

Forum:[Hack Forums](#)

Thread: [Whats the most secure way to remote access a PC/Server](#)

Zahidtz - December 10, 2023, 2:54 pm

I own a server in Linux and im wondering whats the most secure way to access it without a problem and with nobody able to get into it except me

Immortal - December 10, 2023, 3:15 pm

Well, to give you exacts I would need to know what distro of linux you are using. But this in general is what Ill recommend.

Enable Strong Authentication

The foundation of server security starts with strong authentication. Create robust passwords and enable two-factor authentication (2FA). Passwords should contain at least ten characters, including special symbols and a mix of uppercase and lowercase letters. Every username should be unique and passwords even more so.

Create an SSH Key Pair

While passwords have their place, Secure Shell (SSH) key pairs offer a more secure means of accessing your servers. SSH keys make brute-force attacks significantly more challenging. They rely on cryptographic key pairs, which are much more secure than passwords. Although they might be less user-friendly, the security enhancement they offer is well worth it.

Keep the System Up to Date

Regularly updating your Linux server is crucial for maintaining its security. New patches and updates address recently discovered vulnerabilities and security flaws. Failing to do so can leave it vulnerable to attacks.

Remove Unnecessary Software

Not all packages are necessary for your server's functionality. The more packages, software, and third-party repositories you add, the greater the scope of attack and the potential for security vulnerabilities. Conduct periodic audits of your software and cybersecurity measures, removing any unnecessary components. Regularly maintaining your software environment reduces the risk of security breaches and ensures optimal server performance.

Disable Root Login

Keeping the root login enabled can pose a security threat, as hackers can potentially use these credentials to gain access to the server. To strengthen your Linux system hardening, you should disable this login.

Check and Close Open Ports

Open ports can expose information about your network architecture, making it susceptible to attacks.

Enable a Firewall

You can create allow and deny rules for receiving or sending traffic from a specific IP address. These rules restrict unauthorized traffic or any movement on the server.

Harden Your Linux system with SELinux or AppArmor

[SELinux](#), Security-Enhanced Linux, is a fantastic security system for Linux. It provides different security policies for the Linux kernel. This overlay allows you to control processes' access to files in the file system. Only a program with the appropriate role can access a specific resource, and even superuser privileges are not relevant. SELinux significantly enhances the security of the Linux system, as even the root user is considered a regular user here. It is used in the Red Hat, CentOS, and Fedora distributions.

The AppArmor system is used in Ubuntu and operates similarly to SELinux. Profiles are created for each application, specifying which files the application can access, while denying access to everything else. For more information on AppArmor, you can refer to [There site here!](#)

Security Audits Are Important

While the tips mentioned above can help you feel more secure while working on hardening your Linux system, new threats can arise at any time. Even the most secure server becomes vulnerable to new threats if it is not updated properly. Of course, software updates are necessary, but a security audit can identify other useful improvements. That's why you should regularly conduct security audits to avoid all security-related issues with your Linux server.

Regularly Create and Maintain Backups

Backups are essential to the security of any system. With backups, you can restore important data in the event of any server intrusion. In Linux, the Rsync application is a popular choice for data backups. It includes several options that allow you to create daily backups or exclude duplicating specific files.

It is well-known for its versatility, making it an excellent choice for a wide range of Linux server protection tactics. Furthermore, backups work best when you regularly test them. Testing ensures that the backups contain the correct (and most recent) files and that you can quickly restore them in case of data loss.

Written by: Artem Karasev

Slight Edits by: [Immortal](#)

grady - December 10, 2023, 4:09 pm

SSH setup with SSH keys.

https://www.wikiwand.com/en/Secure_Shell

<https://www.digitalocean.com/community/tutorial-collections/how-to-set-up-ssh-keys>

ollyhill424 - December 10, 2023, 7:29 pm

I'm not an expert, but setting up a cloudflare tunnel could help too.