|  |  |  |  |
| --- | --- | --- | --- |
| S08 T06 | | | User Account Security |
| Management of root access and sudo privileges | | |
| User-based access control lists | | Caret Right with solid fill | یکی از اصول حیاتی در امنیت حساب‌های کاربری و سیستم‌های لینوکسی، مدیریت دسترسی کاربر ریشه (root) و امتیازات sudo است. این موضوع به مدیران سیستم کمک می‌کند تا دسترسی‌های مدیریتی را به‌طور دقیق کنترل کرده و از سوءاستفاده‌های احتمالی جلوگیری کنند. در این مقاله به اهمیت مدیریت دسترسی ریشه و امتیازات sudo و روش‌های پیاده‌سازی آن می‌پردازیم. |
| بعد از |
| --- | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **خیر** | | پیاده سازی عملی: **بله** |

## مدیریت دسترسی ریشه و امتیازات sudo در لینوکس

یکی از اصول حیاتی در امنیت حساب‌های کاربری و سیستم‌های لینوکسی، مدیریت دسترسی کاربر ریشه (root) و امتیازات sudo است. این موضوع به مدیران سیستم کمک می‌کند تا دسترسی‌های مدیریتی را به‌طور دقیق کنترل کرده و از سوءاستفاده‌های احتمالی جلوگیری کنند. در این مقاله به اهمیت مدیریت دسترسی ریشه و امتیازات sudo و روش‌های پیاده‌سازی آن می‌پردازیم.

## اهمیت مدیریت دسترسی ریشه و sudo

1. **حفاظت از امنیت سیستم**: دسترسی ریشه به تمامی جنبه‌های سیستم امکان مدیریت دارد و در صورت سوءاستفاده، می‌تواند به نفوذ و تخریب گسترده منجر شود. محدود کردن این دسترسی به کاربران معتمد، امنیت سیستم را افزایش می‌دهد.
2. **جلوگیری از اشتباهات تصادفی**: کاربر ریشه دارای دسترسی کامل به سیستم است و اشتباهات ناخواسته می‌تواند تأثیرات گسترده‌ای داشته باشد. با استفاده از sudo، می‌توان وظایف مدیریتی را به‌طور موقت به کاربران مجاز اختصاص داد.
3. **کنترل و پیگیری فعالیت‌ها**: با استفاده از sudo، می‌توان فعالیت‌های کاربران را ثبت و پیگیری کرد، که این امر به شناسایی رفتارهای مشکوک کمک می‌کند.

## روش‌های مدیریت دسترسی ریشه و sudo

1. **غیرفعال کردن ورود مستقیم به ریشه**: ورود مستقیم به حساب ریشه می‌تواند خطرناک باشد. بهتر است این دسترسی را غیرفعال کنید و به جای آن از حساب‌های کاربری عادی با امتیازات sudo استفاده کنید.

sudo passwd -l root

1. **استفاده از sudo برای دسترسی‌های مدیریتی**: با استفاده از sudo، کاربران می‌توانند دستورات مدیریتی خاصی را اجرا کنند. برای تنظیم این دسترسی‌ها، فایل sudoers را ویرایش کنید:

sudo visudo

و دستورات مورد نظر را اضافه کنید:

username ALL=(ALL) ALL

1. **محدود کردن دسترسی sudo به دستورات خاص**: می‌توان دسترسی کاربران به دستورات خاص را محدود کرد:

username ALL=(ALL) /usr/bin/command1, /usr/bin/command2

1. **فعال‌سازی ورود دو مرحله‌ای (2FA) برای sudo**: با استفاده از احراز هویت دو مرحله‌ای، می‌توان امنیت استفاده از sudo را افزایش داد.

sudo apt-get install libpam-google-authenticator

1. **پیگیری و مانیتورینگ استفاده از sudo**: لاگ‌های استفاده از sudo را به‌طور منظم بررسی کنید تا فعالیت‌های مشکوک را شناسایی کنید.

sudo cat /var/log/auth.log | grep sudo

## نتیجه‌گیری

مدیریت صحیح دسترسی ریشه و امتیازات sudo یکی از اصول اساسی در افزایش امنیت سیستم‌های لینوکسی است. با محدود کردن دسترسی‌ها و استفاده از روش‌های مناسب، می‌توان از سوءاستفاده‌های احتمالی جلوگیری کرده و امنیت سیستم را به طور قابل توجهی افزایش داد. آشنایی و پیاده‌سازی صحیح این روش‌ها 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>
* <https://www.youtube.com/watch?v=O1N8q9zSwsE>