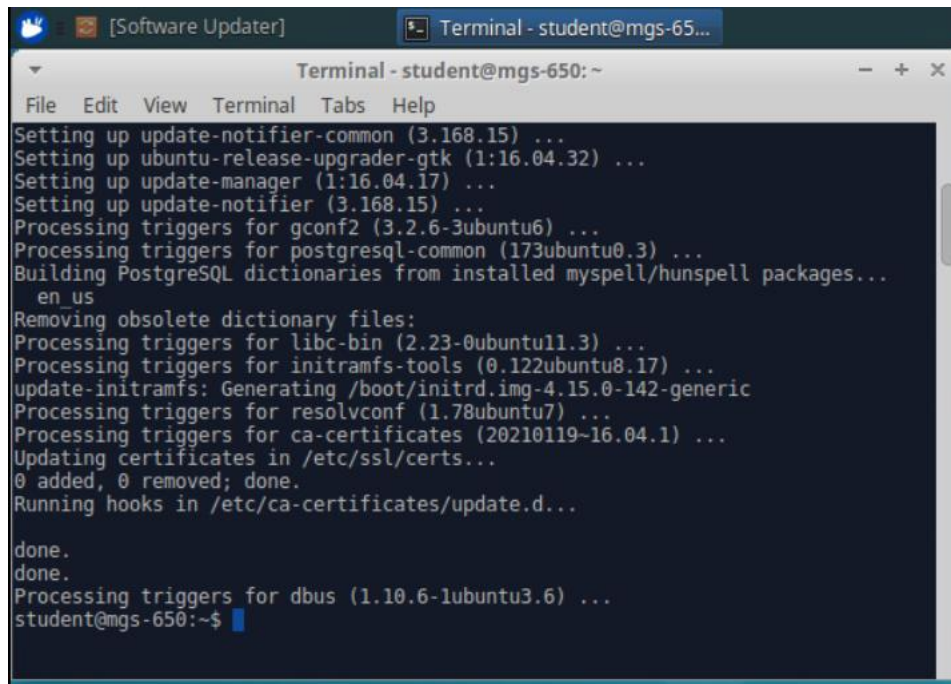


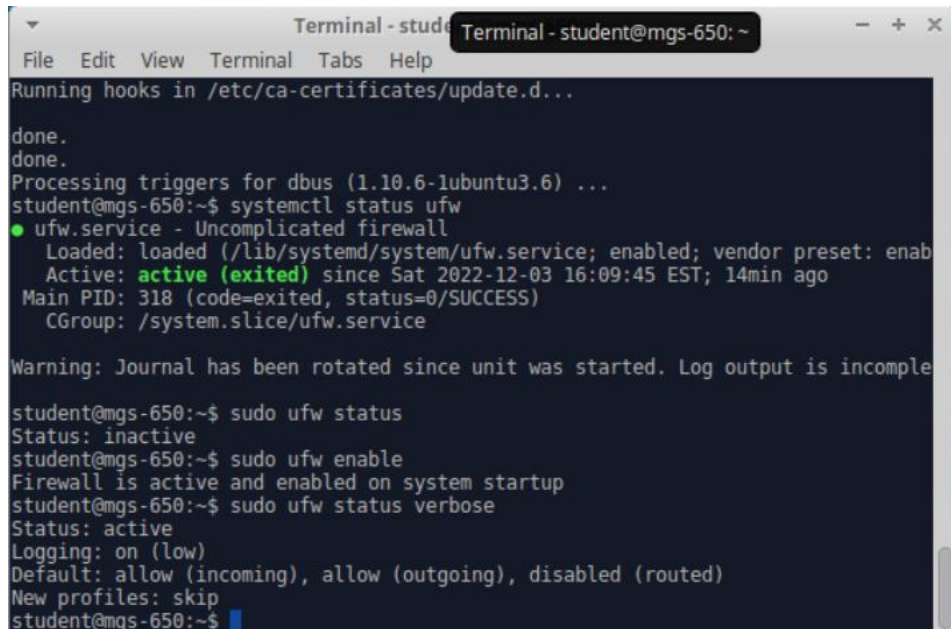
SYSTEM HARDENING LAB

1. Successful update



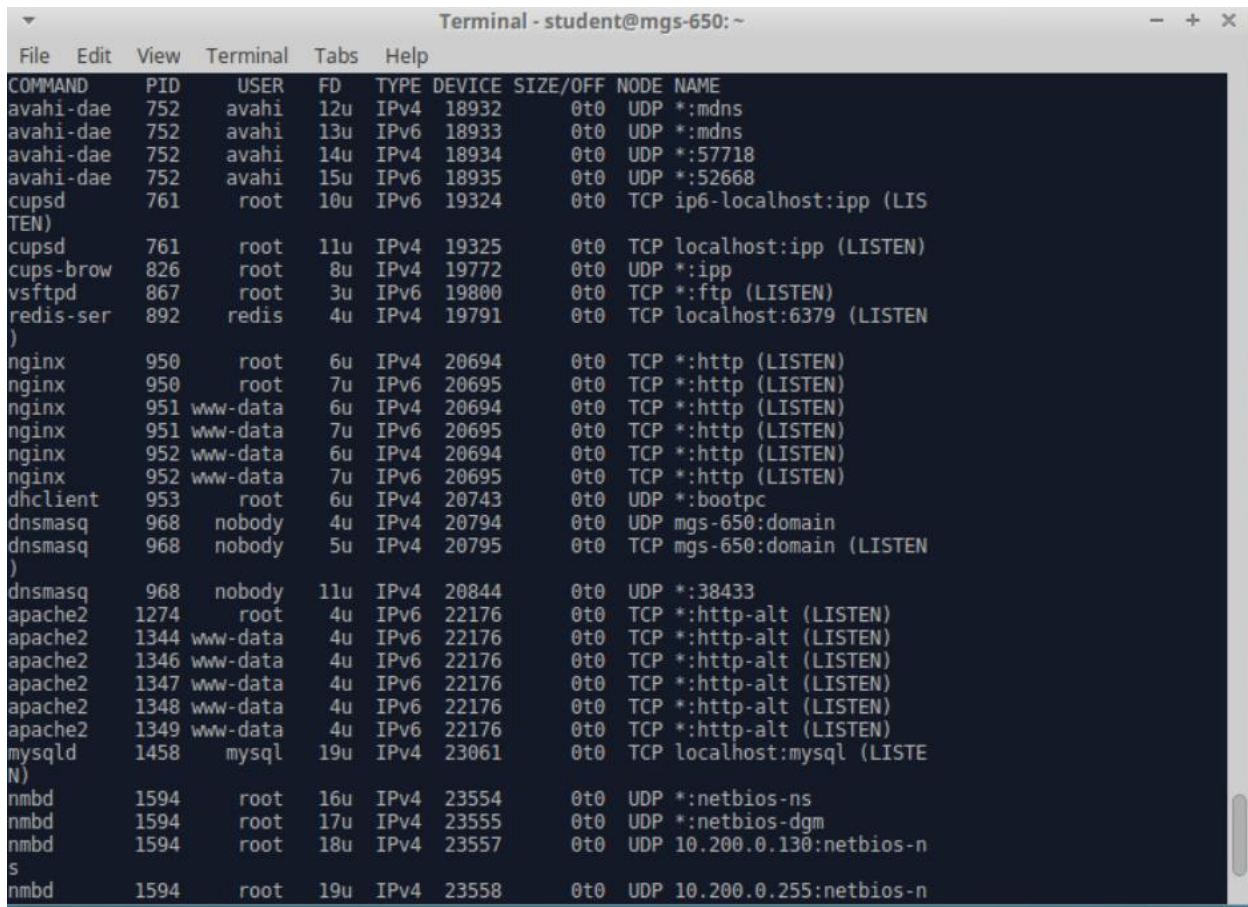
A terminal window titled "Terminal - student@mgs-650: ~" showing the output of a system update. The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal output shows the following steps: Setting up update-notifier-common (3.168.15) ... Setting up ubuntu-release-upgrader-gtk (1:16.04.32) ... Setting up update-manager (1:16.04.17) ... Setting up update-notifier (3.168.15) ... Processing triggers for gconf2 (3.2.6-3ubuntu6) ... Processing triggers for postgresql-common (173ubuntu0.3) ... Building PostgreSQL dictionaries from installed myspell/hunspell packages... en us Removing obsolete dictionary files: Processing triggers for libc-bin (2.23-0ubuntu11.3) ... Processing triggers for initramfs-tools (0.122ubuntu8.17) ... update-initramfs: Generating /boot/initrd.img-4.15.0-142-generic Processing triggers for resolvconf (1.78ubuntu7) ... Processing triggers for ca-certificates (20210119-16.04.1) ... Updating certificates in /etc/ssl/certs... 0 added, 0 removed; done. Running hooks in /etc/ca-certificates/update.d... done. done. Processing triggers for dbus (1.10.6-1ubuntu3.6) ... student@mgs-650:~\$

2. Status of uncomplicated firewall and enabling it.



A terminal window titled "Terminal - student@mgs-650: ~" showing the status and enabling of the uncomplicated firewall. The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal output shows the following steps: Running hooks in /etc/ca-certificates/update.d... done. done. Processing triggers for dbus (1.10.6-1ubuntu3.6) ... student@mgs-650:~\$ systemctl status ufw ● ufw.service - Uncomplicated firewall Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled) Active: active (exited) since Sat 2022-12-03 16:09:45 EST; 14min ago Main PID: 318 (code=exited, status=0/SUCCESS) CGroup: /system.slice/ufw.service Warning: Journal has been rotated since unit was started. Log output is incomplete student@mgs-650:~\$ sudo ufw status Status: inactive student@mgs-650:~\$ sudo ufw enable Firewall is active and enabled on system startup student@mgs-650:~\$ sudo ufw status verbose Status: active Logging: on (low) Default: allow (incoming), allow (outgoing), disabled (routed) New profiles: skip student@mgs-650:~\$

3. Existing firewall rules

A terminal window titled "Terminal - student@mgs-650: ~" displays the output of the 'ss -tlnp' command. The output is a table with columns: COMMAND, PID, USER, FD, TYPE, DEVICE, SIZE/OFF, NODE, and NAME. It lists various network services and their listening ports, including avahi-daemon, cupsd, vsftpd, redis-server, nginx, dnsmasq, apache2, mysqld, nmbd, and s. The window has a menu bar with File, Edit, View, Terminal, Tabs, and Help, and standard window controls (minimize, maximize, close) in the top right corner.

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
avahi-daemon	752	avahi	12u	IPv4	18932	0t0	UDP	*:mdns
avahi-daemon	752	avahi	13u	IPv6	18933	0t0	UDP	*:mdns
avahi-daemon	752	avahi	14u	IPv4	18934	0t0	UDP	*:57718
avahi-daemon	752	avahi	15u	IPv6	18935	0t0	UDP	*:52668
cupsd	761	root	10u	IPv6	19324	0t0	TCP	ip6-localhost:ipp (LISTEN)
cupsd	761	root	11u	IPv4	19325	0t0	TCP	localhost:ipp (LISTEN)
cups-browsed	826	root	8u	IPv4	19772	0t0	UDP	*:ipp
vsftpd	867	root	3u	IPv6	19800	0t0	TCP	*:ftp (LISTEN)
redis-server	892	redis	4u	IPv4	19791	0t0	TCP	localhost:6379 (LISTEN)
nginx	950	root	6u	IPv4	20694	0t0	TCP	*:http (LISTEN)
nginx	950	root	7u	IPv6	20695	0t0	TCP	*:http (LISTEN)
nginx	951	www-data	6u	IPv4	20694	0t0	TCP	*:http (LISTEN)
nginx	951	www-data	7u	IPv6	20695	0t0	TCP	*:http (LISTEN)
nginx	952	www-data	6u	IPv4	20694	0t0	TCP	*:http (LISTEN)
nginx	952	www-data	7u	IPv6	20695	0t0	TCP	*:http (LISTEN)
dhclient	953	root	6u	IPv4	20743	0t0	UDP	*:bootpc
dnsmasq	968	nobody	4u	IPv4	20794	0t0	UDP	mgs-650:domain
dnsmasq	968	nobody	5u	IPv4	20795	0t0	TCP	mgs-650:domain (LISTEN)
dnsmasq	968	nobody	11u	IPv4	20844	0t0	UDP	*:38433
apache2	1274	root	4u	IPv6	22176	0t0	TCP	*:http-alt (LISTEN)
apache2	1344	www-data	4u	IPv6	22176	0t0	TCP	*:http-alt (LISTEN)
apache2	1346	www-data	4u	IPv6	22176	0t0	TCP	*:http-alt (LISTEN)
apache2	1347	www-data	4u	IPv6	22176	0t0	TCP	*:http-alt (LISTEN)
apache2	1348	www-data	4u	IPv6	22176	0t0	TCP	*:http-alt (LISTEN)
apache2	1349	www-data	4u	IPv6	22176	0t0	TCP	*:http-alt (LISTEN)
mysqld	1458	mysql	19u	IPv4	23061	0t0	TCP	localhost:mysql (LISTEN)
nmbd	1594	root	16u	IPv4	23554	0t0	UDP	*:netbios-ns
nmbd	1594	root	17u	IPv4	23555	0t0	UDP	*:netbios-dgm
nmbd	1594	root	18u	IPv4	23557	0t0	UDP	10.200.0.130:netbios-ns
smbd	1594	root	19u	IPv4	23558	0t0	UDP	10.200.0.255:netbios-ns

4. Creating outgoing and incoming rules for the firewall

```
student@mgs-650:~$ sudo ufw allow 22
Rule added
Rule added (v6)
student@mgs-650:~$ sudo ufw allow 80
Rule added
Rule added (v6)
student@mgs-650:~$ sudo ufw allow 8080
Rule added
Rule added (v6)
student@mgs-650:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
student@mgs-650:~$ sudo ufw allow out 53
Rule added
Rule added (v6)
student@mgs-650:~$ sudo ufw allow out 80
Rule added
Rule added (v6)
student@mgs-650:~$ sudo ufw allow out 443
Rule added
Rule added (v6)
student@mgs-650:~$ sudo ufw default reject outgoing
Default outgoing policy changed to 'reject'
(be sure to update your rules accordingly)
student@mgs-650:~$
```

5. Checking the status of the running processes

```
systemd+ 25721 0.0 0.1 12620 2496 ? Ssl 16:19 0:00 /lib/systemd/systemd-timesyncd
root 25722 0.0 0.0 0 0 ? I 16:19 0:00 [kworker/0:0]
student@mgs-650:~$ systemctl status
● mgs-650
   State: running
   Jobs: 0 queued
  Failed: 0 units
   Since: Sat 2022-12-03 16:09:43 EST; 26min ago
  CGroup: /
          └─user.slice
              └─user-1000.slice
                  └─user@1000.service
                      └─init.scope
                          ├─1700 /lib/systemd/systemd --user
                          └─1701 (sd-pam)
                  └─session-c2.scope
                      ├─1689 lightdm --session-child 12 19
                      ├─1706 /usr/bin/gnome-keyring-daemon --daemonize --login
                      ├─1708 /sbin/upstart --user
                      ├─1779 upstart-udev-bridge --daemon --user
                      ├─1780 dbus-daemon --fork --session --address=unix:abstract=/tmp/dbus-4nZuJBZAYC
                      ├─1834 upstart-dbus-bridge --daemon --system --user --bus-name system
                      ├─1836 upstart-file-bridge --daemon --user
                      ├─1838 upstart-dbus-bridge --daemon --session --user --bus-name session
                      ├─1842 /usr/lib/at-spi2-core/at-spi-bus-launcher
                      ├─1847 /usr/bin/dbus-daemon --config-file=/etc/at-spi2/accessibility.conf --nofork --pri
                      ├─1849 /usr/lib/at-spi2-core/at-spi2-registryd --use-gnome-session
                      ├─1856 gpg-agent --homedir /home/student/.gnupg --use-standard-socket --daemon
                      ├─1865 /bin/sh /etc/xdg/xfce4/xinitrc -- /etc/X11/xinit/xserverrc
                      ├─1876 xfce4-session
                      ├─1881 /usr/lib/i386-linux-gnu/xfce4/xfconf/xfconfd
                      ├─1887 xfwm4 --replace
                      ├─1891 xfce4-panel
                      ├─1893 Thunar --daemon
                      ├─1895 xfdesktop
                      └─1900 xfsettingsd
```

6. Checking the grep command status

```
[lines 125-159/159 (END)]
student@mgs-650:~$ systemctl status | grep service
└─user@1000.service
    └─1973 /usr/lib/dconf/dconf.service
    └─1991 /usr/lib/i386-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/i386-linux-gnu/xfce4/pan
el/plugins/libindicator-plugin.so 6 20971567 indicator Indicator Plugin Provides a panel area for Unity in
dicators. Indicators allow applications and system services to display their status and interact with the
user.
    └─2003 upstart --user --startup-event indicator-services-start
    └─2005 /usr/lib/i386-linux-gnu/indicator-messages/indicator-messages.service
    └─2006 /usr/lib/i386-linux-gnu/indicator-sound/indicator-sound.service
    └─2011 /usr/lib/i386-linux-gnu/indicator-application/indicator-application.service
    └─21690 grep --color=auto service
└─irqbalance.service
└─lightdm.service
└─polkitd.service
└─vsftpd.service
└─systemd-timesyncd.service
└─nmbd.service
└─nginx.service
└─upower.service
└─NetworkManager.service
└─dbus.service
└─accounts-daemon.service
    └─769 /usr/lib/accounts.service/accounts-daemon
    └─postgresql@9.5-main.service
└─smbd.service
└─udisks2.service
└─whoopsie.service
└─ssh.service
└─avahi-daemon.service
    └─getty@tty1.service
└─xinetd.service
└─ModemManager.service
└─systemd-logind.service
└─rtkit-daemon.service
```


7. Removing Samba

```
student@mgs-650:~$ sudo apt purge samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  attr libllvm4.0 linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic linux-image-4.10.0-28-generic linux-image-extra-4.10.0-28-generic python-dnspython samba-dsdb-modules samba-vfs-modules
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  samba*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 11.6 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 240265 files and directories currently installed.)
Removing samba (2:4.3.11+dfsg-0ubuntu0.16.04.34) ...
Purging configuration files for samba (2:4.3.11+dfsg-0ubuntu0.16.04.34) ...
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
Processing triggers for man-db (2.7.5-1) ...
student@mgs-650:~$
```

8. Checking nginx status and disabling along with deleting and locking user.

```
Terminal - student@mgs-650:~
File Edit View Terminal Tabs Help
After this operation, 11.6 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 240265 files and directories currently installed.)
Removing samba (2:4.3.11+dfsg-0ubuntu0.16.04.34) ...
Purging configuration files for samba (2:4.3.11+dfsg-0ubuntu0.16.04.34) ...
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
Processing triggers for man-db (2.7.5-1) ...
student@mgs-650:~$ systemctl status nginx
No command 'systemctl' found, did you mean:
  Command 'systemctl' from package 'systemd' (main)
systemctl: command not found
student@mgs-650:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-12-03 16:10:14 EST; 32min ago
     Main PID: 950 (nginx)
    CGroup: /system.slice/nginx.service
            └─950 nginx: master process /usr/sbin/nginx -g daemon on; master_process on
              └─951 nginx: worker process
                └─952 nginx: worker process

Dec 03 16:10:07 mgs-650 systemd[1]: Starting A high performance web server and a reverse proxy server...
Dec 03 16:10:14 mgs-650 systemd[1]: Started A high performance web server and a reverse proxy server.
student@mgs-650:~$ systemctl disable nginx
Unknown operation dfisable.
student@mgs-650:~$ sudo deluser amaright
Removing user 'amaright' ...
Warning: group 'amaright' has no more members.
Done.
student@mgs-650:~$ passwd -l jsweeny
passwd: Permission denied.
student@mgs-650:~$ passwd -l jsweeney
passwd: Permission denied.
student@mgs-650:~$ sudo passwd -l jsweeney
passwd: password expiry information changed.
student@mgs-650:~$
```

9. Password hash

```
cat: etc/shadow: No such file or directory
student@mgs-650:~$ sudo cat /etc/shadow
root:!:17495:0:99999:7:::
daemon*:17379:0:99999:7:::
bin*:17379:0:99999:7:::
sys*:17379:0:99999:7:::
sync*:17379:0:99999:7:::
games*:17379:0:99999:7:::
man*:17379:0:99999:7:::
lp*:17379:0:99999:7:::
mail*:17379:0:99999:7:::
news*:17379:0:99999:7:::
uucp*:17379:0:99999:7:::
proxy*:17379:0:99999:7:::
www-data*:17379:0:99999:7:::
backup*:17379:0:99999:7:::
list*:17379:0:99999:7:::
irc*:17379:0:99999:7:::
gnats*:17379:0:99999:7:::
nobody*:17379:0:99999:7:::
systemd-timesync*:17379:0:99999:7:::
systemd-network*:17379:0:99999:7:::
systemd-resolve*:17379:0:99999:7:::
systemd-bus-proxy*:17379:0:99999:7:::
syslog*:17379:0:99999:7:::
_apt*:17379:0:99999:7:::
messagebus*:17379:0:99999:7:::
uuidd*:17379:0:99999:7:::
lightdm*:17379:0:99999:7:::
whoopsie*:17379:0:99999:7:::
avahi-autoipd*:17379:0:99999:7:::
avahi*:17379:0:99999:7:::
colord*:17379:0:99999:7:::
dnsmasq*:17379:0:99999:7:::
hplip*:17379:0:99999:7:::
```

10. Setting default password for the users that doesn't have any password.

```
student@mgs-650:~$ sudo passwd dunnxter
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@mgs-650:~$ sudo passwd illianaa
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@mgs-650:~$ sudp passwd marshall
No command 'sudp' found, did you mean:
  Command 'sup' from package 'sup' (universe)
  Command 'sfdp' from package 'graphviz' (main)
  Command 'sudo' from package 'sudo-ldap' (universe)
  Command 'sudo' from package 'sudo' (main)
sudp: command not found
student@mgs-650:~$ sudo passwd marshall
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@mgs-650:~$ sudo passwd orlando
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@mgs-650:~$ sudo passwd serenaba
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@mgs-650:~$ sudo passwd solomonw
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@mgs-650:~$
```

11. Looking at the group of users that has sudo privileges.

```
voice:x:22:  
cdrom:x:24:student  
floppy:x:25:  
tape:x:26:  
sudo:x:27:student,veronica,zachbird,jsweeney,postgres  
audio:x:29:pulse  
User 30:student
```

12. Deleting users

```
sotomoniw:x:1010:  
redis:x:133:  
student@mgs-650:~$ sudo deluser postgres sudo  
Removing user 'postgres' from group 'sudo' ...  
Done.  
student@mgs-650:~$ sudo deluser jsweeney sudo  
Removing user 'jsweeney' from group 'sudo' ...  
Done.  
student@mgs-650:~$ sudo deluser veronica sudo  
Removing user 'veronica' from group 'sudo' ...  
Done.  
student@mgs-650:~$
```