Linux Security

Linux systems, while less prone to traditional Windows-based malware, still require robust security practices. Below are key areas to ensure system security.

🔒 Basic Security Practices

- **Keep System Updated**: Always ensure the OS and installed packages are up-to-date.

  ```
  apt update && apt dist-upgrade
  ```

- **Use Firewalls**: Utilize `iptables` or the Linux firewall to restrict traffic.
- **Secure SSH**:
  - Disable password login.
  - Disallow root login via SSH.
  - Use SSH keys for authentication.
- **Principle of Least Privilege**: Grant only necessary access using the `sudoers` file.
- **Use `fail2ban`**: Prevent brute-force attacks by banning IPs after a set number of failed login attempts.

🔍 System Auditing

Regular audits help detect misconfigurations or vulnerabilities:

- Outdated kernel versions
- Misconfigured cron jobs
- World-writable files
- Permission issues

🧱 SELinux & AppArmor

- **Security-Enhanced Linux (SELinux)**:
  - Labels every process and file
  - Enforces access control policies via the kernel
- **AppArmor**: An alternative to SELinux for access control

🛡️ Additional Security Tools

- `Snort`: Network intrusion detection
- `chkrootkit`, `rkhunter`: Rootkit detection
- `Lynis`: Security auditing tool

⚙️ Recommended Security Settings

- Remove unused services and software
- Eliminate services with unencrypted auth
- Enable NTP and Syslog
- Enforce user-level account segregation
- Require strong passwords and use password aging
- Lock accounts after repeated login failures
- Disable unused SUID/SGID binaries

> Security is a continuous process, not a one-time setup.

TCP Wrappers

TCP Wrappers provide host-based access control by allowing or denying services to specific hosts.

🔐 Configuration Files

- `/etc/hosts.allow`: Defines which hosts/services are allowed.
- `/etc/hosts.deny`: Defines which hosts/services are denied.

Example: `/etc/hosts.allow`

```
# Allow access to SSH from local network
sshd : 10.129.14.0/24

# Allow FTP from specific host
ftpd : 10.129.14.10

# Allow Telnet from local domain
telnetd : .inlanefreight.local
```

Example: `/etc/hosts.deny`

```
# Deny all services from inlanefreight.com domain
ALL : .inlanefreight.com

# Deny SSH from a specific host
sshd : 10.129.22.22

# Deny FTP from a range
ftpd : 10.129.22.0/24
```

> ⚠️ First matching rule applies. TCP Wrappers complement but do not replace firewalls.

Stay secure, stay updated.