Solana Validator Security Best Practices

Being a system administrator for an Ubuntu computer requires technical knowledge of the system and best security practices. The following list should help you get started and is considered the bare minimum for keeping your system safe.

Keep Your System Up To Date

Make sure to regularly update packages in your Ubuntu system. Out of date packages may contain known security vulnerabilities that a hacker could exploit. A good practice would be to update weekly at least. To update your system, do the following:

sudo apt update sudo apt upgrade

DO NOT Store Your Withdrawer Key On Your Validator Machine

Your withdrawer key gives the operator full control of the vote account. It is highly sensitive information and should not be stored on the validator itself.

There are a number of options for withdrawer key management. Some operators choose to use hardware wallets or paper wallets for the withdrawer keypair. Another option is a multisig where each key of the multisig is a hardware wallet or paper wallet. Whichever option you choose, make sure the authorized withdrawer key is stored securely and that it has been generated on a trusted computer (other than your validator computer).

To reiterate, the withdrawer keypair should never be stored on your validator at any time.

DO NOT Run The Solana Validator as a Root User

It may be easier to get started by running your application as root, but it is a bad practice.

If there is an exploit in your system, a hacker could have full access if your Solana application is running as theroot user. Instead, see thesetup instructions for creating a user calledsol and running the application as thesol user.

Close Ports That Are Not In Use

Your system should close all ports that do not need to be open to the outside world. A common firewall for closing ports isufw (uncomplicated firewall). You can find a guide to usingufw fromDigital Ocean .

Eliminate Brute Force Attacks With fail2ban

fail2ban is a network security tool that checks your logs for suspicious login attempts and bans those IP addresses after repeated attempts. This will help mitigate brute force attacks on your serve.

The default setup should work out-of-the-box by doing the simply installingfail2ban :

sudo apt install fail2ban

DO NOT Use Password Authentication for SSH

In addition to installingfail2ban , it is recommended to disable password based authentication for SSH access. SSH key based authentication is preferred. Previous Best Practices: Validator Monitoring Next Validator Guides: Starting a Validator