**Security Best Practices**

Keeping your Fedora Server secure is crucial for protecting data, users, and services. Whether you’re running a public-facing web server or an internal DNS, adopting security best practices can prevent unauthorized access, minimize risks, and ensure system integrity.

This article covers key **security best practices** you should follow when managing a Fedora Server.

🔑 1. Disable Root SSH Login

Allowing direct login as root is dangerous. Disable it by editing the SSH configuration file:

1. sudo nano /etc/ssh/sshd\_config

Change the following:

1. PermitRootLogin no

Then restart SSH:

1. sudo systemctl restart sshd

👤 2. Use SSH Key Authentication

Password-based logins are vulnerable to brute-force attacks. Instead:

* Generate SSH keys on your client:

1. ssh-keygen

* Copy the public key to the Fedora server:

1. ssh-copy-id youruser@server-ip

Now you can log in securely using your key pair.

🔥 3. Enable the Firewall

Fedora uses **firewalld** by default. Make sure it’s active:

1. sudo systemctl enable firewalld
2. sudo systemctl start firewalld

Use this to allow only specific services:

1. sudo firewall-cmd --add-service=ssh --permanent
2. sudo firewall-cmd --add-service=http --permanent
3. sudo firewall-cmd --reload

🚫 4. Install and Configure Fail2ban

Prevent brute-force attacks by banning IPs that fail authentication multiple times:

1. sudo dnf install fail2ban -y
2. sudo systemctl enable --now fail2ban

Create or modify the jail:

1. sudo nano /etc/fail2ban/jail.local

Enable the [sshd] section and set your preferred ban parameters.

🕵️ 5. Keep Your System Updated

Apply security patches regularly:

1. sudo dnf update -y

You can also automate updates by enabling dnf-automatic:

1. sudo dnf install dnf-automatic -y
2. sudo systemctl enable --now dnf-automatic.timer

🧱 6. Use SELinux (Don't Disable It)

Fedora ships with SELinux enabled for Mandatory Access Control. Check its status:

1. sestatus

Keep it in **enforcing** mode unless you have a very specific reason to disable it.

🔍 7. Monitor Login and System Logs

Watch for suspicious activity:

1. journalctl -xe

Check authentication logs:

1. sudo cat /var/log/secure

You can also set up system monitoring tools like **Logwatch**, **Auditd**, or integrate with a SIEM.

🛡️ 8. Remove Unused Services and Ports

Use this command to list listening services:

1. sudo ss -tuln

Stop and disable unnecessary services:

1. sudo systemctl disable --now servicename

For example, if you're not running FTP:

1. sudo systemctl disable --now vsftpd

👥 9. Use the Principle of Least Privilege

Only give users access to what they need. Use **sudo** instead of logging in as root. For managing sudo access:

1. sudo visudo

📦 10. Verify Software Sources

Install software only from trusted sources or the official Fedora repositories. Avoid random .rpm files or third-party repos unless you verify their integrity and purpose.

🧠 Summary

Security on Fedora Server isn’t just about installing one tool — it’s a mindset and routine. By implementing these best practices, you're taking proactive steps to harden your system against common threats.

✅ Disable root login  
✅ Use SSH keys  
✅ Keep your system updated  
✅ Enable the firewall  
✅ Set up Fail2ban  
✅ Monitor logs  
✅ Remove unused services  
✅ Apply least privilege principles