

Notice anything different between this picture and your own file?

```

root:x:0:0:root:/root:/bin/bash
toor: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:Mail 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
messagebus:x:106:110:./var/run/dbus:/bin/false
uidd:x:107:111:./run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117:./nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false

```

Read 46 lines

What is the UID for that different line?

Why is that a security issue that must be resolved?

/etc/shadow

- file that contains all the passwords of all users (x in the /etc/passwd file)
- **sudo nano /etc/shadow**
- passwords are **hashed** (encrypted for security)
 - \$1: MD5
 - \$5: SHA-256
 - \$6: SHA-512 (most secure)
- don't worry too much about the hash types, just be aware of them



/etc/shadow in detail

vivek:\$1\$fnfffc\$pgteyHdicpGOfffXX4ow#5:13064:0:99999:7:::



1



2



3



4



5



6

1. Name of User
2. Encrypted Password (! and * what is this)
3. Last Password Change
4. Minimum Password Age
5. Max Password Age
6. Warning Period (days)

Guest Account

Guest account: standard account that can be used temporarily (does not require password)

- Is this secure?
- What should we do about that?

Guest account config is located in:

- `/etc/lightdm/lightdm.conf`
- `/usr/lightdm/lightdm.conf`

It may vary based on version (so research!) but we'll go over proper configuration next!



Picture of /etc/lightdm/

```
user@ubuntu: ~  
File Edit View Search Terminal Help  
GNU nano 2.5.3 File: /etc/lightdm/lightdm.conf.d/00-yes.conf Modified  
[SeatDefaults]  
allow-guest=false
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```
user@ubuntu: /etc/lightdm  
File Edit View Search Terminal Help  
user@ubuntu:/etc/lightdm$ ls -la  
total 24  
drwxr-xr-x 3 root root 4096 Feb 26 2019 .  
drwxr-xr-x 135 root root 12288 Oct 3 23:26 ..  
drwxr-xr-x 2 root root 4096 Oct 3 23:26 lightdm.conf.d  
-rw-r--r-- 1 root root 452 Mar 31 2017 users.conf  
user@ubuntu:/etc/lightdm$
```


/etc/lightdm/lightdm.conf

- **allow-guest=false**
 - essentially disables the guest account (logical if you read it)
- **autologin=user**
 - self-explanatory
 - could be a security issue but really a preference



What do these commands look like?

ORACLE[®]
VM
VirtualBox



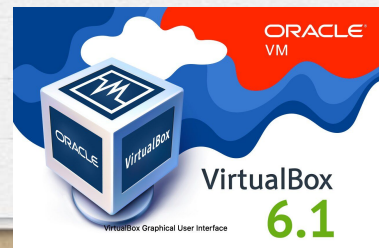
- Let's check it out in VirtualBox woooo000o0 practice



VirtualBox



"boy oh boy
VirtualBox"
- Ryan Nguyen
2020



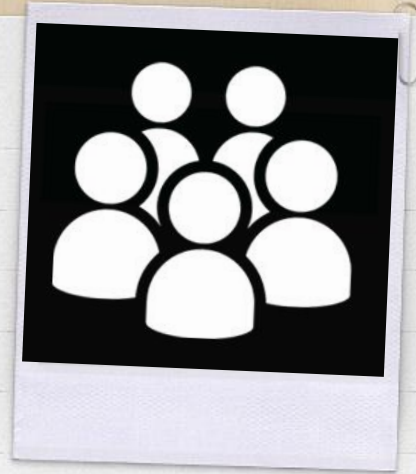
Groups

Groups: multiple users that are organized based on certain file permissions on the system

- ex. engineering, IT, marketing (real-life business application)

In a Linux system, there are groups that also have certain permissions for files

- root, sudo, admin, etc.



Commands for Groups

- **addgroup [group_name]**
 - creates a new group w/ [group_name]
- **delgroup [group_name]**
 - deletes an existing group
- **gpasswd -a [user_name] [group_name]**
 - adds a user to the specified group
 - also **adduser [user_name] [group_name]**
 - **-d**: deletes a users from the group

groupadd and **groupdel** outdated versions of the respective commands above



/etc/group file

- file that contains all information about groups and the users within them
- just like /etc/passwd file, with the right perms, you can add/remove groups and their members manually



```
oracle:x:1000:dba,oinstall,grid
```



1. name of group
2. Encrypted Password
3. GID
4. Members of Group


```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,user
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:user
floppy:x:25:
tape:x:26:
sudo:x:27:user,martha,jay
audio:x:29:pulse
dip:x:30:user
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:user
staff:x:50:
games:x:60:
```