|  |  |  |  |
| --- | --- | --- | --- |
| S07 T05 | | | Application Security |
| Application isolation techniques | | |
| User and group security | | Caret Right with solid fill | یکی از مفاهیم کلیدی در امنیت نرم‌افزارها و سرورهای لینوکسی، تکنیک‌های جداسازی برنامه‌ها است. این تکنیک‌ها به مدیران سیستم کمک می‌کنند تا برنامه‌ها را از یکدیگر ایزوله کرده و به این ترتیب سطح حملات و آسیب‌پذیری‌های احتمالی را کاهش دهند. در این مقاله، به معرفی مفهوم جداسازی برنامه‌ها، اهمیت آن و روش‌های مختلف پیاده‌سازی این تکنیک‌ها در لینوکس می‌پردازیم. |
| بعد از |
| --- | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **بله** | | پیاده سازی عملی: **خیر** |

## تکنیک‌های جداسازی برنامه‌ها در لینوکس

یکی از مفاهیم کلیدی در امنیت نرم‌افزارها و سرورهای لینوکسی، تکنیک‌های جداسازی برنامه‌ها است. این تکنیک‌ها به مدیران سیستم کمک می‌کنند تا برنامه‌ها را از یکدیگر ایزوله کرده و به این ترتیب سطح حملات و آسیب‌پذیری‌های احتمالی را کاهش دهند. در این مقاله، به معرفی مفهوم جداسازی برنامه‌ها، اهمیت آن و روش‌های مختلف پیاده‌سازی این تکنیک‌ها در لینوکس می‌پردازیم.

## اهمیت جداسازی برنامه‌ها

جداسازی برنامه‌ها به دلایل زیر اهمیت دارد:

1. **کاهش سطح حملات**: با جداسازی برنامه‌ها، حتی اگر یکی از برنامه‌ها دچار نقص امنیتی شود، مهاجمان نمی‌توانند به سایر بخش‌های سیستم دسترسی پیدا کنند.
2. **بهبود امنیت داده‌ها**: با ایزوله کردن برنامه‌ها، داده‌های حساس و مهم می‌توانند به طور جداگانه محافظت شوند.
3. **افزایش پایداری سیستم**: در صورت بروز خطا یا نقص در یکی از برنامه‌ها، تاثیر آن بر روی سایر بخش‌های سیستم کاهش می‌یابد.
4. **مدیریت و نگهداری آسان‌تر**: جداسازی برنامه‌ها به مدیران سیستم کمک می‌کند تا به راحتی برنامه‌ها را مدیریت و به‌روزرسانی کنند.

## تکنیک‌های جداسازی برنامه‌ها

1. **استفاده از کانتینرها (Containers)**: کانتینرها ابزارهای قدرتمندی برای جداسازی برنامه‌ها و محیط‌های اجرایی آن‌ها هستند. Docker یکی از محبوب‌ترین ابزارهای کانتینر در لینوکس است که به شما امکان می‌دهد برنامه‌ها را در کانتینرهای مجزا اجرا کنید.

sudo apt-get install docker.io

sudo systemctl start docker

sudo systemctl enable docker

docker run -d --name myapp-container myapp-image

1. **ماشین‌های مجازی (Virtual Machines)**: ماشین‌های مجازی به شما اجازه می‌دهند تا سیستم‌عامل‌های مجزا را بر روی یک سخت‌افزار واحد اجرا کنید. ابزارهایی مانند KVM و VirtualBox برای این منظور استفاده می‌شوند.

sudo apt-get install qemu-kvm libvirt-bin

sudo virsh create myvm.xml

1. **chroot**:

chroot به شما اجازه می‌دهد تا یک محیط فایل سیستم جداگانه برای یک برنامه ایجاد کنید. این ابزار به ویژه برای جداسازی برنامه‌های خاص مفید است.

sudo mkdir -p /var/chroot/myapp

sudo chroot /var/chroot/myapp /bin/bash

1. **LXC/LXD**:

LXC (Linux Containers) و LXD ابزارهایی برای ایجاد و مدیریت کانتینرهای سبک هستند که از هسته لینوکس برای جداسازی استفاده می‌کنند.

sudo apt-get install lxc lxd

sudo lxd init

lxc launch ubuntu:18.04 myapp-container

1. **استفاده از Namespaces و Cgroups**:

لینوکس از Namespaces و Cgroups برای جداسازی و محدود کردن منابع برنامه‌ها استفاده می‌کند. این ابزارها به شما امکان می‌دهند تا منابع سیستم مانند CPU، حافظه و I/O را برای برنامه‌های مختلف محدود کنید.

sudo cgcreate -g cpu,memory:myapp

sudo cgset -r memory.limit\_in\_bytes=512M myapp

sudo cgexec -g cpu,memory:myapp /path/to/myapp

## ابزارها و برنامه‌های مفید

1. **Docker**: ابزاری برای ایجاد و مدیریت کانتینرهای مجزا.

sudo apt-get install docker.io

1. **KVM (Kernel-based Virtual Machine)**:

ابزاری برای ایجاد و مدیریت ماشین‌های مجازی.

sudo apt-get install qemu-kvm libvirt-bin

1. **chroot**:

ابزاری برای ایجاد محیط‌های فایل سیستم مجزا.

sudo chroot /path/to/new/root /bin/bash

1. **LXC/LXD**:

ابزارهایی برای ایجاد و مدیریت کانتینرهای سبک.

sudo apt-get install lxc lxd

1. **Namespaces و Cgroups**:
2. ابزارهای داخلی لینوکس برای جداسازی و محدود کردن منابع برنامه‌ها.

sudo apt-get install cgroup-tools

## نتیجه‌گیری

استفاده از تکنیک‌های جداسازی برنامه‌ها یکی از موثرترین روش‌ها برای افزایش امنیت و پایداری سرورهای لینوکسی است. با جداسازی برنامه‌ها و محیط‌های اجرایی آن‌ها، می‌توان از نفوذهای غیرمجاز جلوگیری کرد و امنیت کلی سیستم را بهبود بخشید. آشنایی و پیاده‌سازی صحیح این تکنیک‌ها به مدیران سیستم کمک می‌کند تا از داده‌های حساس خود محافظت کرده و از عملکرد بهینه سرورهای خود اطمینان حاصل کنند.

Bottom of Form

## منابع و ارجاعات

* <https://roadmap.sh/linux>
* <https://roadmap.sh/r/general-linux-server-hardening>