# Article information:

Linux Hardening Guide | Madaidan's Insecurities
<https://madaidans-insecurities.github.io/guides/linux-hardening.html>

# Article summary:

1. This guide explains how to harden Linux for security and privacy.

2. It is not tied to any specific distribution and provides steps that can be taken to reduce the attack surface of a system.

3. It covers topics such as kernel hardening, mandatory access control, sand-boxing, firewalls, identifiers, file permissions, core dumps, memory safe languages, root account security, IPv6 privacy extensions, partitioning and mount options, entropy sources, distribution-specific hardening and physical security best practices.

# Article rating:

Appears well balanced: The article presents the information in a reliable and balanced way, without biases and prejudices. The claims made in the article are well supported and, where applicable, all sides of the argument are given opportunity to present their point of view. The article appears trustworthy and reliable.

# Article analysis:

The article titled “Linux Hardening Guide | Madaidan’s Insecurities” is an informative guide on how to secure a Linux system from potential attacks. The article is written in a clear and concise manner which makes it easy to understand for readers with varying levels of technical knowledge. The author has provided detailed instructions on how to harden a Linux system as well as explanations of the various techniques used in order to do so.

The article does not appear to have any biases or one-sided reporting as it provides an unbiased overview of the different methods available for securing a Linux system. Furthermore, the author has provided evidence for each claim made in the form of commands which can be used to implement the various techniques discussed in the article.

The article does not appear to be missing any points of consideration or evidence for its claims as it covers all aspects of hardening a Linux system from choosing the right distribution through to physical security best practices. Additionally, there are no unexplored counterarguments or promotional content present in the article which could lead readers astray or give them false information about securing their systems.

Finally, possible risks are noted throughout the article where applicable and both sides of an argument are presented equally when discussing certain topics such as systemd service sandboxing versus gVisor virtual machines. All in all this appears to be a reliable source of information on how to secure a Linux system from potential attacks and should be consulted by anyone looking for advice on this topic.

# Topics for further research:

* Linux security best practices
* Linux hardening tools
* Linux firewall configuration
* Linux privilege escalation prevention
* Linux system auditing
* Linux intrusion detection systems

# Report location:

<https://www.fullpicture.app/item/e3eb4080687f77c0364994293a9e28a7>