|  |  |  |  |
| --- | --- | --- | --- |
| S03 T03 | | | Linux Kernel Hardening |
| SELinux or AppArmor | | |
| Kernel parameter tuning | | Caret Right with solid fill | امن‌سازی یک سرور لینوکسی شامل چندین لایه دفاعی است که یکی از حیاتی‌ترین آنها سخت‌افزار هسته است. این مقاله بر دو ماژول امنیتی اصلی هسته لینوکس تمرکز خواهد کرد: SELinux و AppArmor |
| بعد از |
| Linux kernel security updates | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: خیر | پژوهشی: **بله** | | پیاده سازی عملی: |

## SELinux چیست؟

لینوکس امنیتی افزایش‌یافته (SELinux) یک مکانیزم کنترل دسترسی قوی است که در هسته پیاده‌سازی شده است. این مکانیزم کنترل دسترسی اجباری (MAC) را اعمال می‌کند که کاربران و فرایندها را به حداقل سطح مجوزهایی که برای عملکرد نیاز دارند محدود می‌کند.

**ویژگی‌های کلیدی:**

* کنترل دقیق بر همه فرایندها و فایل‌ها.
* سیاست‌ها تعریف می‌کنند که چگونه فرایندها و کاربران با یکدیگر و سیستم تعامل دارند.
* مدل رد به طور پیش‌فرض.

**مزایا:**

* امنیت افزایش‌یافته با محدود کردن خسارتی که می‌تواند توسط برنامه‌های مخرب وارد شود.
* قابلیت‌های ثبت و نظارت دقیق.

## AppArmorچیست؟

AppArmor (آرمور برنامه) یک ماژول امنیتی دیگر لینوکس است که نیز MAC ارائه می‌دهد، اما به‌طور کلی کاربرپسندتر و آسان‌تر برای پیکربندی نسبت به SELinux در نظر گرفته می‌شود.

**ویژگی‌های کلیدی:**

* پروفایل‌ها تعریف می‌کنند که برنامه‌های فردی به چه منابعی دسترسی دارند.
* آسان‌تر برای پیکربندی و مدیریت نسبت به SELinux.
* از یک روش مبتنی بر مسیر برای تعریف سیاست‌ها استفاده می‌کند.

**مزایا:**

* ایجاد و مدیریت سیاست‌ها ساده‌تر.
* تعادلی بین امنیت و قابلیت استفاده فراهم می‌کند.
* مناسب برای محیط‌هایی که سهولت استفاده و استقرار سریع اولویت دارند.

| **SELinux** | **AppArmor** | **ویژگی** |
| --- | --- | --- |
| پیچیده، نیازمند سیاست‌های دقیق | آسان‌تر، مبتنی بر پروفایل | پیکربندی |
| بسیار انعطاف‌پذیر، پشتیبانی از کنترل دقیق | کمتر انعطاف‌پذیر ولی مدیریت ساده‌تر | انعطاف پذیری |
| مبتنی بر برچسب (هر فایل/فرایند برچسب دارد) | مبتنی بر مسیر (سیاست‌ها مبتنی بر مسیر فایل) | مدل سیاست |
| ایده‌آل برای محیط‌های با امنیت بالا | مناسب برای استفاده‌های عمومی | موارد استفاده |
| قابلیت‌های ثبت گسترده | ثبت کافی | ثبت و نظارت |

## مراحل عملی برای پیاده سازی SELinux

### گام 1: بررسی وضعیت SELinux

sestatus

### گام 2: فعال‌سازی SELinux

فایل پیکربندی SELinux را در مسیر /etc/selinux/config ویرایش کنید:

sudo nano /etc/selinux/config

خط SELINUX را به این شکل تغییر دهید:

SELINUX=enforcing

فایل را ذخیره و خارج شوید، سپس سیستم را مجدداً راه‌اندازی کنید:

sudo reboot

### گام 3: پیکربندی سیاست‌های SELinux

برای مدیریت سیاست‌های SELinux می‌توانید از دستورات semanage و setsebool استفاده کنید. به عنوان مثال، برای اجازه به اسکریپت‌ها و ماژول‌های HTTPD برای اتصال به شبکه:

sudo setsebool -P httpd\_can\_network\_connect on

### گام 4: عیب‌یابی

اگر دسترسی یک فرایند رد شود، لاگ‌های بررسی در /var/log/audit/audit.log می‌توانند جزئیات را ارائه دهند. از ابزارهای ausearch و audit2allow برای تحلیل و ایجاد سیاست‌های سفارشی استفاده کنید.

sudo ausearch -m avc -ts recent

sudo audit2allow -w -a

## مراحل عملی برای پیاده سازی AppArmor

### نگاهی دوباره به AppArmor

AppArmor یک جایگزین مبتنی بر دبیان برای SELinux است که معمولاً در سیستم‌های Red Hat، CentOS، و Fedora استفاده می‌شود. این امکان را فراهم می‌کند که برای اسکریپت‌ها یا برنامه‌های سفارشی پروفایل‌هایی ایجاد کنید و تعریف کنید که چه اقداماتی می‌توانند انجام دهند و به کدام بخش‌های سیستم دسترسی داشته باشند. این ویژگی به‌خصوص زمانی مفید است که با اسکریپت‌هایی سروکار دارید که نیاز به دسترسی خاص یا دسترسی به اجزای مشخصی از سیستم دارند.

### بررسی وضعیت AppArmor

برای شروع، ضروری است که بدانید چگونه وضعیت AppArmor را در سیستم خود بررسی کنید. دستور

aa-status

اطلاعات دقیقی از وضعیت فعلی AppArmor ارائه می‌دهد. اگر هیچ خروجی دریافت نمی‌کنید یا ماژول بارگذاری نشده است، می‌توانید سرویس را با استفاده از دستور

systemctl start apparmor

شروع کنید. برای بررسی اینکه آیا سرویس در حال اجرا است، از دستور

systemctl status apparmor

استفاده کنید.

### درک حالت‌های AppArmor

AppArmor در سه حالت عمل می‌کند:

* Enforcing (اجرایی): برنامه را مجبور می‌کند تا به پروفایل تعریف شده خود پایبند باشد و هرگونه اقدامی که خارج از پارامترهای مجاز است را رد می‌کند.
* Complain (اعتراض): به برنامه اجازه می‌دهد تا اقدامات خارج از پروفایل خود را انجام دهد، اما این وقایع را ثبت و درباره آنها اعتراض می‌کند.
* Unconfined (آزاد): به برنامه دسترسی بدون محدودیت به سیستم می‌دهد، بدون ثبت یا اعتراض به اقدامات آن.

### ایجاد پروفایل برای یک اسکریپت سفارشی

برای ایجاد پروفایل برای یک اسکریپت سفارشی، از دستور

aa-genprof <script\_name>

استفاده کنید. این دستور پروفایلی بر اساس رفتار اسکریپت ایجاد می‌کند. از شما خواسته می‌شود که لاگ سیستم را برای رویدادهای AppArmor اسکن کنید و سپس ایجاد پروفایل را تکمیل کنید. پس از اتمام، می‌توانید پروفایل را با استفاده از دستور aa-status بررسی کنید.

### نگهداری پروفایل‌های AppArmor

سومین دستور ضروری برای نگهداری AppArmor،

aa-logprof

است. این دستور ورودی‌های لاگ را می‌خواند و پروفایل‌های موجود در سیستم شما را به‌روزرسانی می‌کند. این دستور به‌خصوص پس از ایجاد یک پروفایل مفید است، زیرا اطمینان حاصل می‌کند که AppArmor همچنان به درستی عمل می‌کند، حتی زمانی که برنامه به‌روزرسانی شده و نیاز به دسترسی‌های بیشتری دارد.

**نتیجه‌گیری**

هر دو SELinux و AppArmor مکانیزم‌های امنیتی قوی برای سخت‌افزار هسته شما ارائه می‌دهند. SELinux ایده‌آل برای محیط‌هایی است که نیاز به سیاست‌های امنیتی سختگیرانه دارند، در حالی که AppArmor یک رویکرد ساده‌تر ارائه می‌دهد که آن را برای استفاده‌های عمومی مناسب می‌سازد. پیاده‌سازی هر کدام از اینها به طور قابل توجهی وضعیت امنیتی سرورهای لینوکسی شما را بهبود خواهد بخشید.

## منابع و ارجاعات

* <https://www.youtube.com/watch?v=KYM-Dzivnjs>
* <https://chatwith.tools/youtube-summarizer/configuring-app-armor-on-ubuntu-1804-step-by-step-guide>
* <https://www.youtube.com/watch?v=KkTDdHDAaYI>
* <https://pureooze.com/blog/posts/2016-07-28-the-comprehensive-guide-to-apparmor-p1/>
* <https://www.youtube.com/watch?v=PQo9PEdVuIw>
* <https://null-byte.wonderhowto.com/how-to/locking-down-linux-using-ubuntu-as-your-primary-os-part-3-application-hardening-sandboxing-0185710/>
* <https://www.youtube.com/watch?v=QxNsyrftJ8I>
* <https://christitus.com/linux-security-mistakes/>
* <https://medium.com/information-and-technology/so-what-is-apparmor-64d7ae211ed>