



File System Hardening	S04 T03	
	Sticky bit, SUID, SGID	
<p>در فرآیند سخت کردن سرورهای لینوکس، یکی از مهم ترین موضوعات مربوط به امنیت، مدیریت صحیح مجوزها و سطح دسترسی ها به فایل ها و پوشه ها است. در این زمینه، Sticky Bit، SUID و SGID نقش مهمی ایفا می کنند. این ویژگی ها به مدیر سیستم اجازه می دهند تا کنترل بیشتری بر روی نحوه دسترسی کاربران به منابع مختلف داشته باشند و از سوء استفاده های احتمالی جلوگیری کنند.</p>		Mount options for system file systems
	بعد از	
		ACL (access control lists)
	قبل از	
پیاده سازی عملی: خیر	پژوهشی: بله	راهنمای عملی: بله

آشنایی با Sticky Bit، SUID و SGID در لینوکس

در فرآیند سخت کردن سرورهای لینوکس، یکی از مهم ترین موضوعات مربوط به امنیت، مدیریت صحیح مجوزها و سطح دسترسی ها به فایل ها و پوشه ها است. در این زمینه، Sticky Bit، SUID و SGID نقش مهمی ایفا می کنند. این ویژگی ها به مدیر سیستم اجازه می دهند تا کنترل بیشتری بر روی نحوه دسترسی کاربران به منابع مختلف داشته باشند و از سوء استفاده های احتمالی جلوگیری کنند.

Sticky Bit چیست؟

Sticky Bit یکی از ویژگی های سطح دسترسی در سیستم فایل های یونیکس و لینوکس است که معمولاً برای پوشه ها به کار می رود. هنگامی که Sticky Bit بر روی یک پوشه تنظیم می شود، تنها مالک فایل ها یا پوشه ها و کاربر root می توانند آن ها 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 فایل ها توسط کاربران دیگر
 - افزایش امنیت پوشه های مشترک مانند /tmp
- برای تنظیم Sticky Bit می توان از فرمان `chmod` استفاده کرد:

```
chmod +t /path/to/directory
```

SUID چیست؟

SUID یا Set User ID یک بیت مجوز خاص است که به فایل های اجرایی اعمال می شود. زمانی که SUID بر روی یک فایل تنظیم می شود، هر کاربری که آن فایل را اجرا کند، به صورت موقت با سطح دسترسی مالک فایل اجرا می شود. این ویژگی برای برنامه هایی که نیاز به دسترسی های ویژه دارند، اما نباید همیشه با این دسترسی ها 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>