

[Skip to main content](#)

r/linuxquestions

[Search in r/linuxquestions](#)[Log In](#)

r/linuxquestions • 4 yr. ago

Redcurrent19



What can a beginner do to secure their system?

As the title suggests, I'm a beginner Linux user. I'm currently running Manjaro and want to make sure my system is secure. Currently, I have:

- Enabled UFW and set it to deny all incoming
- Regularly update my system
- Have some common sense when browsing the web
- Have an Adblocker
- Have Clam AV (No additional pgp signatures added yet)

I don't download a whole lot of software and really just program some software and games on it or watch some youtube. Am I being paranoid or am I still running a completely unsecured system?

Also, I'm not going to the lengths of doing stuff like installing Qubes OS. I want some basic security and I'm just looking for some key things I might have missed.

Thanks in advance!

Edit: Wow, this post really blew up! I want to thank everyone for their time and answers, I just can't possibly go through and respond to all. Ill try my best to read through all of them and want you to know that I really appreciate the support!



Archived post. New comments cannot be posted and votes cannot be cast.

160

90

[Share](#)[Single comment thread](#)[See full discussion](#)

muchTasty • 4y ago • Edited 4y ago

[Skip to main content](#)[Log In](#)

- Set up automatic screen locking.
- Use Full-disk encryption.
 - LUKS is linux native and can be simply installed with `apt-get install cryptsetup`
- Use a password manager like BitWarden.
- Use sudo, not su. If you've got a "regular" user account sudo is most likely enabled by default.
 - With that I mean you don't want to set a separate root password but use sudo to elevate instead.
- If you've got SSH enabled, only use public key authentication.
 - Additional SSH hardening [here](#)
- If possible and feasible, use a [YubiKey](#) or similar
- You can use something like [PiHole](#) and add blocklists for malicious hosts. (that requires some more setup though.)
 - Alternatively you can use your own-built setup with dnsmasq and some custom lists (which is basically what PiHole is).
- If you've got a modern enough system: use EFI and EFI's [SecureBoot](#) feature
- In your web browser the following extensions can provide additional protection:
 - Ghostery (**caution** see [u/ConfidentVegetable81's](#) response below regarding Ghostery)
 - NoScript
 - HTTPS Everywhere
 - uBlock Origin
 - EFF Privacy Badger
 - Containerized tabs
 - uMatrix
 - Decentraleyes
- Some additional [FireFox hardening](#)

Keep in mind the list below is pretty advanced, and you shouldn't just go tinkering with it unless you have a decent understanding of what you're doing:

- Most linux distro's these days utilise Systemd. You can use systemd's functionality to greatly reduce the permissions a service can use.
 - <https://github.com/alegrey91/systemd-service-hardening>
- Disable unneeded kernel modules
 - You don't need things like SCTP, DCCP, NFS, etc. on a regular desktop.
- Enable and configure AppArmor or SELinux
- Make sure at least /boot and /tmp are on separate partitions and set the `nosuid`, `noexec` and `nodedv` flags
- Look into sandboxing - firejail is popular but has some downsides when it comes to vulnerabilities. Personally I'd go for [bubblewrap](#) because I don't have to run that as root, where I do have to run firejail as root.

Here are some good reads and pointers:

<https://madaidans-insecurities.github.io/linux.html>

[Skip to main content](#)[Log In](#)<https://madaidans-insecurities.github.io/security-privacy-advice.html>

For AppArmor:

<https://wiki.archlinux.org/title/AppArmor><https://medium.com/information-and-technology/so-what-is-apparmor-64d7ae211ed>

Be warned some measures may break things, try out things one at a time so you know what to reverse if your system won't boot.

That's all on-top-of-my-head stuff I could think of, if you want more just poke me and I'll conjure up some things.

Edit: Added FDE (I forgot that at first :\$) Edit2: Added apparmor and bubblewrap links Edit3: Fixed browser addons after comment

131 ...



ConfidentVegetable81 • 4y ago

Ghostery

AFAIK Ghostery is not recommended because it violates your privacy. EFF Privacy Badger does the same without all the botnet. Don't use Ghostery.

17 ...



muchTasty • 4y ago

I couldn't really find anything on that with a quick duckduckgo-ing but it surely sparked my interest, so I'm gonna dig into that myself.

Thanks for the heads up, I edited the post to reflect your warning :)

3 ...

1 more reply



Redcurrent19 OP • 4y ago

Thanks so much! I'll set up a VM and try the "Yeah I hope this won't brick my system" settings, and as for the rest I'll do those things directly on my machine.

This is a really extensive list so I'll go over everything and reply again once I'm through it. Thanks so much for this detailed reply and see you again soon!

14 ...



[deleted] • 4y ago

That's always good and I do it that way for years: keep an identical configured VM around, make a snapshot, and try out one change at a time. If it works well enough: implement on main system. Make another snapshot, try out the next thing you want to test.

[Skip to main content](#)[Log In](#)**muchTasty** • 4y ago

You're welcome - in the chance I miss your response, feel free to send a PM.

3

**bionor** • 4y ago

Though what they said was very good, your'e already doing good. Applying some good sense like you already show is halfway there. You're good. Do what they said if you want to take it to the next level.

3



4 more replies

**zpangwin** • 4y ago • Edited 4y ago

[Skip to main content](#)[Log In](#)

- Use `sudo`, not `su`. If you've got a regular user account `sudo` is most likely enabled by default.

I just wanted to add that I think what was meant here was that in general it is better to run a one-off elevated command rather than running `su -` to login as root and run everything through the root terminal. BUT that a root terminal isn't inherently insecure *for someone like a sysadmin that knows what they are doing**; it's just that it is entirely on the user to follow safe practices (e.g. only running commands thatt are absolutely necessary as root, not copy-pasting things off the web, logging out when done, etc). But for a regular user, `sudo` is a better "default" way to run things.

Also a few other things I didn't see mentioned:

- Using `firejail` to run things like browser and wine processes while providing some level of sandboxing.
- Configuring `fail2ban` to make things like bruteforcing your ssh login much more difficult
- Enabling AppArmor (or SELinux) if they are not already... you can check if a security module is loaded by your kernel by running either `grep -Pi '(selinux|apparmor)' /sys/kernel/security/lsm` or `grep -Pi 'CONFIG_SECURITY_(APPARMOR|SELINUX)=y' /boot/config-$(uname -r)`. You can check if the AA / SEL are actually enforcing by running `sudo aa-status` or `getenforce` respectively.
- In addition to using a Password Manager, also use randomly generated passwords with a sufficient amount of entropy. I use KeePass / KeePassXC instead of BitWarden (I don't like the idea of storing passwords in the cloud, partly bc I have passwords that I need access to offline); it displays entropy of each password (I assume BitWarden would as well though).
- Use LUKS full disk encryption (cryptsetup package) to protect data against physical theft
- Use a custom ssh port (more important if you are port-forwarding to the internet or doing this on an internet facing-server box. somewhat good idea for a laptop if you ever use public wifi. less important for personal desktops that always connect through a dedicated router and only use ssh on a lan).
- I believe there is also a way to enable realtime memory scans with clamav. They call it On-Access Scanning. I don't necessarily recommend this as to the best of my knowledge, I don't think it has been performance-tuned. But if you want to do it, I believe it is an option. [Here](#) is a link if you are interested. If anyone has actually used this, I would be very interested to know about the performance on a desktop (linked article mentions it but they were also using it on a pi... so not a big surprise there); I haven't gotten around to testing it myself and while I thought I remembered someone saying it wasn't good performance-wise I can't seem to find any links.

Edit: one other thing I was reading that I thought worth considering: Running browser in a app container format such as flatpak. This would basically be as an alternative to the `firejail` suggestion I gave earlier (but I suppose it might be possible to have `firejail` run the flatpak if you really want lol - edit 2: [nope](#)).. [Here](#) is an article comparing the defaults for firefox running in flatpak vs snap (note: if you are just looking at the table, that is only the *defaults* - the article mentions throughout that many of those can be changed in flatpak. not as familiar with snaps as their loop devices thing drives me crazy, so I refuse to even consider them until they stop cluttering my terminal output with that crap.)



7

...

[Skip to main content](#)[Log In](#)



I just wanted to add that I think what was meant here was that in general it is better to run a one-off elevated command rather than running su - to login as root and run everything through the root terminal. BUT that a root terminal isn't inherently insecure for someone like a sysadmin that knows what they are doing*;
it's just that it is entirely on the user to follow safe practices (e.g. only running commands that are absolutely necessary as root, not copy-pasting things off the web, logging out when done, etc). But for a regular user, sudo is a better "default" way to run things.

That's exactly what I meant! - Thanks, I clarified it :)

I agree with the rest of your points too, though I didn't elaborate that much on the ones I listed too ^^

5

...

  4 more replies **[deleted]** • 4y ago

I don't think they could configure SELinux because the docs aren't that good

5

...

  1 more reply [View more replies](#)

New to Reddit?

Create your account and connect with a world of communities.

[Continue with Google](#)[Continue with Email](#)[Continue With Phone Number](#)

By continuing, you agree to our [User Agreement](#) and acknowledge that you understand the [Privacy Policy](#).



r/EngineeringStudents • 5 days ago

I'm not sure I can keep doing this

161 upvotes · 77 comments

[Skip to main content](#)[Log In](#)

798 upvotes · 119 comments



r/outside • 5 days ago

How to decrease game difficulty?

133 upvotes · 34 comments



r/webdev • 4 yr. ago

What are some tools people should be using regularly for front-end development that you wish you were pointed to earlier?

207 upvotes · 94 comments



r/dismissiveavoidants • 9 days ago

Book recommendations for becoming more secure?

34 upvotes · 40 comments



r/ShittySysadmin • 6 mo. ago

Need help. Can't get into computer. Don't know what to do or how to do it.

39 upvotes · 30 comments



r/bulsu • 6 mo. ago

I think I made a mistake by choosing BS Computer Engineering

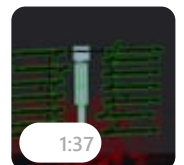
7 upvotes · 25 comments



r/peopleplayground • 2 mo. ago

my compute survived this time

32 upvotes · 10 comments



r/ShittySysadmin • 1 mo. ago

Just deployed my first client server!

104 upvotes · 24 comments



r/AtariVCS • 3 mo. ago

Helping new users who aren't computer nerds.

29 upvotes · 29 comments



r/computerforensics • 11 days ago

[Skip to main content](#)[Log In](#)

r/transguns • 11 days ago

Legal Resources?

38 upvotes · 12 comments



r/DHExchange • 28 days ago

Archive of abandoned large-system software?

24 upvotes · 8 comments



r/osdev • 8 mo. ago

Is making a OS for a custom computer system right for this subreddit?

25 upvotes · 17 comments



r/HueForge • 18 days ago

Delving into the software for the first time

78 upvotes · 7 comments



r/cobol • 4 mo. ago

New to Mainframe, HELP ME OUT

22 upvotes · 61 comments



r/familylink • 14 days ago

U remember secure folder? Help

5 upvotes · 14 comments



r/macsysadmin • 4 yr. ago

What would be the best way to go around installing applications while setting up a new device

12 upvotes · 48 comments



r/rust • 4 yr. ago

Beginner here who doesn't know what to use Rust for looking for advice from those who have done awesome things with it

24 upvotes · 19 comments



r/Phobia • 13 days ago

Is anyone else extremely scared of stuff like BIOS, the windows terminal, blue screen and any type of computer errors?

7 upvotes · 3 comments

[Log In](#)

429 upvotes · 102 comments



r/PetPeeves • 6 days ago

I'll admit I get irritated by people who don't have basic computer skills.

66 upvotes · 58 comments



r/CasualConversation • 1 mo. ago

I'm always kinda shocked by people who don't know how to use computers of any kind

182 upvotes · 127 comments



r/gamedev • 3 mo. ago

I screwed up, and now I have to start over. Has this ever happened to you?

212 upvotes · 181 comments



r/KSPMemes • 1 mo. ago

Really? Right in front of my main KSP install?

207 upvotes · 12 comments



TOP POSTS



Reddit

reReddit: Top posts of August 30, 2021



Reddit

reReddit: Top posts of August 2021



Reddit

reReddit: Top posts of 2021

[Reddit Rules](#) [Privacy Policy](#) [User Agreement](#) [Reddit, Inc. © 2025. All rights reserved.](#)