<table>
<tr><td rowspan="2">User Account Security</td><td colspan="2">S08 T01</td></tr>
<tr><td colspan="2">Password policy enforcement</td></tr>
<tr><td rowspan="2">یکی از جنبه‌های حیاتی امنیت حساب‌های کاربری در سرورهای لینوکس، اجرای سیاست‌های کلمه‌عبور است. کلمه‌عبورهای قوی و امن، اولین خط دفاعی در برابر دسترسی‌های غیرمجاز و حملات مخرب محسوب می‌شوند. در این مقاله به بررسی اهمیت اجرای سیاست‌های کلمه‌عبور، اصول و روش‌های پیاده‌سازی آن‌ها و ابزارها و برنامه‌های مرتبط می‌پردازیم.</td><td>›<br>بعد از</td><td>---</td></tr>
<tr><td>‹<br>قبل از</td><td>Default account settings</td></tr>
<tr><td>پیاده سازی عملی: بله</td><td>پژوهشی: بله</td><td>راهنمای عملی: بله</td></tr>
</table>

## اجرای سیاست‌های کلمه‌عبور در لینوکس

یکی از جنبه‌های حیاتی امنیت حساب‌های کاربری در سرورهای لینوکس، اجرای سیاست‌های کلمه‌عبور است. کلمه‌عبورهای قوی و امن، اولین خط دفاعی در برابر دسترسی‌های غیرمجاز و حملات مخرب محسوب می‌شوند. در این مقاله به بررسی اهمیت اجرای سیاست‌های کلمه‌عبور، اصول و روش‌های پیاده‌سازی آن‌ها و ابزارها و برنامه‌های مرتبط می‌پردازیم.

## اهمیت اجرای سیاست‌های کلمه‌عبور

کلمه‌عبورهای ضعیف و قابل حدس می‌توانند به راحتی توسط مهاجمان شکسته شوند و دسترسی غیرمجاز به سیستم‌ها و داده‌های حساس را فراهم کنند. اجرای سیاست‌های کلمه‌عبور قوی و پیچیده به موارد زیر کمک می‌کند:

۱. **افزایش امنیت سیستم** :با استفاده از کلمه‌عبورهای قوی و پیچیده، احتمال دسترسی غیرمجاز به سیستم کاهش می‌یابد.

۲. **محافظت از داده‌های حساس** :داده‌های حساس و مهم با استفاده از کلمه‌عبورهای قوی بهتر محافظت می‌شوند.

۳. **جلوگیری از حملات Brute Force:** کلمه‌عبورهای پیچیده‌تر می‌توانند زمان لازم برای شکستن کلمه‌عبور را افزایش دهند و از حملات Brute Force جلوگیری کنند.

## اصول سیاست‌های کلمه‌عبور

سیاست‌های کلمه‌عبور می‌توانند شامل موارد زیر باشند:

۱. **حداقل طول کلمه‌عبور** :تعیین حداقل طول برای کلمه‌عبور به افزایش پیچیدگی آن کمک می‌کند.

۲. **ترکیب حروف، اعداد و نمادها** :استفاده از ترکیبی از حروف بزرگ و کوچک، اعداد و نمادها می‌تواند امنیت کلمه‌عبور را افزایش دهد.

۳. **محدودیت تکرار کاراکترها** :جلوگیری از استفاده مکرر از یک کاراکتر در کلمه‌عبور.

٤. **تغییر دوره‌ای کلمه‌عبور** :الزام کاربران به تغییر کلمه‌عبور خود به صورت دوره‌ای می‌تواند امنیت حساب‌ها را بهبود بخشد.

۵. **عدم استفاده از کلمه‌عبورهای قدیمی** :جلوگیری از استفاده مجدد از کلمه‌عبورهای قبلی.

٦. **قفل کردن حساب کاربری پس از تلاش‌های ناموفق مکرر** :محدود کردن تعداد تلاش‌های ناموفق برای ورود به سیستم می‌تواند از حملات Brute Force جلوگیری کند.

## ابزارها و برنامه‌های مفید برای اجرای سیاست‌های کلمه‌عبور

1. **PAM (Pluggable Authentication Modules)**:

PAM یک مجموعه از ماژول‌های احراز هویت است که به مدیران سیستم امکان می‌دهد سیاست‌های کلمه‌عبور را به طور دقیق کنترل کنند.

2. **libpam-pwquality**:

این ماژول PAM به بررسی کیفیت کلمه‌عبور و اجرای سیاست‌های پیچیدگی کمک می‌کند. برای نصب و پیکربندی آن، می‌توانید از دستورات زیر استفاده کنید:

```
sudo apt-get install libpam-pwquality
```

سپس فایل /etc/pam.d/common-passwordرا ویرایش کنید و خط زیر را اضافه کنید:

```
password requisite pam_pwquality.so retry=3 minlen=12 dcredit=-1 ucredit=-1
ocredit=-1 lcredit=-1 enforce_for_root
```

3. **chage**:

ابزار chageبرای مدیریت و تغییر سیاست‌های کلمه‌عبور کاربران استفاده می‌شود. با استفاده از این ابزار می‌توانید زمان انقضای کلمه‌عبور و سایر تنظیمات را مشخص کنید.

```
sudo chage -M 90 -m 7 -W 7 username
```

4. **faillock**:

ابزار faillockبرای قفل کردن حساب‌های کاربری پس از تلاش‌های ناموفق مکرر استفاده می‌شود. برای پیکربندی آن، می‌توانید فایل /etc/security/faillock.confرا ویرایش کنید و تنظیمات مورد نظر را اعمال کنید.

```
deny=5

unlock_time=600
```

## نتیجه‌گیری

اجرای سیاست‌های کلمه‌عبور قوی و پیچیده یکی از مهم‌ترین اقدامات برای افزایش امنیت حساب‌های کاربری در سرورهای لینوکس است. با استفاده از ابزارها و روش‌های مناسب، می‌توان از دسترسی‌های غیرمجاز و حملات مخرب جلوگیری کرد و امنیت سیستم را به طور قابل توجهی بهبود بخشید. آشنایی و پیاده‌سازی صحیح این سیاست‌ها به مدیران سیستم کمک می‌کند تا از داده‌های حساس خود محافظت کرده و از عملکرد بهینه سرورهای خود اطمینان حاصل کنند.

## منابع و ارجاعات


- https://roadmap.sh/linux
- https://roadmap.sh/r/general-linux-server-hardening
- https://www.pluralsight.com/cloud-guru/labs/aws/working-with-linux-accounts-and-password-policies
- https://www.baeldung.com/linux/password-complexity
- https://ostechnix.com/how-to-set-password-policies-in-linux/
- https://linux.die.net/man/8/pam_pwquality