Ubuntu Server Security Best Practice

Securing a Linux server is crucial to protecting it from various vulnerabilities and attacks. Below is a step-by-step guide to Linux server security best practices:

1. Update the System Regularly

• Keep your system and installed packages up to date to patch security vulnerabilities.

```
sudo apt update && sudo apt upgrade -y  # Debian/Ubuntu
sudo yum update -y  # CentOS/Red Hat
```

Set up automatic updates:

```
sudo apt install unattended-upgrades  # For Debian/Ubuntu
```

2. Create a Non-Root User

• Avoid using the root user for daily operations. Create a non-root user with administrative privileges.

```
sudo adduser username
sudo usermod -aG sudo username  # For Debian/Ubuntu
sudo usermod -aG wheel username  # For CentOS/Red Hat
```

3. Secure SSH Access

• Disable root login via SSH.

Edit /etc/ssh/sshd_config and set:

```
PermitRootLogin no
```

• Use SSH keys for authentication and disable password authentication.

```
PasswordAuthentication no
```

• Limit SSH access to specific IP addresses (if possible).

```
AllowUsers username@ip_address
```

Restart SSH service:

```
sudo systemctl restart sshd
```

4. Set Up a Firewall

• Use ufw (Uncomplicated Firewall) on Debian/Ubuntu or firewalld on CentOS/Red Hat.

```
sudo ufw enable
sudo ufw allow ssh
sudo ufw allow http
sudo ufw allow https
sudo ufw status
```

5. Install and Configure Fail2Ban

• Fail2Ban helps prevent brute-force attacks by blocking IP addresses after several failed login attempts.

Install:

```
sudo apt install fail2ban  # For Debian/Ubuntu
sudo yum install fail2ban  # For CentOS/Red Hat
```

Configure by editing /etc/fail2ban/jail.local and enabling SSH protection:

```
[sshd]
enabled = true
```

6. Disable Unused Services

• Disable any services that you don’t need to minimize attack vectors.

List services:

```
sudo systemctl list-units --type=service
```

Disable services:

```
sudo systemctl disable service_name
```

7. Implement SELinux (CentOS/Red Hat) or AppArmor (Debian/Ubuntu)

• SELinux (Security-Enhanced Linux) or AppArmor provides additional layers of security to limit the access of applications.

• Check the status of SELinux:

```
sudo getenforce
```

• Enable SELinux:

```
sudo setenforce 1
```

8. Enable Automatic Security Updates

• Set up unattended updates to automatically apply security patches.

For Debian/Ubuntu:

```
sudo apt install unattended-upgrades
```

For CentOS/Red Hat:

```
sudo yum install yum-cron
sudo systemctl enable yum-cron
```

9. Configure Log Management

• Ensure that logs are rotated and stored securely to monitor suspicious activities.

Install logwatch:

```
sudo apt install logwatch  # Debian/Ubuntu
sudo yum install logwatch  # CentOS/Red Hat
```

10. Backup Regularly

• Set up regular backups of important files and databases.

Use tools like rsync, tar, or Bacula to create backup scripts.

Ensure backups are stored offsite or in the cloud.

11. Use Strong Passwords

• Enforce strong password policies to prevent easy-to-guess passwords.

Edit /etc/login.defs to define password policies:

```
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_MIN_LEN    12
```

Use pam_cracklib to enforce password complexity.

12. Monitor System Activity

• Install system monitoring tools like top, htop, netstat, and nmap to regularly check resource usage and active connections.

Set up auditd for more detailed auditing:

```
sudo apt install auditd  # For Debian/Ubuntu
sudo yum install auditd  # For CentOS/Red Hat
sudo systemctl enable auditd
```

13. Use Encryption

• Encrypt sensitive data in transit and at rest.

• Use SSL/TLS to encrypt web traffic.

• Enable disk encryption for sensitive files (e.g., LUKS on Linux).

14. Install Antivirus and Anti-Malware

• Though Linux is less prone to malware, it’s still important to have antivirus software to protect against malicious files.

Install ClamAV:

```
sudo apt install clamav  # Debian/Ubuntu
sudo yum install clamav  # CentOS/Red Hat
```

15. Use Two-Factor Authentication (2FA)

• Add an extra layer of security by enabling 2FA for SSH or other services.

You can use Google Authenticator or Authy for 2FA.

Install pam_google_authenticator:

```
sudo apt install libpam-google-authenticator  # For Debian/Ubuntu
sudo yum install google-authenticator  # For CentOS/Red Hat
```

16. Audit and Regularly Check Security

• Regularly perform security audits using tools like Lynis or Tiger:

```
sudo apt install lynis  # For Debian/Ubuntu
sudo yum install lynis  # For CentOS/Red Hat
sudo lynis audit system
```

17. Disable IPv6 if Not Needed

• If you don’t use IPv6, disable it to reduce the attack surface.

Edit /etc/sysctl.conf:

```
net.ipv6.conf.all.disable_ipv6 = 1
```

18. Check for Vulnerabilities

• Regularly check for known vulnerabilities using tools like **Nessus** or **OpenVAS**.

By following these steps and continuously monitoring and updating your system, you can significantly improve the security of your Linux server.

Revision #2
Created 20 December 2024 03:43:48 by Admin Diskominfo
Updated 20 December 2024 04:01:45 by Admin Diskominfo