|  |  |  |  |
| --- | --- | --- | --- |
| S08 T02 | | | User Account Security |
| Default account settings | | |
| Password policy enforcement | | Caret Right with solid fill | یکی از اصول مهم در امنیت حساب‌های کاربری در سرورهای لینوکسی، تنظیمات پیش‌فرض حساب‌های کاربری است. این تنظیمات می‌توانند نقش مهمی در محافظت از سیستم در برابر دسترسی‌های غیرمجاز و سوءاستفاده‌ها ایفا کنند. در این مقاله به بررسی مفهوم تنظیمات پیش‌فرض حساب کاربری، اهمیت آن و نحوه پیاده‌سازی آن در لینوکس می‌پردازیم. |
| بعد از |
| User activity logging | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **خیر** | | پیاده سازی عملی: **خیر** |

## تنظیمات پیش‌فرض حساب کاربری در لینوکس

یکی از اصول مهم در امنیت حساب‌های کاربری در سرورهای لینوکسی، تنظیمات پیش‌فرض حساب‌های کاربری است. این تنظیمات می‌توانند نقش مهمی در محافظت از سیستم در برابر دسترسی‌های غیرمجاز و سوءاستفاده‌ها ایفا کنند. در این مقاله به بررسی مفهوم تنظیمات پیش‌فرض حساب کاربری، اهمیت آن و نحوه پیاده‌سازی آن در لینوکس می‌پردازیم.

## اهمیت تنظیمات پیش‌فرض حساب کاربری

تنظیمات پیش‌فرض حساب‌های کاربری از چند جنبه اهمیت دارند:

1. **حفاظت از امنیت سیستم**: با تنظیمات پیش‌فرض مناسب، می‌توان از دسترسی‌های غیرمجاز به سیستم جلوگیری کرد و امنیت کلی سیستم را افزایش داد.
2. **مدیریت آسان‌تر کاربران**: با تعریف تنظیمات پیش‌فرض، مدیران سیستم می‌توانند به راحتی کاربران جدید را ایجاد و مدیریت کنند.
3. **جلوگیری از سوءاستفاده‌های احتمالی**: با محدود کردن دسترسی‌ها و تنظیمات پیش‌فرض، می‌توان از سوءاستفاده‌های احتمالی کاربران جلوگیری کرد.

## تنظیمات پیش‌فرض حساب کاربری

1. **تنظیمات کلمه‌عبور**: یکی از مهم‌ترین تنظیمات پیش‌فرض حساب‌های کاربری، تنظیمات مربوط به کلمه‌عبور است. باید اطمینان حاصل شود که کاربران از کلمه‌عبورهای قوی و پیچیده استفاده می‌کنند.

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. **غیرفعال کردن ورود به حساب‌های غیرضروری**: حساب‌های کاربری پیش‌فرض که به آن‌ها نیازی نیست باید غیرفعال شوند تا از دسترسی‌های غیرمجاز جلوگیری شود.

sudo usermod -L username

1. **تنظیم شل پیش‌فرض**: حساب‌های کاربری که نباید به سیستم وارد شوند باید یک شل غیرتعاملی داشته باشند.

sudo usermod -s /sbin/nologin username

1. **مدیریت دسترسی sudo**: حساب‌های کاربری که نیاز به دسترسی مدیریتی دارند باید به گروه sudo اضافه شوند و سایر کاربران نباید این دسترسی را داشته باشند.

sudo usermod -aG sudo username

sudo deluser username sudo

1. **تنظیمات خانه کاربر**: تنظیمات پیش‌فرض دایرکتوری خانه کاربر باید به گونه‌ای باشد که تنها خود کاربر و مدیر سیستم به آن دسترسی داشته باشند.

sudo chmod 700 /home/username

1. **استفاده از فایل‌های اسکلت (Skeleton Files)**: فایل‌های اسکلت در دایرکتوری /etc/skel قرار دارند و به عنوان الگو برای دایرکتوری‌های خانه کاربران جدید استفاده می‌شوند. این فایل‌ها می‌توانند شامل تنظیمات پیش‌فرض مورد نظر باشند.

sudo cp /etc/skel/.bashrc /home/username/

sudo cp /etc/skel/.profile /home/username/

sudo chown username:username /home/username/.bashrc /home/username/.profile

## ابزارها و برنامه‌های مفید

1. **libpam-pwquality**:

ماژولی برای تنظیم سیاست‌های کلمه‌عبور قوی و پیچیده.

sudo apt-get install libpam-pwquality

1. **usermod**:

ابزاری برای مدیریت کاربران و تنظیمات پیش‌فرض آن‌ها.

sudo usermod -aG groupname username

1. **chmod**:

ابزاری برای تنظیم مجوزهای فایل و دایرکتوری.

sudo chmod 700 /home/username

1. **/etc/skel**:

دایرکتوری حاوی فایل‌های اسکلت برای تنظیمات پیش‌فرض دایرکتوری خانه کاربران جدید.

## نتیجه‌گیری

تنظیمات پیش‌فرض حساب کاربری یکی از اصول اساسی در امنیت حساب‌های کاربری در سرورهای لینوکسی است. با استفاده از روش‌ها و ابزارهای مناسب، می‌توان دسترسی به منابع سیستم را کنترل کرد و از سوءاستفاده‌های احتمالی جلوگیری کرد. آشنایی و پیاده‌سازی صحیح این تنظیمات 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>