|  |  |  |  |
| --- | --- | --- | --- |
| S07 T04 | | | Application Security |
| User and group security | | |
| Deploying application firewalls | | Caret Right with solid fill | یکی از جنبه‌های حیاتی امنیت نرم‌افزارها در سرورهای لینوکسی، مدیریت صحیح امنیت کاربران و گروه‌ها است. این جنبه از امنیت به مدیران سیستم اجازه می‌دهد تا دسترسی به منابع سیستم را کنترل کرده و از سوء استفاده‌های احتمالی جلوگیری کنند. در این مقاله به بررسی مفهوم امنیت کاربران و گروه‌ها، اهمیت آن و روش‌های پیاده‌سازی آن در لینوکس می‌پردازیم. |
| بعد از |
| Application isolation techniques | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **خیر** | | پیاده سازی عملی: **خیر** |

## امنیت کاربران و گروه‌ها در لینوکس

یکی از جنبه‌های حیاتی امنیت نرم‌افزارها در سرورهای لینوکسی، مدیریت صحیح امنیت کاربران و گروه‌ها است. این جنبه از امنیت به مدیران سیستم اجازه می‌دهد تا دسترسی به منابع سیستم را کنترل کرده و از سوء استفاده‌های احتمالی جلوگیری کنند. در این مقاله به بررسی مفهوم امنیت کاربران و گروه‌ها، اهمیت آن و روش‌های پیاده‌سازی آن در لینوکس می‌پردازیم.

## اهمیت امنیت کاربران و گروه‌ها

امنیت کاربران و گروه‌ها از چند جهت اهمیت دارد:

1. **کنترل دسترسی**: مدیریت صحیح کاربران و گروه‌ها به مدیران سیستم این امکان را می‌دهد که دسترسی به فایل‌ها، دایرکتوری‌ها و سرویس‌های مختلف را به طور دقیق کنترل کنند.
2. **جلوگیری از سوء استفاده**: با تنظیم مجوزهای مناسب، می‌توان از سوء استفاده کاربران و برنامه‌ها از منابع سیستم جلوگیری کرد.
3. **افزایش امنیت کلی سیستم**: با محدود کردن دسترسی‌های غیرضروری، سطح حملات احتمالی کاهش یافته و امنیت کلی سیستم افزایش می‌یابد.

## اصول امنیت کاربران و گروه‌ها

1. **ایجاد کاربران و گروه‌های خاص برای هر سرویس**: هر سرویس یا برنامه باید با یک کاربر و گروه خاص اجرا شود. این کار به ایزوله کردن سرویس‌ها و محدود کردن دسترسی آن‌ها به منابع سیستم کمک می‌کند.

sudo useradd -r -s /sbin/nologin service\_user

sudo groupadd service\_group

sudo usermod -a -G service\_group service\_user

1. **استفاده از مجوزهای مناسب فایل‌ها و دایرکتوری‌ها**: با تنظیم مجوزهای مناسب بر روی فایل‌ها و دایرکتوری‌ها، می‌توان دسترسی‌های غیرمجاز را محدود کرد.

sudo chown service\_user:service\_group /path/to/directory

sudo chmod 750 /path/to/directory

1. **استفاده از sudo برای دسترسی‌های مدیریتی**: به جای استفاده از کاربر root برای انجام وظایف مدیریتی، از sudo استفاده کنید. این کار به محدود کردن دسترسی‌های غیرضروری کمک می‌کند و همچنین فعالیت‌های کاربران را قابل ردیابی می‌سازد.

sudo usermod -aG sudo username

1. **تنظیم سیاست‌های کلمه‌عبور قوی**: برای کاربران سیستم، سیاست‌های کلمه‌عبور قوی و پیچیده تنظیم کنید تا از دسترسی‌های غیرمجاز جلوگیری شود.

sudo apt-get install libpam-pwquality

sudo vi /etc/pam.d/common-password

سپس خط زیر را اضافه کنید:

password requisite pam\_pwquality.so retry=3 minlen=12 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1

1. **محدود کردن دسترسی به سرویس‌های خاص**: با استفاده از فایل‌های پیکربندی مانند /etc/hosts.allow و /etc/hosts.deny می‌توان دسترسی به سرویس‌های خاص را بر اساس آدرس IP محدود کرد.

sshd: 192.168.1.100

ALL: ALL

1. **مانیتورینگ فعالیت‌های کاربران**: فعالیت‌های کاربران را مانیتور کنید تا هرگونه رفتار مشکوک یا غیرمجاز را شناسایی و به موقع واکنش نشان دهید. ابزارهایی مانند auditd می‌توانند به این کار کمک کنند.

sudo apt-get install auditd

sudo systemctl enable auditd

sudo systemctl start auditd

**ابزارها و برنامه‌های مفید**

1. **sudo**: ابزاری برای اجرای دستورات با دسترسی‌های مدیریتی به صورت موقت.

sudo command

1. **libpam-pwquality**: ماژولی برای تنظیم سیاست‌های کلمه‌عبور قوی و پیچیده.

sudo apt-get install libpam-pwquality

1. **auditd**: یک سرویس برای مانیتورینگ و لاگ‌گیری فعالیت‌های کاربران.

sudo apt-get install auditd

sudo systemctl enable auditd

sudo systemctl start auditd

1. **usermod**: ابزاری برای مدیریت کاربران و گروه‌ها.

sudo usermod -aG groupname username

## نتیجه‌گیری

مدیریت صحیح امنیت کاربران و گروه‌ها یکی از اصول اساسی در افزایش امنیت سرورهای لینوکسی است. با استفاده از روش‌ها و ابزارهای مناسب، می‌توان دسترسی به منابع سیستم را کنترل کرد و از سوء استفاده‌های احتمالی جلوگیری کرد. آشنایی و پیاده‌سازی صحیح این اصول 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>