



User Account Security	S08 T02	
	Default account settings	
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.		Password policy enforcement
	بعد از	
		User activity logging
	قبل از	
پیاده سازی عملی: خیر	پژوهشی: خیر	راهنمای عملی: بله

تنظیمات پیش فرض حساب کاربری در لینوکس

یکی از اصول مهم در امنیت حساب‌های کاربری در سرورهای لینوکسی، تنظیمات پیش فرض 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 پیش فرض حساب کاربری، اهمیت آن و نحوه پیاده‌سازی آن در لینوکس می‌پردازیم.

اهمیت تنظیمات پیش فرض حساب کاربری

تنظیمات پیش فرض حساب‌های کاربری از چند جنبه اهمیت دارند:

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

تنظیمات پیش فرض حساب کاربری

۱. **تنظیمات کلمه عبور:** یکی از مهم‌ترین تنظیمات پیش فرض حساب‌های کاربری، تنظیمات مربوط به کلمه عبور 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
```

۲. **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
```

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

```
sudo usermod -s /sbin/nologin username
```

۴. **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
```

۵. **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
```

۶. **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 کلمه عبور قوی و پیچیده.

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

2. **usermod:**

ابزاری برای مدیریت کاربران و تنظیمات پیش‌فرض آن‌ها.

```
sudo usermod -aG groupname username
```

3. **chmod:**

ابزاری برای تنظیم مجوزهای فایل و دایرکتوری.

```
sudo chmod 700 /home/username
```

4. **/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.

منابع و ارجاعات

- <https://roadmap.sh/linux>
- <https://roadmap.sh/r/general-linux-server-hardening>