|  |  |  |  |
| --- | --- | --- | --- |
| S04 T03 | | | File System Hardening |
| Sticky bit, SUID, SGID | | |
| Mount options for system file systems | | Caret Right with solid fill | در فرآیند سخت‌کردن سرورهای لینوکس، یکی از مهم‌ترین موضوعات مربوط به امنیت، مدیریت صحیح مجوزها و سطح دسترسی‌ها به فایل‌ها و پوشه‌ها است. در این زمینه، Sticky Bit، SUID و SGID نقش مهمی ایفا می‌کنند. این ویژگی‌ها به مدیر سیستم اجازه می‌دهند تا کنترل بیشتری بر روی نحوه دسترسی کاربران به منابع مختلف داشته باشند و از سوء استفاده‌های احتمالی جلوگیری کنند. |
| بعد از |
| ACL (access control lists) | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **بله** | | پیاده سازی عملی: **خیر** |

### آشنایی باSticky Bit ، SUIDو SGID در لینوکس

در فرآیند سخت‌کردن سرورهای لینوکس، یکی از مهم‌ترین موضوعات مربوط به امنیت، مدیریت صحیح مجوزها و سطح دسترسی‌ها به فایل‌ها و پوشه‌ها است. در این زمینه، Sticky Bit، SUID و SGID نقش مهمی ایفا می‌کنند. این ویژگی‌ها به مدیر سیستم اجازه می‌دهند تا کنترل بیشتری بر روی نحوه دسترسی کاربران به منابع مختلف داشته باشند و از سوء استفاده‌های احتمالی جلوگیری کنند.

## Sticky Bit چیست؟

Sticky Bit یکی از ویژگی‌های سطح دسترسی در سیستم‌ فایل‌های یونیکس و لینوکس است که معمولاً برای پوشه‌ها به کار می‌رود. هنگامی که Sticky Bit بر روی یک پوشه تنظیم می‌شود، تنها مالک فایل‌ها یا پوشه‌ها و کاربر root می‌توانند آن‌ها را حذف یا تغییر نام دهند، حتی اگر سایر کاربران مجوزهای نوشتن (write) بر روی آن پوشه داشته باشند.

**کاربرد Sticky Bit**

* جلوگیری از حذف اشتباهی فایل‌ها توسط کاربران دیگر
* افزایش امنیت پوشه‌های مشترک مانند /tmp

برای تنظیم Sticky Bit می‌توان از فرمان chmod استفاده کرد:

chmod +t /path/to/directory

## SUID چیست؟

SUID یا Set User ID یک بیت مجوز خاص است که به فایل‌های اجرایی اعمال می‌شود. زمانی که SUID بر روی یک فایل تنظیم می‌شود، هر کاربری که آن فایل را اجرا کند، به صورت موقت با سطح دسترسی مالک فایل اجرا می‌شود. این ویژگی برای برنامه‌هایی که نیاز به دسترسی‌های ویژه دارند، اما نباید همیشه با این دسترسی‌ها اجرا شوند، بسیار مفید است.

**مثال:**

برنامه passwd که برای تغییر رمز عبور کاربران استفاده می‌شود، با بیت SUID تنظیم شده است. این برنامه به کاربر اجازه می‌دهد تا رمز عبور خود را تغییر دهد، حتی اگر به فایل‌های مورد نیاز برای این کار دسترسی نداشته باشد.

برای تنظیم SUID می‌توان از فرمان chmod استفاده کرد:

chmod u+s /path/to/file

## SGID چیست؟

SGID یا Set Group ID مشابه SUID است، با این تفاوت که به جای تنظیم سطح دسترسی کاربر، سطح دسترسی گروه تنظیم می‌شود. وقتی SGID بر روی یک فایل اجرایی تنظیم می‌شود، کاربری که آن فایل را اجرا می‌کند، به صورت موقت با سطح دسترسی گروه مالک فایل اجرا می‌شود.

**کاربرد SGID در پوشه‌ها:**

* در پوشه‌هایی که SGID تنظیم شده است، هر فایلی که در آن پوشه ایجاد شود، به طور خودکار به گروه مالک پوشه تعلق خواهد داشت.

برای تنظیم SGID می‌توان از فرمان chmod استفاده کرد:

chmod g+s /path/to/file\_or\_directory

## ابزارها و برنامه‌های مفید

برای مدیریت و بررسی Sticky Bit، SUID و SGID، می‌توان از ابزارها و برنامه‌های زیر استفاده کرد:

* **ls**: با استفاده از گزینه -l در فرمان ls می‌توان مجوزهای فایل‌ها و پوشه‌ها را مشاهده کرد و متوجه تنظیمات SUID، SGID و Sticky Bit شد.

ls -l /path/to/directory

* **find**: این فرمان به مدیر سیستم کمک می‌کند تا فایل‌ها و پوشه‌هایی که دارای SUID، SGID یا Sticky Bit هستند را شناسایی کند.

find / -perm /6000 2>/dev/null

* **chmod:** ابزار اصلی برای تنظیم و تغییر مجوزهای فایل‌ها و پوشه‌ها است.

**نتیجه‌گیری**

مدیریت صحیح مجوزها با استفاده از ویژگی‌های Sticky Bit، SUID و SGID یکی از جنبه‌های مهم در امنیت سرورهای لینوکس است. با درک صحیح و استفاده مناسب از این ویژگی‌ها، می‌توان دسترسی‌ها را بهینه‌سازی و امنیت سیستم را افزایش داد. هر مدیر سیستمی باید با این مفاهیم آشنا باشد و بتواند آن‌ها را به درستی پیاده‌سازی کند تا از سیستم‌های خود به بهترین نحو ممکن محافظت نماید.

## منابع و ارجاعات

* <https://roadmap.sh/linux>
* <https://tosinso.com/bGn>