Updated: 2024-10-16
This is not a script. Just follow along and paste in the commands.
This file is for hardening Ubuntu desktop 24.10, not Ubuntu server.

The best results will be obtained by re-installing Ubuntu first and applying this
configuration prior to going online because we are not certain that the machine is
un-infected.

Disconnect from internet

Go to Settings > Privacy & Security > File History & Trash
Turn OFF file history
Turn ON automatically delete temporary files
Set automatic deletion period to 1 hr

set Dash as login shell instead of bash – less features, less hackable, also faster
```
sudo sed 's:/bin/bash:/usr/bin/dash:' < /etc/passwd > /Documents/passwd
sudo mv ~/Documents/passwd /etc/passwd
```

Reboot Now

Set firewall to default deny incoming traffic, because we only go outbound with ### firefox. Returning traffic will be allowed by default because of firewall statefulness
```
sudo ufw default deny incoming
sudo ufw default deny outgoing
sudo ufw allow out 123/udp
sudo ufw allow out 53/udp
sudo ufw allow out 853/tcp
sudo ufw allow out 80/tcp
sudo ufw allow out 443/tcp
sudo ufw enable
```

Turn off IPv6, we don't need it. Plus maybe your router/hardware firewall don't support it
then ipv6 traffic will pass right through.
```
nano /etc/default/grub
```

Find the line that says "GRUB_CMDLINE_LINUX…"
Append to the end of it with: (be careful to leave the last close quote ")
```
ipv6.disable=1 kernel.shmmax=0 kernel.shmmin=0 kernel.msgmax=0 audit=1
```

Then enforce it
```
grub-mkconfig -o /boot/grub/grub.cfg
```

Remove cups - historically hackable
Skip if you do print things, I don't
```
sudo apt remove cups-daemon
```

Remove unnecessary networking daemons less network attack surface
```
sudo dpkg -r -force-depends libfreerdp-server3-3
```

Remove WiFi - I live in a crowded apartment complex, WiFi Direct/p2p can
reach me without authentication, so I disable Wifi in BIOS and disable WiFi
components and use USB Ethernet adapter
Skip these 4 lines if you do need WiFi
```
sudo systemctl stop wpa_supplicant.service
sudo systemctl disable wpa_supplicant.service
sudo systemctl stop geoclue.service
sudo systemctl disable geoclue.service
```

Error reporting for Canonical - no need to report to Ubuntu/Canonical
```
sudo dpkg -P whoopsie
sudo rm /usr/share/apport/whoopsie-upload-all
```

Mask the unneeded networking services we don't need so they don't run
Reduce your attack surface
```
sudo systemctl stop ModemManager.service
sudo systemctl mask ModemManager.service
sudo systemctl stop avahi-daemon.service
sudo systemctl mask avahi-daemon.service
```

umask determines the permissions of any file or directory we create. This setting
allows owner rights only.
```
sudo nano /etc/init.d/sysstat
```

Ctrl-W find `UMASK 022`, and change it to `077`

Set home directory access to allow owners only
Setup home access defaults. It is not properly set because we only changed the
umask just now
```
chmod -R 770 /home/<yourAccount>/
chmod -R 770 /home/<nextAccount>/
```

Edit this file and enable/un-comment (erasing the '#') in front of each setting except
the lines mentioning 'forwarding'
```
sudo nano /etc/sysctl.conf
```

Edit this file
```
sudo nano /etc/systemd/resolved.conf
```

uncomment (remove the #) and change this to yes:
```
DNSOverTLS=
```

Make TLS 1.3 usage default. TLS 1.3 is the latest encryption for use with https and other things
It has enhanced security features.
However, small parts of the internet's web servers may still be on TLS 1.2, and if you configure
this section, you may not be able to connect to those sites. You decide.
```
sudo nano /etc/gnutls/config
```

Add these two lines:
```
disabled-version = tls1.2
disabled-version = dtls1.2
```

Use the Quad9 DNS servers, it filters out malware sites
Go to Settings > Network > WiFi/Ethernet > IPv4
Turn off Automatic DNS, enter these ip addresses:
```
9.9.9.9,149.112.112.112
```

Reboot Now

Now connect to internet

Install things we need
Synaptic is a GUI app that stands in for the command line '`apt`' package manager.
```
sudo apt install synaptic
```

Start Synaptic, click on Search button,
Type in
```
firejail
```
Checkmark it. Mark for Installation
Click the Apply button, then Apply again in the dialog box

Turn on Firejail tracelog so that blacklist violations are logged in syslog
```
sudo nano /etc/firejail/firejail.config
```

Search for "tracelog" and set it to yes

Now install the following using Synaptic:

```
apparmor-profiles
clamav
tcsh
```

Next we change the shell to tcsh, which is friendlier than dash

```
sudo sed 's:dash:tcsh:' < /etc/passwd > ~/Documents/passwd
sudo mv ~/Documents/passwd /etc/passwd
```

Reboot

Ubuntu 24.10 comes with a new Security app
When we enable it, it will Prompt us whenever Firefox needs to access a /home folder
Like Documents, Downloads and Pictures.
So start the Security app, then enable “Require apps to ask …”

You are Strongly Advised NOT to allow access to Documents, because you will
have confidential files there.

Next we disable some bindings of Firefox
Go to Settings > Apps > Firefox
Disable the following:
-Run in background
-system-files
-gsetting
-Access hardware information
-mount control
-system-files
-Use any connected joystick
-login session observe
-network bind
-read/write files on removable storage
-system-packages-doc

Configure safe defaults for Firefox
You need to do these steps for each Ubuntu account because Firefox stores it’s settings
separately for each

Go to Firefox > Settings
> General > Confirm before closing multiple tabs = checkmark
> General > Network Settings > Settings button > select No Proxy
> Home > Homepage and new windows = Blank page
> Home > New Tabs = Blank Page
> Search > Search Suggestions > Show trending search suggestions = Uncheck

> Search > Address Bar > Shortcuts = Uncheck
> Privacy & Security > Strict radio button
> Privacy & Security > Cookies and Site Data > Delete cookies and site data when
Firefox is closed = Checkmark (This stops info-stealer malware from stealing your ### cookies when you are not using Firefox)
> Privacy & Security > Passwords > Use a Primary Password = create this
> Privacy & Security > Autofill > Save and fill addresses = Uncheck
> Privacy & Security > Autofill > Save and fill payment methods = Uncheck
> Privacy & Security > Firefox Data Collection > Allow Firefox (3) = Uncheck
(it is better to not store sensitive data like address and credit cards in your browser)
> Privacy & Security > Firefox Data Collection > Allow Firefox to install and run
studies = Uncheck
> Privacy & Security > HTTPS Only Mode > Enable HTTPS Only Mode in all
windows = selected
> Privacy & Security > Enable DNS over HTTPS > Max Protection = selected
Go to Firefox > Add ons and themes > Find more Addons > Search for :
> PRIVACY BADGER
> Add an ad blocker of your choice to block annoying ads that block the screen

Make a second account for Daily Use
The second account does not have the capability to issue sudo commands until you
add the account to the admin group or make a rule via visudo. This is good
because any attack on apps run by this account cannot elevate to gain root
privilege. Go to Settings > System > Users.

ClamAV does not fetch updates automatically upon install
You need to define a service to start 'freshclam'

```
sudo nano /usr/lib/systemd/system/freshclam.service
```

and put the following lines inside:

```
[Unit]
Description=Run freshclam in daemon mode to fetch updates
After=multi-user.target

[Service]
Type=oneshot
ExecStart=/usr/bin/fr
eshclam -d
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

Then enable and start the service
```
sudo systemctl enable freshclam.service && sudo systemctl start freshclam.service
```

Then if you want scheduled scans do the following:
```
sudo crontab -e
```

Place the following line inside crontab to scan the whole drive at 22:00 every day
22 means 10pm in 24 hr clock military time. To have more than 1 scan per day,
add more lines like it specifying a different time.
```
0 22 * * * /usr/bin/clamscan -r /
```

For a periodic 2nd opinion scanner, use Kaspersky Virus Scan
It is Not a real time AV, it is only meant for periodic use to double check
```
https://www.kaspersky.com/downloads/free-virus-removal-tool
```

So we have done the protections
Now we setup detections
Every time somebody uses sudo we want it logged to a file named sudo.log
```
sudo visudo
```

Add this line to the bottom
```
Defaults logfile=/var/log/sudo.log
Defaults timestamp_timeout=1
```

You can view all past sudo commands issued with this:
```
sudo less /var/log/sudo.log
```

And now we install Logwatch:
Use Synaptic as before

Here is how to use it :
```
sudo /usr/sbin/logwatch -detail high -range Today -filename <YouProvideFilename>
less <YourProvidedFilename>
```

You can replace the word Today with Yesterday or All

Install ChkRootkit and rkhunter. As the package name says, they check for root kits,
which are used by hackers to hide themselves
Use Synaptic as before
```
chkrootkit
rkhunter
```

Install Wazuh SIEM (Security Information and Event Management)
It is a full featured open source security monitoring tool.
If installing on single machine, no need to install the agent
After install, use Firefox to browse to 127.0.0.1
Look at it at least once per day.
Home > Overview > Threat Hunting > sort by Level, and investigate the higher ### priority alerts
https://documentation.wazuh.com/current/quickstart.html

For quick remediation, I use Clonezilla disk imaging.
It is VERY IMPORTANT to have a backup! Because if all protections fail, and you ### were unable to detect the threat actor, you will have to restore from this backup when ### you are compromised.
You need 2 USB sticks. A small one to put the clonezilla onto. And a large one to store ### the backup image
https://clonezilla.org/