LINUX SERVER SECURITY HARDENING

Essential measures to protect your Linux servers from common cyber threats

Set Up Firewall

A firewall controls incoming and outgoing network traffic based on predefined security rules.

Remove Unnecessary Services

Every running service can be a potential attack vector. Disabling unused services reduces the attack surface.

Disable root Login

the root account will mostly never need to log in directly. Disabling it make it harder for attackers to gain control.

Set up File Permissions

Setting proper file permissions ensures that only authorized users can read, write, or execute important files.

Ensure Time Synchronization

Accurate timekeeping is crucial for log accuracy, auditing, and preventing replay attacks.

Linux File Permissions

Permission Types

- Read (r)
- Write (w)
- Execute (x)

User Categories

- Owner
- Group
- Others

Representation

Permissions are typically displayed as a string of ten characters.

1	2-4	5-7	8-10
File Type	Owner Permission	Group Permission	Others Permission

Example

-rwxr-xr-x

File	rwx	r-x	r-x

All can read and execute, but only owner can write

Firewall Configuration with UFW (Uncomplicated Firewall)

```
# Default policies
sudo ufw default deny incoming
sudo ufw default allow outgoing

# Allow specific services
sudo ufw allow 22
sudo ufw allow 80
sudo ufw allow 443

# Enable firewall
sudo ufw enable
```

Best Practice

- Deny Incoming Traffic by Default
- Allow Only Necessary Ports
- Use Specific IP Address Rules When Possible
- Enable Logging for Monitoring
- Backup UFW Configuration