User Account Security	S08 T04	
	User environment restriction	
یکی از جنبه‌های حیاتی در امنیت حساب‌های کاربری در سرورهای لینوکسی، اعمال محدودیت‌های محیط کاربری است. این محدودیت‌ها به مدیران سیستم کمک می‌کند تا کنترل بیشتری بر دسترسی‌ها و فعالیت‌های کاربران داشته باشند و از سوءاستفاده‌های احتمالی جلوگیری کنند. در این مقاله، به بررسی مفهوم محدودیت‌های محیط کاربری، اهمیت آن و روش‌های پیاده‌سازی آن در لینوکس می‌پردازیم.	 بعد از	User activity logging
	 قبل از	User-based access control lists
راهنمای عملی: **بله**	پژوهشی: **خیر**	پیاده سازی عملی: **خیر**

محدودیت‌های محیط کاربری در لینوکس

یکی از جنبه‌های حیاتی در امنیت حساب‌های کاربری در سرورهای لینوکسی، اعمال محدودیت‌های محیط کاربری است. این محدودیت‌ها به مدیران سیستم کمک می‌کند تا کنترل بیشتری بر دسترسی‌ها و فعالیت‌های کاربران داشته باشند و از سوءاستفاده‌های احتمالی جلوگیری کنند. در این مقاله، به بررسی مفهوم محدودیت‌های محیط کاربری، اهمیت آن و روش‌های پیاده‌سازی آن در لینوکس می‌پردازیم.

اهمیت محدودیت‌های محیط کاربری

اعمال محدودیت‌های محیط کاربری از چند جنبه اهمیت دارد:

۱. **جلوگیری از دسترسی‌های غیرمجاز** :با محدود کردن محیط کاربری، می‌توان از دسترسی‌های غیرمجاز کاربران به فایل‌ها و دایرکتوری‌های حساس جلوگیری کرد.

۲. **افزایش امنیت سیستم** :با محدود کردن دسترسی کاربران به تنها ابزارها و دستورات ضروری، سطح حملات احتمالی کاهش یافته و امنیت کلی سیستم افزایش می‌یابد.

۳. **کاهش احتمال خطاهای کاربران** :محدود کردن محیط کاربری می‌تواند از انجام عملیات غیرمجاز یا اشتباه توسط کاربران جلوگیری کند.

٤. **کنترل فعالیت‌های کاربران** :با محدود کردن محیط کاربری، مدیران سیستم می‌توانند فعالیت‌های کاربران را بهتر کنترل و مانیتور کنند.

روش‌های پیاده‌سازی محدودیت‌های محیط کاربری

۱. **استفاده از Shell محدود (Restricted Shell)**: یک Shell محدود مانند rbashبه کاربر اجازه می‌دهد تا تنها دستورات خاصی را اجرا کند و دسترسی به سایر دستورات و ابزارها را محدود می‌کند.

```
sudo usermod -s /bin/rbash username
```

۲. **استفاده از ابزار chroot**: chroot به شما اجازه می‌دهد تا یک محیط فایل سیستم جداگانه برای یک کاربر ایجاد کنید. این کار به ایزوله کردن کاربر و محدود کردن دسترسی او به فایل‌ها و دایرکتوری‌های سیستم کمک می‌کند.

```
sudo mkdir -p /var/chroot/myuser

sudo chown root:root /var/chroot/myuser

sudo mkdir -p /var/chroot/myuser/{bin,lib,lib64,usr}

sudo chroot /var/chroot/myuser /bin/bash
```

۳. **استفاده از AppArmor و SELinux**: این ابزارها به شما امکان می‌دهند تا سیاست‌های امنیتی خاصی برای کاربران و فرآیندها تعریف کنید و دسترسی‌های آن‌ها را محدود کنید.

```
sudo apt-get install apparmor

sudo systemctl start apparmor

sudo aa-enforce /etc/apparmor.d/usr.bin.myapp
```

٤. **استفاده از sudo**: با استفاده از sudo می‌توان دسترسی کاربران به دستورات خاص را محدود کرد. فایل پیکربندی sudo را با دستور visudo ویرایش کنید.

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

٥. **محدود کردن دسترسی به منابع سیستم با cgroups**: با استفاده از cgroups می‌توان منابع سیستم مانند CPU ، حافظه و I/O را برای کاربران خاص محدود کرد.

```
sudo cgcreate -g cpu,memory:myusergroup

sudo cgset -r memory.limit_in_bytes=512M myusergroup

sudo cgexec -g cpu,memory:myusergroup /bin/bash
```

ابزارها و برنامه‌های مفید

1. **rbash**:

یک Shell محدود که دسترسی کاربران به دستورات غیرمجاز را محدود می‌کند.

```
sudo usermod -s /bin/rbash username
```

2. **chroot**:

ابزاری برای ایجاد محیط فایل سیستم جداگانه برای کاربران.

```
sudo chroot /path/to/new/root /bin/bash
```

3. **AppArmor و SELinux**:

ابزارهای امنیتی برای تعریف و اعمال سیاست‌های امنیتی خاص برای کاربران و فرآیندها.

```
sudo apt-get install apparmor

sudo systemctl start apparmor
```

4. **sudo**:

ابزاری برای محدود کردن دسترسی کاربران به دستورات خاص.

```
sudo visudo
```

5. **cgroups**:

ابزارهای داخلی لینوکس برای محدود کردن منابع سیستم برای کاربران خاص.

```
sudo apt-get install cgroup-tools
```

نتیجه‌گیری

اعمال محدودیت‌های محیط کاربری یکی از اصول اساسی در افزایش امنیت حساب‌های کاربری و سیستم‌های لینوکسی است. با استفاده از روش‌ها و ابزارهای مناسب، می‌توان دسترسی به منابع سیستم را کنترل و از سوءاستفاده‌های احتمالی جلوگیری کرد. آشنایی و پیاده‌سازی صحیح این محدودیت‌ها 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