

# The Linux Desktop For Security Professionals

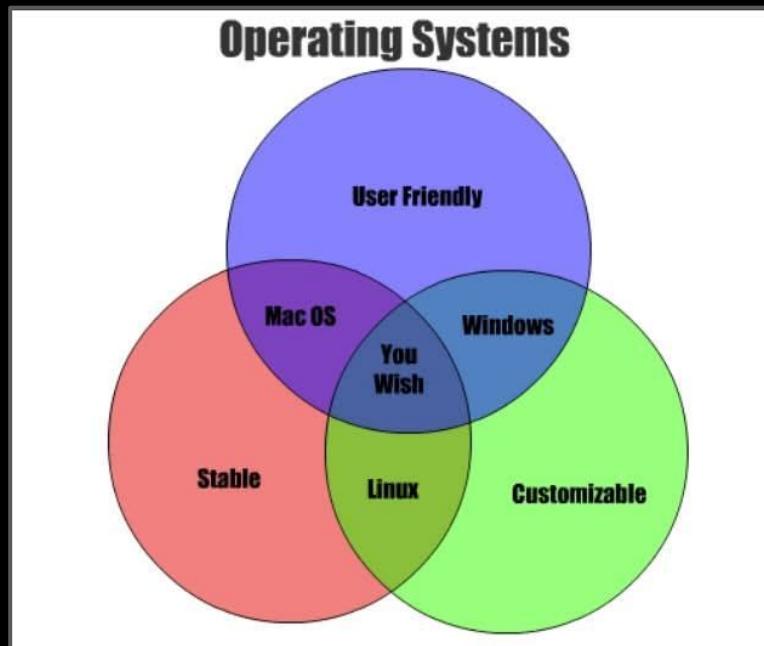
```
$ ./start-linux-presentation.sh
# Paul Asadoorian
# Principal Security Researcher
# Eclysium | https://eclysium.com

Dispelling Myths...
Generating Reasons To Run Linux...
Downloading Ridiculous Linux Memes...
Creating Linux Desktop Tips and Tricks...
git clone https://github.com/pasadoorian/Linux/Desktop_Security_Pro
```



# \$ NOW Is The Time To Talk About Switching To Linux

- Windows 10 EoS Oct 2025
- Windows 11 hardware requirements
- Microsoft Recall
- Apple HW restrictions and ARM platform
- Microsoft tries to require MS accounts for Windows installations
- Microsoft wants to collect your data in case of a failure (prevent future incidents such as Crowdstrike)

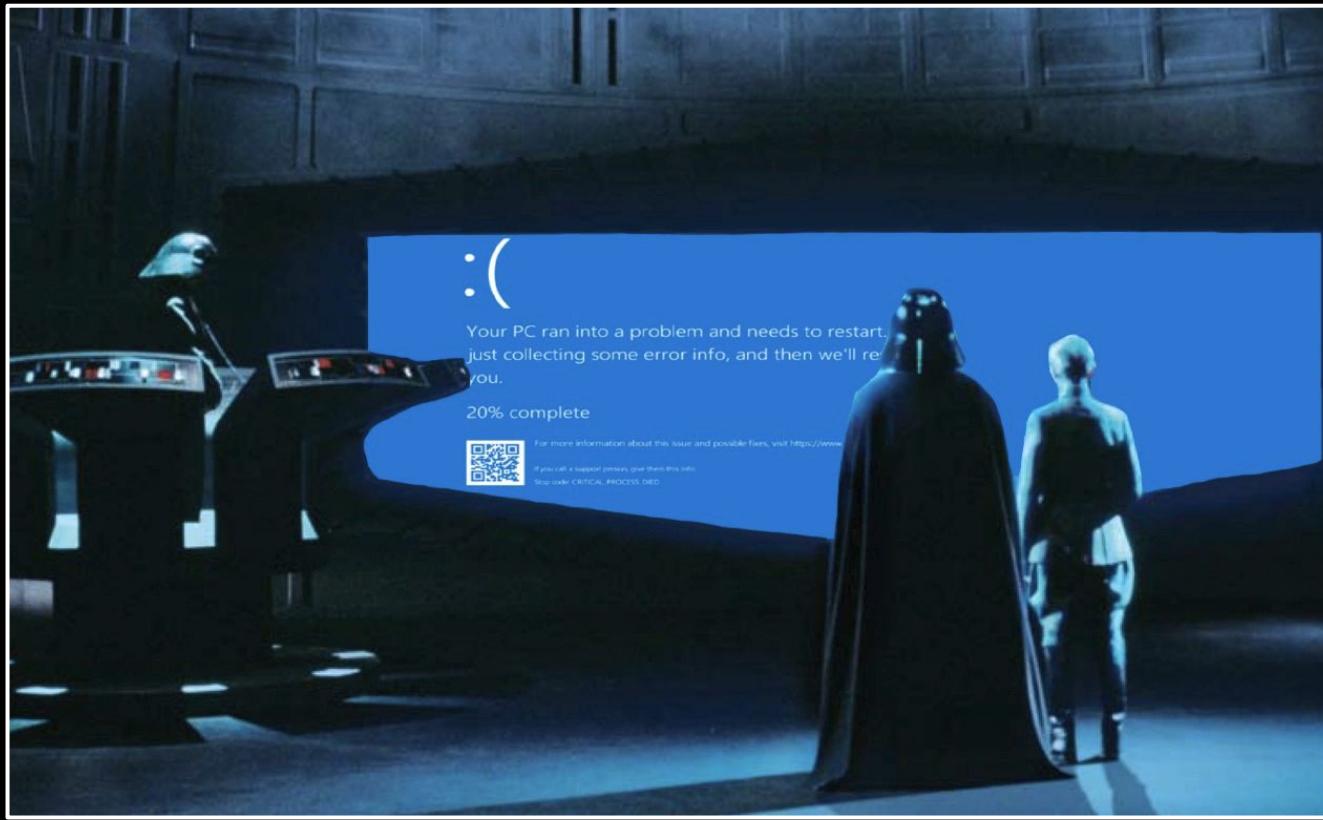


# \$ What This Presentation Will Not Be Like



*And other lies...*

# \$ I Won't Poke Fun At Microsoft Windows



*And more lies...*

# \$ I Will Spare macOS Users



*And even more lies...*

# \$ What I Will Talk About

- **Debunk Myths:** reasons you are not using Linux as your daily driver
- Why Linux is a better OS for **most security professionals**
- Tips and tricks for a better Linux desktop experience

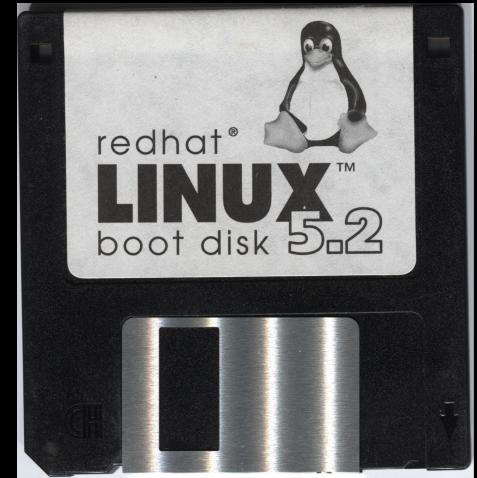


Note: All slides, examples, scripts, etc.. are here:

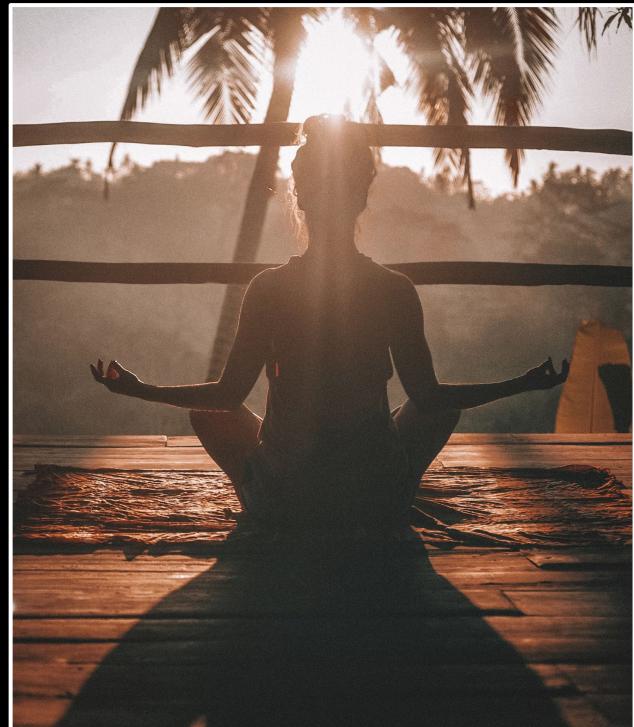
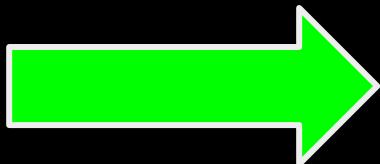
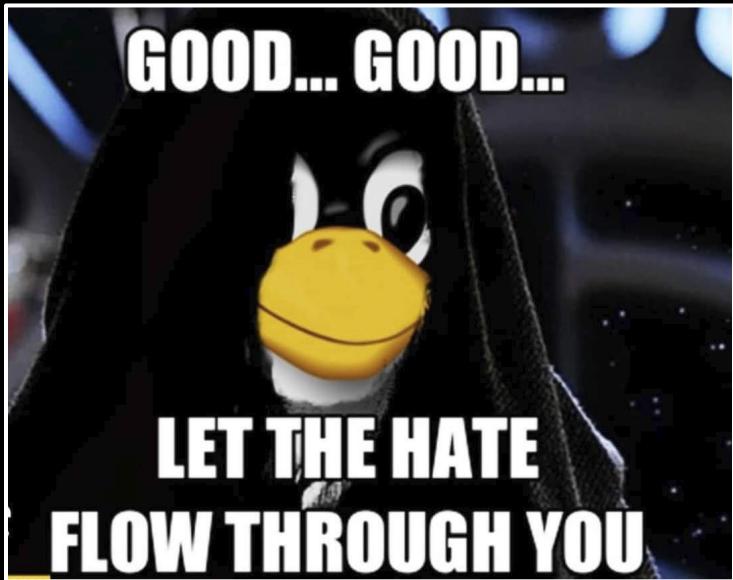
[https://github.com/pasadoorian/Linux/Desktop\\_Security\\_Pro](https://github.com/pasadoorian/Linux/Desktop_Security_Pro)

# \$ cat MyLinuxJourney.txt

- A friend recommended Linux to me in 1999 (same friend who taught me vim), ran Red Hat 5.2, got hacked
- Landed a job as a UNIX/Linux sysadmin (Solaris, Linux, AIX) - Had a Linux workstation (secondary)
- Worked at a university, Solaris/Linux admin and security, ran Solaris as my workstation
- The dark years: Switched to Mac after some failed attempts at Linux desktops
- In 2016 I switched to Linux on my laptop(s)
- In 2019 I made the final switch to Linux on my desktop(s)
- Today: 2 Linux laptops, 2 Linux desktops, 10+ Linux servers/PCs that run my podcast studio and home network



# Common Linux Desktop Myths and Misconceptions



Please keep an open  
mind...



## \$ I Don't Use Linux As My Desktop Because:

1. I can't edit MS Office Documents locally
2. I have one or two software applications that won't run on Linux
3. Display drivers are a nightmare on Linux
4. I have hardware that is not supported on Linux
5. I can't print using Linux
6. I have a life
7. Gaming on Linux sucks
8. I don't want to "fiddle" with my daily driver OS
9. I tried it, ran into issues, and switch back to Windows or MacOS
10. I don't want to compile software (e.g. my kernel)

# \$ Office

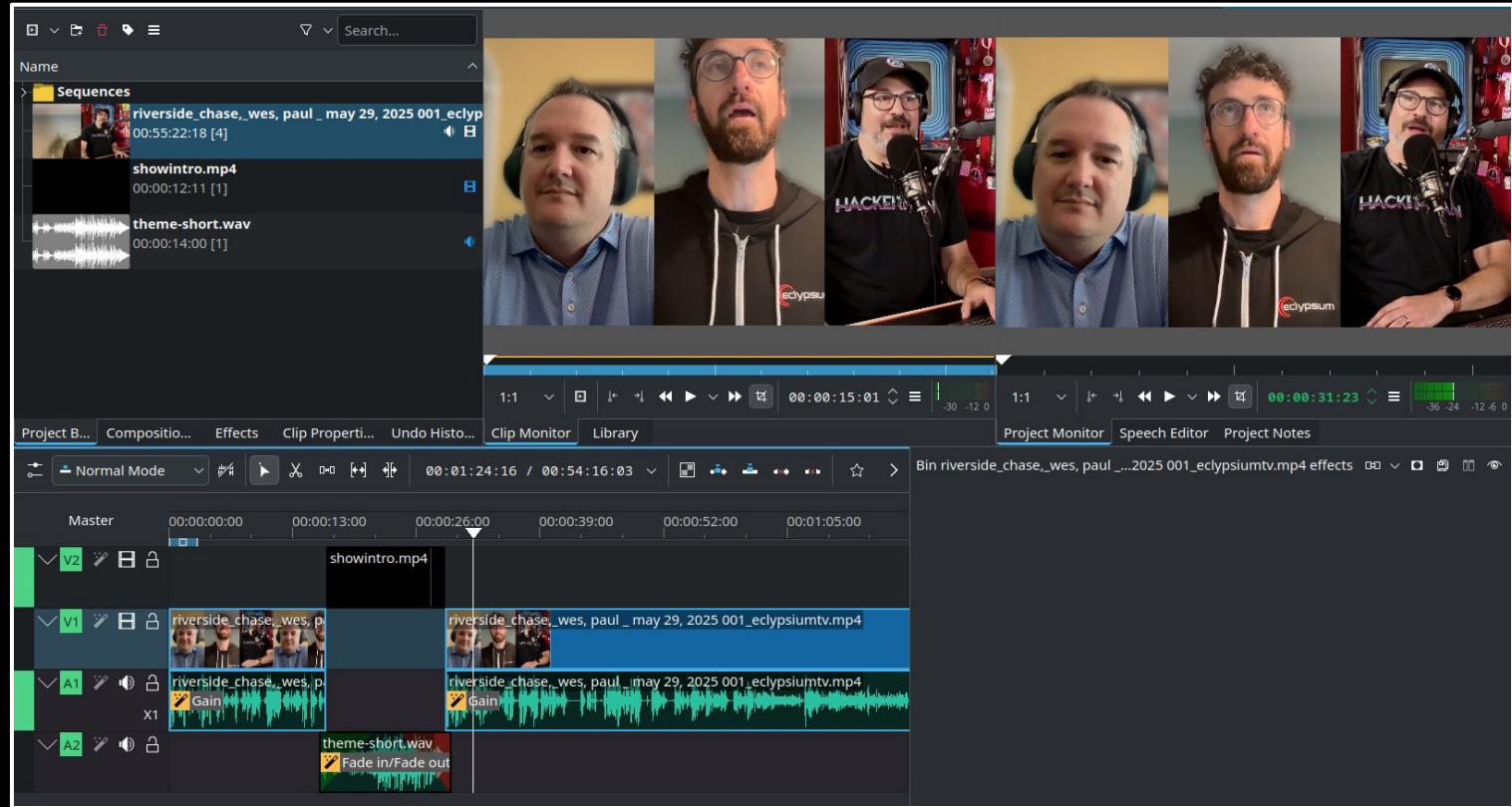
- Use ONLYOFFICE or Libreoffice
  - Both allow you to edit PDF documents (and sign them)
- Google and MS allow you to run all the office applications in a web browser (including Teams)
- TIP: MS Edge runs great on Linux and lets you link your MS account!



# \$ Software

- **Audio Editing** - Audacity, Aurdor
- **Video Editing** - Kdenlive
- **Communications** - Slack, Discord, Signal, Teams (browser or unofficial clients), Zoom, Pulse SMS
- **Browsers** - Chrome, Firefox, Brave, Edge
- **Music** - Spotify, YouTube Music (unofficial apps exist)
- **Photos** - Gimp (now with GTK3 and a huge update)
- **Development** - Vscode/Vscodium, Arduino, Jetbrains Suite
- **Virtualization** - VMware, KVM, and I suppose VirtualBox
- **3d Modeling/Printing** - Bambu Studio, Blender, OpenScad

# \$ Kdenlive is impressive!



# \$ Tip: Bambu Studio Needs Tweaking

```
# My bambu studio startup script - Disables dark mode, clears cache, etc...

export WEBKIT_DISABLE_DMABUF_RENDERER=1

export GALLIUM_DRIVER=zink

export MESA_LOADER_DRIVER_OVERRIDE=zink

export __GLX_VENDOR_LIBRARY_NAME=mesa

export __EGL_VENDOR_LIBRARY_FILERAMES=/usr/share/glvnd/egl_vendor.d/50_mesa.json

export GTK_THEME=Adwaita:light

rm -fr ~/.cache/bambu-studio

bambu-studio
```

Note: This file is on my Github repo for this talk.

# \$ Meetings?

I've successfully done video chats and webinars on:

- ✓ Google Meets
- ✓ Zoom
- ✓ Teams (Browser or Unofficial Clients)
- ✓ Brighttalk

**NOTE: You need Windows to be a presenter on GotoWebinar (I have not had to use this in some time)**



[OBSBOT Meet 4k Webcam](#)

# \$ Virtualization Tips

- VMware is free! I keep a Windows VM to run Windows-only software and update firmware for select hardware (Cameras, Audio interfaces, etc..)
- KVM and Libvirt - Amazing speed and agility, fully scriptable (bit of a learning curve)
- Containers - Run natively on Linux!



# \$ See Github For KVM Install Notes

The screenshot shows a GitHub repository page for 'Linux/Desktop\_Security\_Pro' with the file 'kvm-qemu-libvirt.md'. The page has a dark theme.

**Notes**

These are just some notes and example commands, experimental, use at your own risk!

**Client**

```
ssh-copy-id -i ~/.ssh/mykey hostname
ssh -i ~/.ssh/mykey hostname
vi config

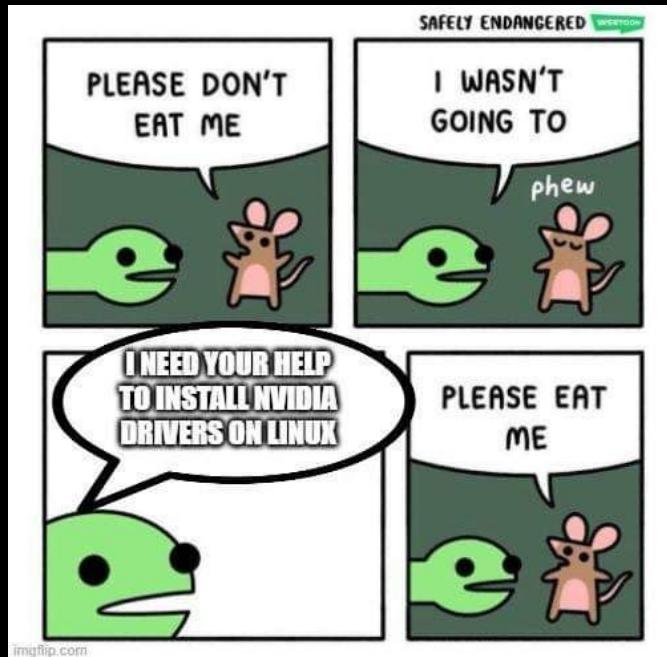
pamac install openssh-askpass
pamac install x11-ssh-askpass
virt-manager -c 'qemu+ssh://paulda@hostname/system?keyfile=mykey'
```

**Server**

```
sudo apt install qemu-system-x86 libvirt-daemon-system virtinst virt-manager virt-viewer ovmf swtpm qemu-utils gu
sudo systemctl enable libvirtd.service
sudo virt-host-validate qemu
sudo systemctl enable --now tuned
tuned-adm active
```

# \$ Display Drivers

- NVIDIA drivers are not as problematic as the memes indicate
- NVIDIA NOVA driver - Open-source, developed in Rust by Red Hat, supports RTX 2000 series and later
  - Like many of these things, some are optimistic, and some are skeptical...
- Kernel 6.15 - “*two thirds of the patch being driver updates*”



# \$ Hardware Support

- This has gotten MUCH better, but older hardware is still an area where Linux shines
- You may just have to wait a bit for developers to figure it out (E.g., Screen brightness on my Framework 13)
- Running newer kernels helps...

## Minimum Requirements For Linux



**Tip:** Reboot after kernel updates as sometimes new USB devices will not be recognized.

# \$ Newer Kernels Have Better Hardware Support

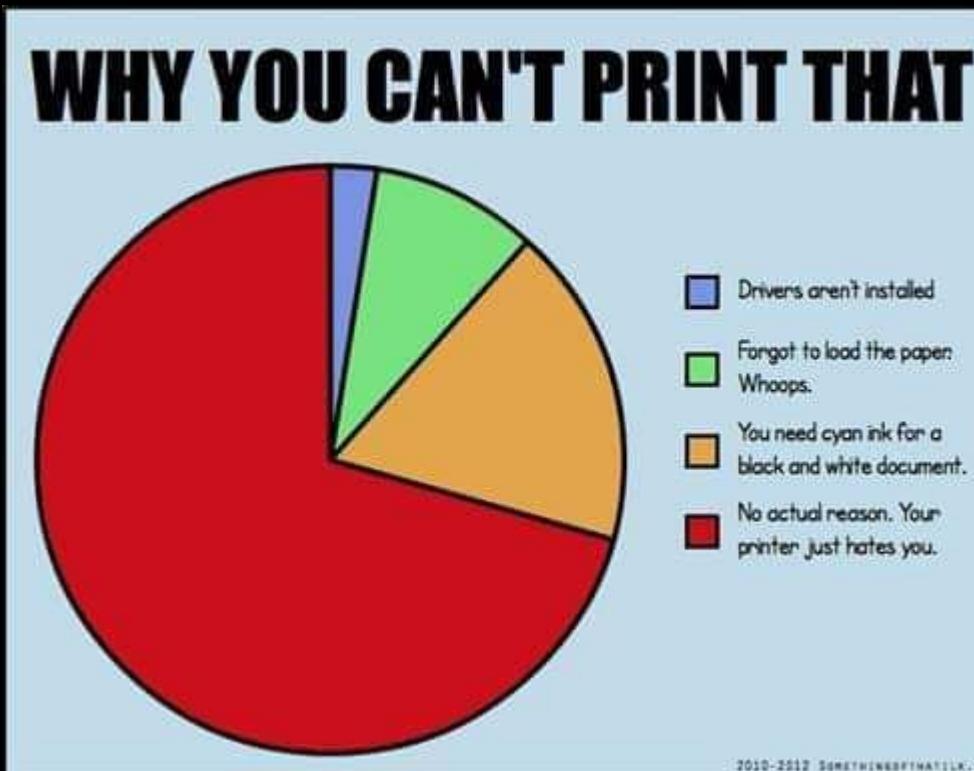
## Hardware Support and Kernel Infrastructure

Linux 6.15 significantly expands hardware compatibility and kernel infrastructure:

- **Apple Touch Bar:** Dedicated drivers now support both Intel and Apple M1/M2 MacBook Pros, enabling backlight, touch interaction, and function key display.
- **Samsung GalaxyBook:** New drivers provide full ACPI platform support, battery management, and function key handling.
- **Game Controllers:** Improved support for Sony PlayStation 5, Xbox, and Turtle Beach controllers, as well as new drivers for racing and flight simulator peripherals.
- **Intel Killer E5000 Ethernet:** Now supported with minimal code changes.

## \$ I can't print

- Varies greatly per distribution and printer model
- Most users can't print, regardless of OS
- When I need to print, I add the file to Google Drive and use my phone
- **Printers hate you regardless of OS**



# \$ I Have A Life

- I do too, I still use Linux
- Sometimes I blame Linux, but it's user error or hardware failure
- Windows and Mac users still:
  - Can't join the meeting due to a technical problem
  - Have USB devices that don't always work (power/bandwidth issue typically)
  - Get blue screens of death
  - Have to apply updates that take a long time



# \$ Gaming

The screenshot shows the ProtonDB homepage with a dark background. At the top left is the ProtonDB logo with a red hexagon icon. To its right is a search bar containing the placeholder "Search games...". Above the search bar are navigation links: EXPLORE, CONTRIBUTE, NEWS, DASHBOARD, and HELP. The main content area features a welcome message: "Welcome to your home for crowdsourced Linux and Steam Deck game compatibility reports!". To the right of this message are four categories with their respective counts:

Category	Count
Chromebook Ready Games	176
Deck Verified Games	6,290
Games on ProtonDB	11,296
► recommended by three or more	15,258
► recommended by two or more	25,157
► recommended by at least one	

- Proton has advanced Linux gaming in a huge way!
  - “*a compatibility layer developed by Valve allowing Windows games to run on Linux systems. Combination of Wine, DXVK (DirectX to Vulkan graphics API converter), and other tools.*
- Visit <https://www.protondb.com/> for a searchable database of games that run on Linux
- You can install Steam on Linux or even use SteamOS
- Note: Some games require Windows, UEFI, and/or Secure Boot to support Anti-Cheat...

# \$ I Don't Want To "Fiddle"

- You have to "Fiddle" less today as:
  - Many people are maintaining desktop software in AUR, Snap, AppImage, and Flatpak
  - There are countless Linux distributions designed for easy desktop use (EndeavorOS, Linux Mint, etc...)
  - Sometimes you just have to wait until developers fix integration bugs (e.g. OBS Studio, virtual cameras, and newer kernels)

How different OS users react to error message appearing:

Windows	
MacOS	
Linux	 It's showtime... <small>www.linux.com</small>

**\$ I tried, it didn't work out...**

- Try it again!
- Don't try (again) if:
  - Everything has to work perfectly
  - I do not want to learn Linux as it has little or no value to my career path
  - I am so happy with Microsoft/Apple I see no reason to switch



# \$ I Don't Want To Compile Anything

- Most software is compiled and packaged for you
- The Linux kernel as packaged by your Linux distribution is perfectly fine for 99.99% of the users, no need to tweak and re-compile
- Software does compile during installation and (mostly) you don't have to mess with it
- You CAN compile something if you need to

**Tip:** Don't challenge yourself to make something work outside the given scope. E.g., if software recommends "X, Y, Z", use that in a VM or container. Example: EMBA

# Why Linux Is A Great Choice For Security Professionals



# \$ Keeping Your Skills Sharp

- I actually enjoy when I run into a problem as its an opportunity to learn something new
- Updating your system, reading release notes, studying previously encountered problems, following instructions on how to update components adds to your knowledge!

**Tip:** To avoid downtime, update frequently, read the update release notes, if possible have multiple systems for backup, backup your system, install at least 4 kernels as backups.

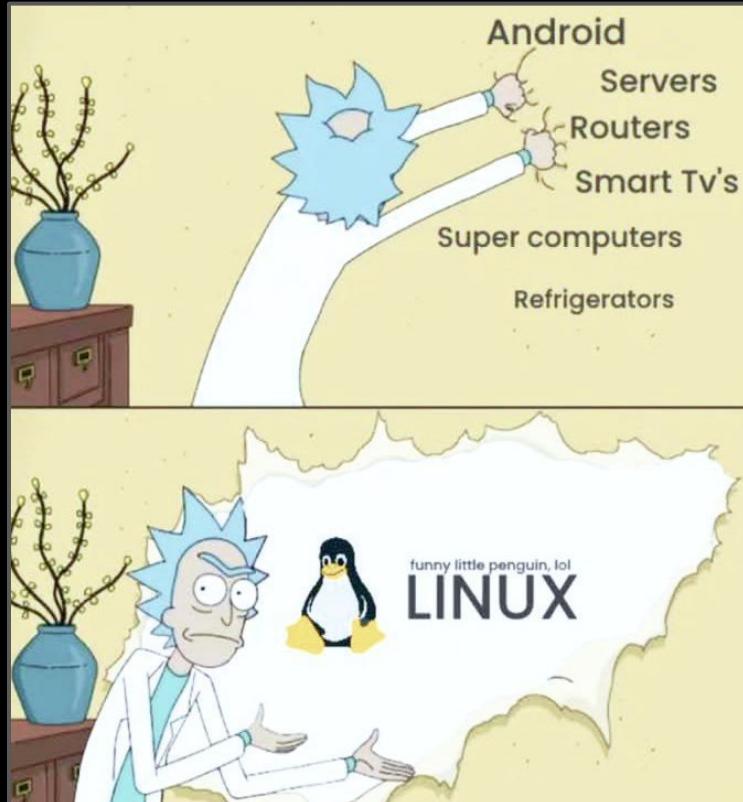
Windows: has a complex and graceful shutdown process to make sure programs close correctly

Linux:



# \$ Applying Linux Your Skills

- Threat actors are targeting Linux-based devices more than ever
- Network and security appliances are largely Linux-based systems
- ARM-based Linux devices are everywhere, and getting hacked all the time
- Linux malware typically lives-off-the-land, making Linux knowledge essential for incident response, forensics, and detections



# \$ Security Tools On Linux

- Nmap - From a container with Vulners
- Nuclei - Also from a container with templates in a Docker volume
- Other security tools in AUR include:
  - Subfinder
  - Massdns
  - Dnsx
  - Uefitool
  - So many more...

**Tip: Use pre-built packages, containers, VMs, and Python virtual environments to avoid conflicts with your system software.**

```
FROM ubuntu:25.04 as builder
ARG nmap_ver=7.95
RUN set -eux; \
    apt-get update; \
    apt-get install -y --no-install-recommends \
    build-essential \
    automake \
    libgcrypt20-dev \
    openssl \
    zlib1g \
    ca-certificates \
    libssh-4 \
    liblua5.2-dev \
    libssl-dev \
    libssh2-1-dev \
    curl \
    git && \
    curl -fL -o /tmp/nmap.tar.bz2 https://nmap.org/dist/nmap-${nmap_ver}.tar.bz2 && \
    tar -xjf /tmp/nmap.tar.bz2 -C /tmp && \
    cd /tmp/nmap* && \
    ln -s /usr/bin/automake /usr/local/bin/automake-1.16 && \
    ln -s /usr/bin/aclocal /usr/local/bin/aclocal-1.16 && \

```

**Tip: This is my Nmap/Vulners multi-stage container build. It is also on the presentation Github.**

## Compiling Nmap and retrieve the latest Vulners.

\$

```
./configure \
--prefix=/opt \
--sysconfdir=/opt/etc \
--mandir=/opt/share/man \
--infodir=/opt/share/info \
--without-zenmap \
--without-nmap-update \
--without-ndiff \
--without-nping \
--without-ncat \
--with-openssl=/usr/lib \
--with-liblua=/usr/include && \
make && make install && \
git clone https://github.com/vulnersCom/nmap-vulners \
/opt/share/nmap/scripts/vulners && \
/opt/bin/nmap --script-updatedb
```

## Final stage build!

\$

```
FROM ubuntu:25.04
```

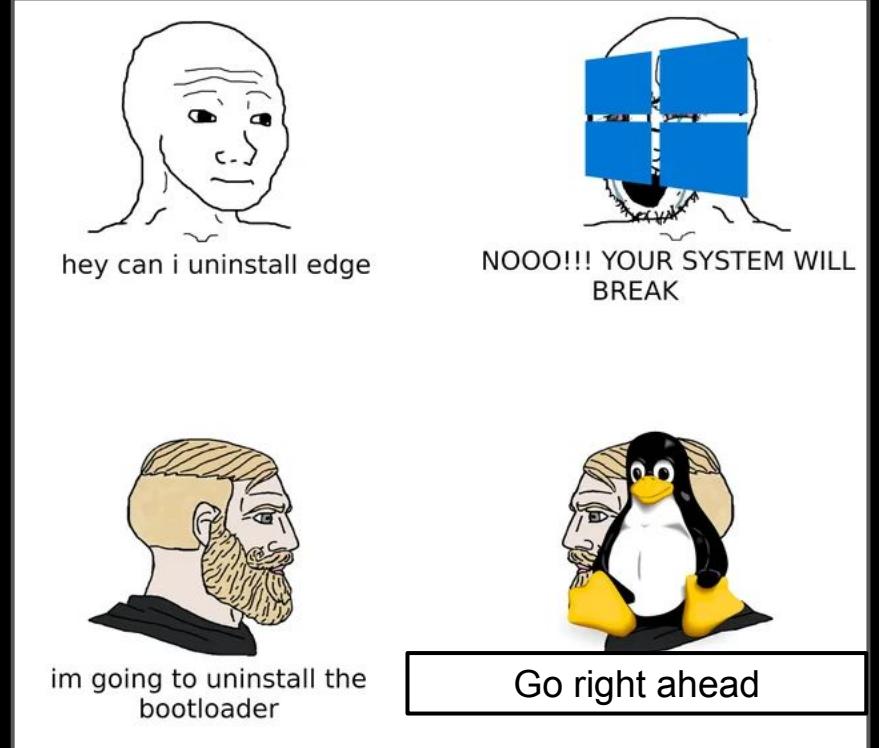
```
RUN apt-get update && \
    apt-get install -y --no-install-recommends \
        libgcrypt20 \
        zlib1g \
        libssh-4 \
        liblua5.2-0 \
        libssl3 \
        libssh2-1 \
        ca-certificates && \
    update-ca-certificates && \
    rm -rf /var/lib/apt/lists/*
```

```
COPY --from=builder /opt /opt
```

```
ENTRYPOINT ["/opt/bin/nmap"]
```

# \$ Freedom

- If you want to modify or customize something, you can
- Less likely to be forced to upgrade hardware/software
- Note: For many the primary reason to run Linux is privacy.



**Tip: Just because you can, doesn't mean you should. E.g., My friend told me not to try Autopsy on Linux. He was correct (I tried and failed LOL)**

# \$ Which Linux Distributions Should I Use?

- Arch based - I love these for the vast software repository (AUR)
- Ubuntu Based - A little more polished (E.g, printing works) great for specific applications
- Others - Stick to what is popular
- Linux from scratch, Gentoo, even straight Arch can be VERY TEDIOUS

Newbie: So which Linux distro should I use first?

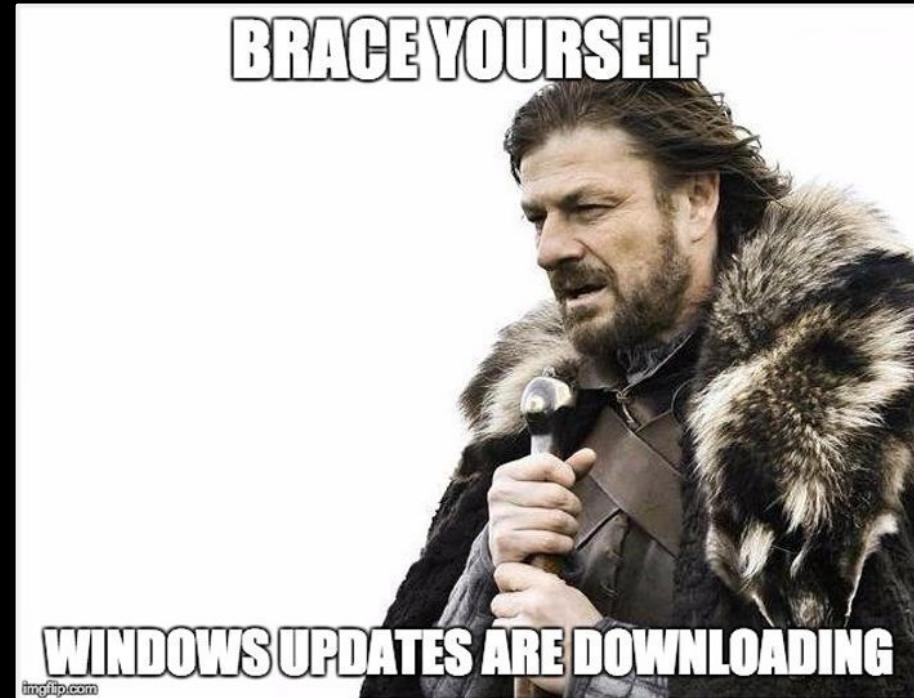
Linux users: ...



**Tip: Do not use Kali Linux as your desktop.**

# \$ Updates Are Important

- Updated all 6 Linux boxes before the coffee was ready
- Windows laptop took almost all afternoon...
- Windows VM will not apply updates, errors out every time
- **Bonus:** you get to test new vulnerabilities, exploits, and remediation (E.g. GRUB2)



# \$ The Update Script

PSW #877 technical segment features a complete tutorial on this script, topgrade, and other things to consider when upgrade Linux!

My Manjaro update script is in the Github!

```
# Perform a full update
# Refresh the mirrors list and select the fastest ones
# Then upgrade packages, including AUR, allow Pamac to downgrade if needed
# Allow refresh the package database for good measure

echo "Performing update..."
echo "-----"
sudo pacman-mirrors -f ; pamac update -a --enable-downgrade --force-refresh

# List any packages that require a rebuild:
echo "The following packages may require a re-build:"
echo "-----"
checkrebuild

echo "The following pacnew files may require attention:"
echo "-----"
pacdiff -o

# Check for firmware updates:
echo "Checking for firmware updates with fwupd"
echo "-----"

fwupdmgr refresh
fwupdmgr get-updates
```

## \$ Conclusion

- Give Linux another shot, it's much better now
- Get involved with the <https://endof10.org/> initiative
- Did I mention **I use Arch BTW?**



## \$ The End

My website:

<https://securitypodcaster.com>

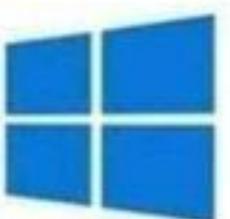
Github for this presentation:

[https://github.com/pasadoorian/Linux/Desktop\\_Security\\_Pro](https://github.com/pasadoorian/Linux/Desktop_Security_Pro)

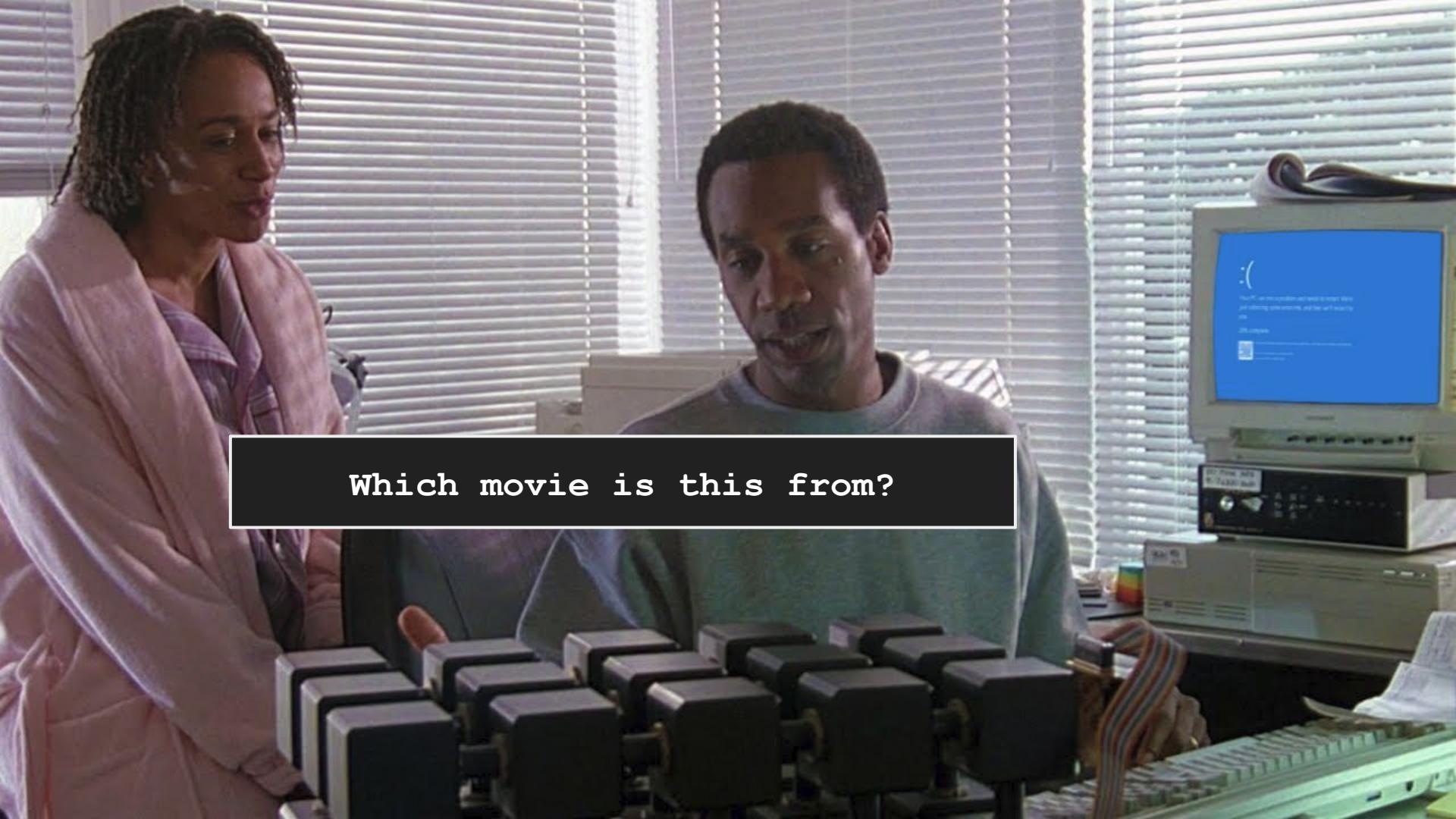
Podcasts: Paul's Security Weekly, Eclypsium's Below The Surface

New: Hacker Syndicate (BETA)  
Live Stream (follow my socials for schedule)

## License agreements of different operating systems

	 Ubuntu	 Mac OS
	<p>I promise that I will tell every person without asking why Linux is so much better than every other operating system.</p> <input checked="" type="checkbox"/>	

**Bonus  
Memes**

A scene from the movie 'The Matrix' set in a server room. Trinity, played by Laurence Fishburne, is on the left, wearing a light-colored jacket over a dark shirt, looking towards the camera. Neo, played by Keanu Reeves, is in the center, looking slightly down. In the background, there are rows of computer monitors displaying a blue screen with a sad face icon and error text. A keyboard is visible in the foreground.

Which movie is this from?

\$



which movie is this from?

ChatGPT: WRONG!

The image you've shared is a scene from the 1995 movie ***Hackers***. However, it's been digitally altered—the original film did not feature a "blue screen of death" (BSOD) or a Windows crash screen, as shown on the CRT monitor. That detail is anachronistic and likely added as a joke or meme.

The scene shows the character **Darryl "Dade" Murphy's father**, played by actor **Laurence Mason**, talking with his wife. The unusual keyboard in the foreground is also a recognizable prop from the film, often associated with the flamboyant computer setups used by the hacker characters.

# \$ AI Is Hilarious

## Perplexity: WRONG!

### which movie is this from

[Answer](#)[Sources · 11](#)[Tasks](#)[youtube](#)[Screens of Death \(Old Video - New Videos in...\)](#)[I am getting the blue screen of death every time I try to...](#)[The Great Disney Movie The Computer Wore Tennis Shoes \(1969\)](#)

This image is from the 1999 movie *Office Space*. The scene features the character Michael Bolton (played by David Herman) and Samir Nagheenanajar (played by Ajay Naidu) in their office. The computer screen in the background humorously displays a modern "blue screen of death" (BSOD), which is anachronistic for the era of computers shown, adding to the comedic effect. The film is well-known for its satirical take on corporate culture and office life, and this particular scene is often referenced for its depiction of outdated technology and workplace frustrations.

# \$ Hat Tip: Adrian Sanabria



TERMINATOR 2: JUDGMENT DAY, Joe Morton,  
1991. ©TriStar Pictures/courtesy Everett Collection...

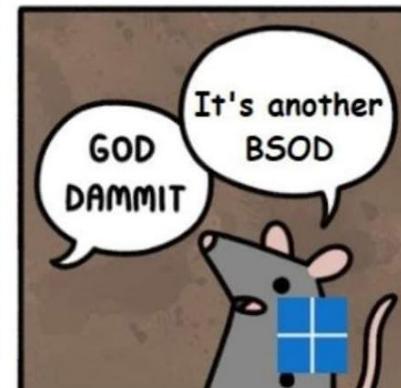
Visit >

Get this image on: [Alamy](#) | [License details](#)

Want to know where this information comes from? [Learn more](#)

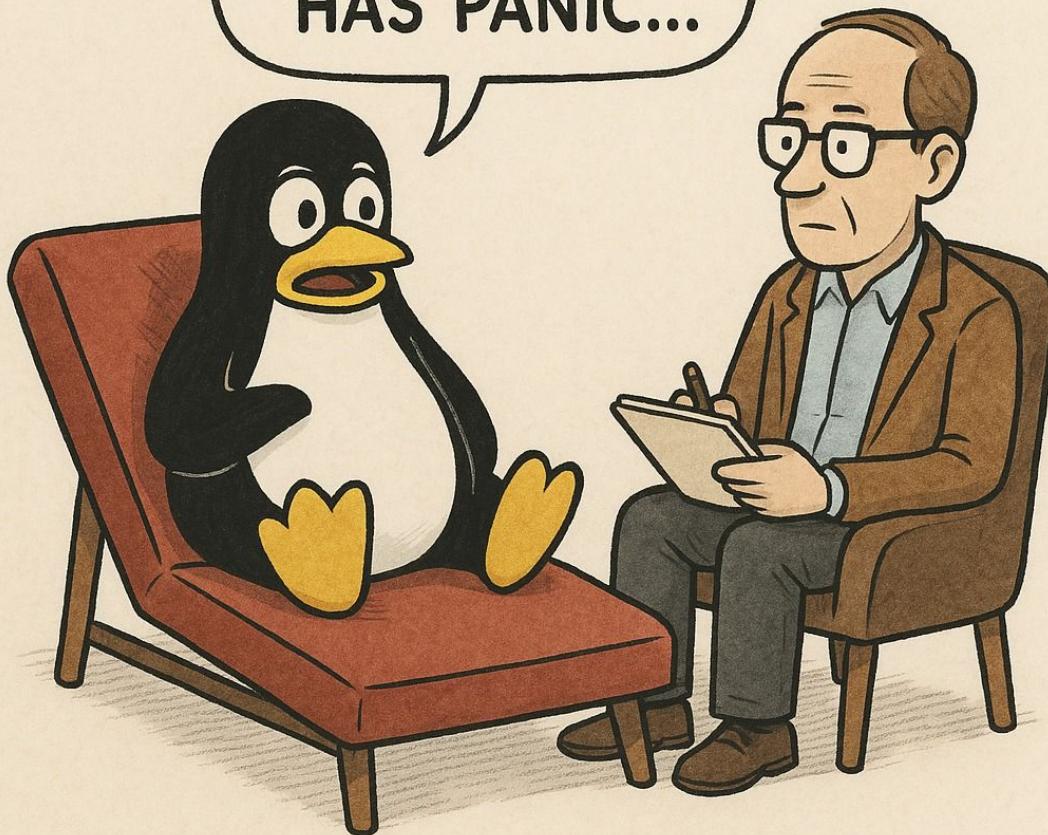
Share

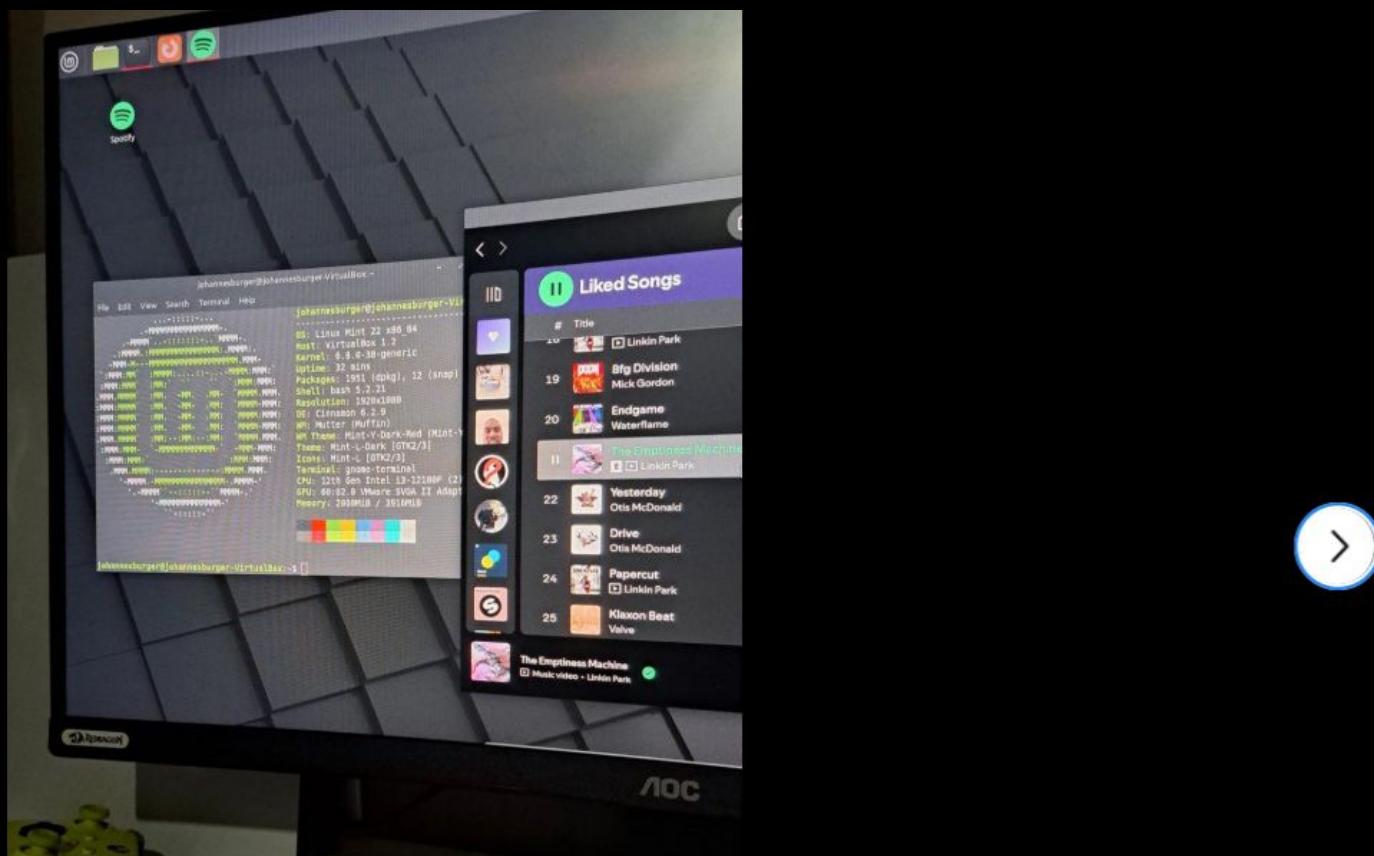
Save



\$

THE KERNEL  
HAS PANIC...





Bang Chris Yan  
March 30 at 10:42 PM ·

It took me about 40 minutes to install spotify on Linux Mint as a lifelong Windows user. Turns out the memes were accurate all along

775

380 14

All comments ▾

Jordan JB  
sudo apt update (or install snap, but you need to delete the file in Linux Mint which prevents the install of snaps).  
then...  
sudo apt install spotify -y (for yes confirmation).... See more

1d Like Reply Share Edited 71

View all 27 replies

Bui Phuc  
40 minutes while you can just install it from software manager or

**If you tweak  
Linux to look like  
Windows, you  
need therapy.**

\$



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

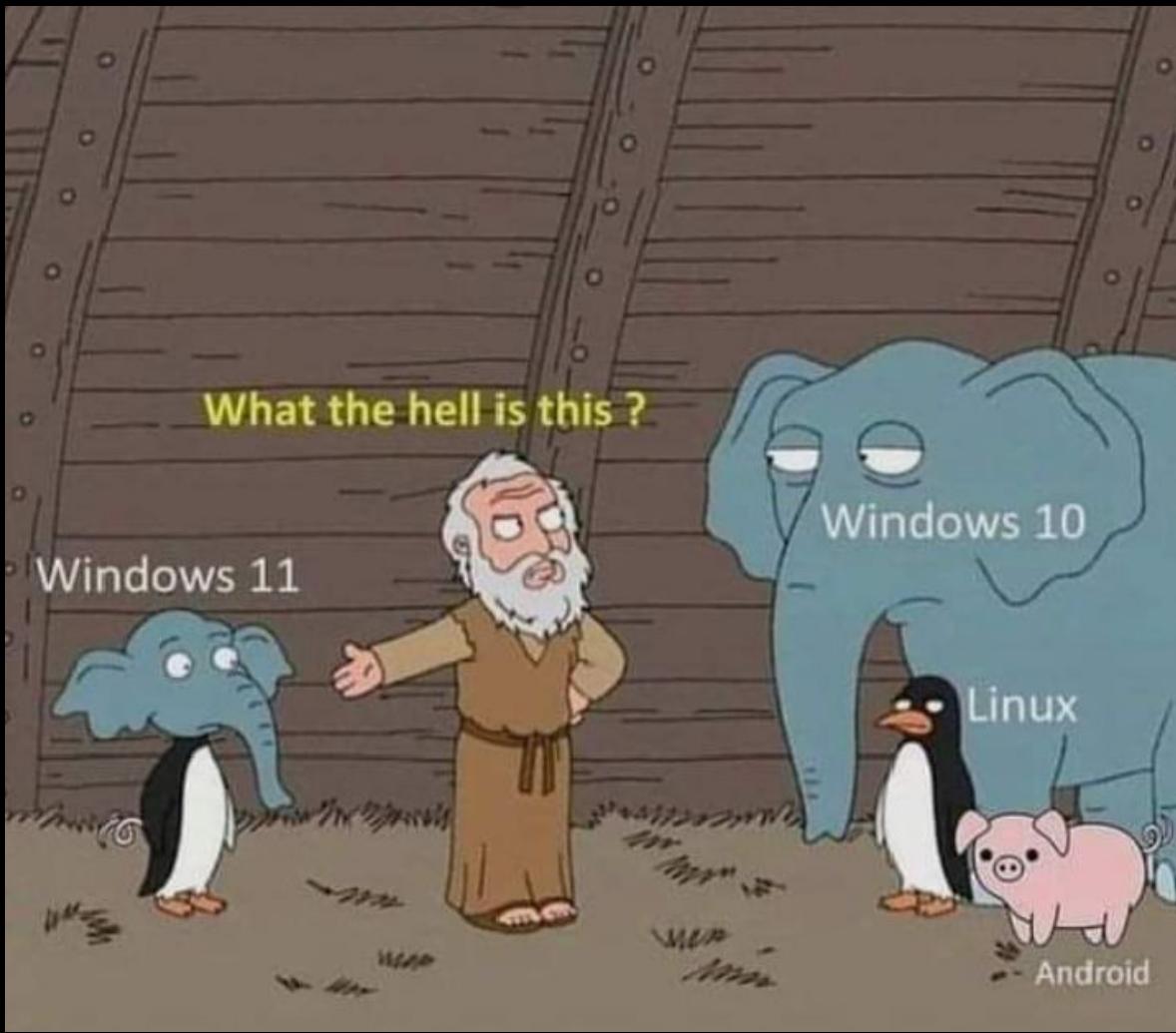


For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

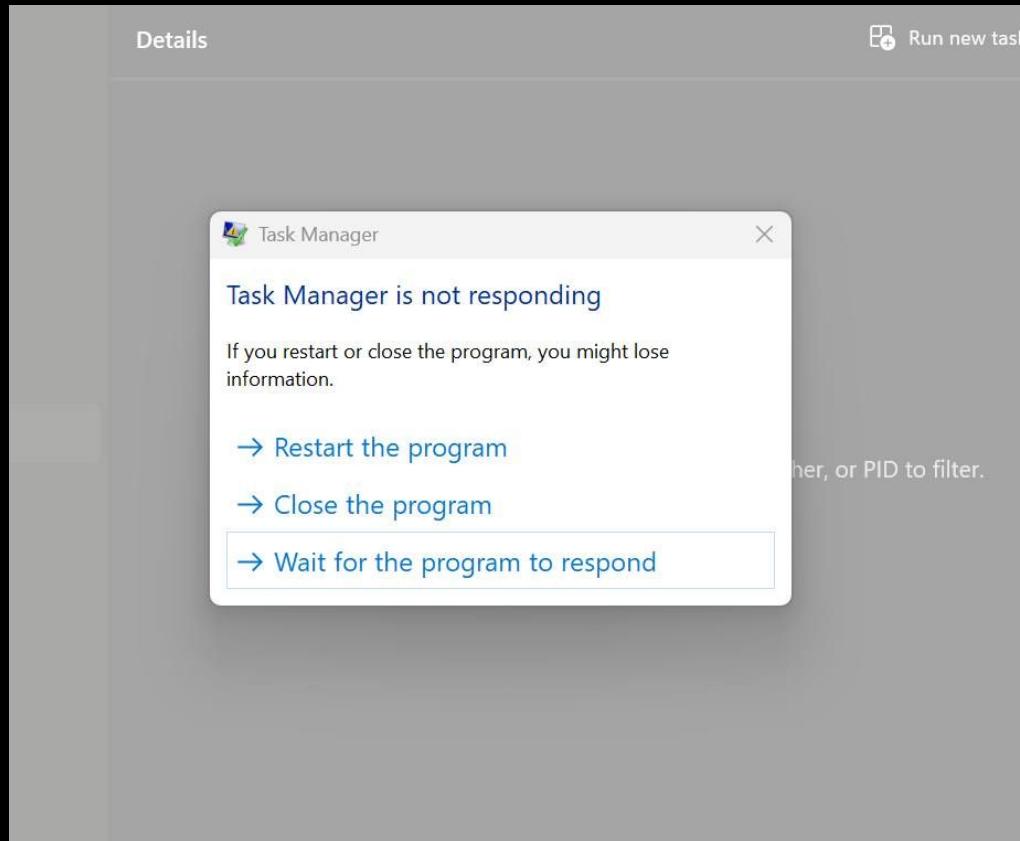
If you call a support person, give them this info:

Stop code: CRITICAL\_PROCESS\_DIED

\$



# \$ You Were The Chosen One!



\$

You're stuck on a 10 hour flight  
Where are you sitting?

guy who really likes  
to talk about linux

1



hungry pack of  
wolves



Microsoft  
Gives You Windows

LINUX

Gives You The  
Whole House!

@Coder



\$

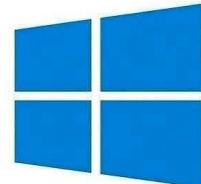
2020



DON'T FORCE ME  
TO INSTALL 10



2025



Windows 10  
DON'T LEAVE  
ME



# The evolution of the trash icon



1995



1998



2000



2001



2006



2015



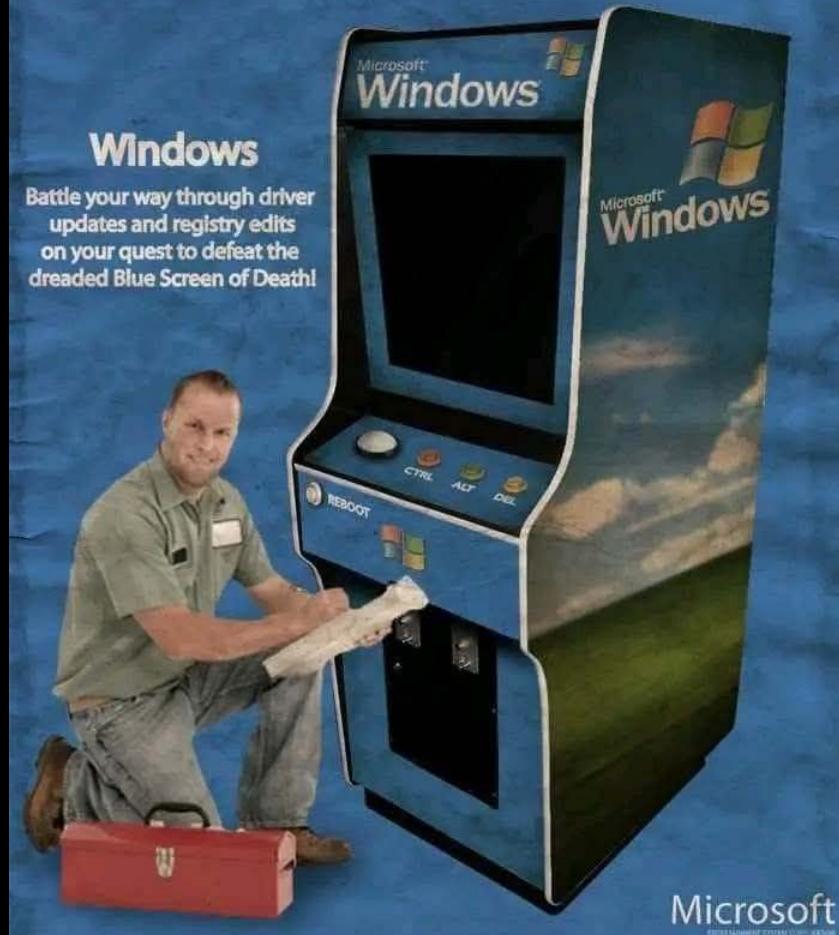
2024

Can YOU make it work?

\$

## Windows

Battle your way through driver updates and registry edits on your quest to defeat the dreaded Blue Screen of Death!



Microsoft  
ENTERTAINMENT SYSTEM ©1998 Microsoft

nixCraft boosted



Gareth Halfacree

@ghalfacree

10h

Dear Microsoft. Here is a list of things I want the Start Menu to do:

- \* Show my installed programs
- \* Search my local files
- \* Provide access to system settings

Here is a list of things I do \*not\* want the Start Menu to do:

- \* Show the weather for a randomly-selected town near my network's public IP infrastructure
- \* Show tabloid headlines
- \* Show programs I \*don't\* have installed
- \* Search the web via Bing
- \* Show adverts(!)
- \* Attempt to engage me in conversation with a hallucinating LLM

Thanks.



122



I'm sorry but this is clever as f



Global Stat

@[REDACTED]

when you grab the Windows mug but  
your gf takes the Mac OS mug

\$

\$

