



User Account Security	S08 T03	
	User activity logging	
<p>یکی از جنبه‌های حیاتی در امنیت حساب‌های کاربری در سرورهای لینوکسی، لاگ‌گیری فعالیت‌های کاربران است. این فرآیند به مدیران سیستم امکان می‌دهد تا فعالیت‌های کاربران را مانیتور کرده و هرگونه رفتار مشکوک یا غیرمجاز را شناسایی کنند. در این مقاله، به معرفی مفهوم لاگ‌گیری فعالیت‌های کاربران، اهمیت آن و ابزارها و روش‌های پیاده‌سازی آن در لینوکس می‌پردازیم.</p>		Default account settings
	بعد از	
		User environment restriction
	قبل از	
پیاده سازی عملی: بله	پژوهشی: خیر	راهنمای عملی: بله

## لاگ‌گیری فعالیت‌های کاربران در لینوکس

یکی از جنبه‌های حیاتی در امنیت حساب‌های کاربری در سرورهای لینوکسی، لاگ‌گیری فعالیت‌های کاربران است. این فرآیند به مدیران سیستم امکان می‌دهد تا فعالیت‌های کاربران را مانیتور کرده و هرگونه رفتار مشکوک یا غیرمجاز را شناسایی کنند. در این مقاله، به معرفی مفهوم لاگ‌گیری فعالیت‌های کاربران، اهمیت آن و ابزارها و روش‌های پیاده‌سازی آن در لینوکس می‌پردازیم.

## اهمیت لاگ‌گیری فعالیت‌های کاربران

لاگ‌گیری فعالیت‌های کاربران از چند جنبه اهمیت دارد:

۱. **شناسایی رفتارهای مشکوک:** با مانیتورینگ و بررسی لاگ‌های فعالیت‌های کاربران، مدیران سیستم می‌توانند هرگونه رفتار مشکوک یا غیرمجاز را شناسایی کرده و به موقع واکنش نشان دهند.
۲. **افزایش امنیت سیستم:** لاگ‌گیری فعالیت‌ها می‌تواند به مدیران سیستم کمک کند تا نقاط ضعف امنیتی را شناسایی و برطرف کنند، که این امر به افزایش امنیت کلی سیستم منجر می‌شود.
۳. **ردیابی و تحلیل رخدادها:** در صورت بروز حادثه امنیتی، لاگ‌های فعالیت‌های کاربران می‌توانند به عنوان منبعی مفید برای ردیابی و تحلیل رخدادها استفاده شوند.
۴. **مطابقت با مقررات و استانداردها:** بسیاری از مقررات و استانداردهای امنیتی نیازمند لاگ‌گیری فعالیت‌های کاربران به منظور اطمینان از رعایت اصول امنیتی هستند.

## ابزارها و روش‌های لاگ‌گیری فعالیت‌های کاربران

### 1. **auditd:** استفاده از ابزار

auditd یک سرویس لاگ‌گیری پیشرفته در لینوکس است که به مدیران سیستم امکان می‌دهد تا فعالیت‌های کاربران و رخدادهای سیستم را به طور دقیق مانیتور کنند.

- auditd نصب:

```
sudo apt-get install auditd

sudo systemctl enable auditd

sudo systemctl start auditd
```

- پیکربندی قوانین لاگ‌گیری: فایل پیکربندی قوانین لاگ‌گیری در مسیر `/etc/audit/audit.rules` قرار دارد. می‌توانید قوانین مختلفی برای لاگ‌گیری فعالیت‌های کاربران تعریف کنید:

```
-w /etc/passwd -p wa -k passwd_changes

-w /var/log/auth.log -p wa -k auth_changes
```

## 2. syslog استفاده از ابزار:

syslog یک سیستم لاگ‌گیری استاندارد در لینوکس است که لاگ‌های مختلف سیستم را جمع‌آوری و ذخیره می‌کند.

- پیکربندی syslog: فایل پیکربندی syslog در مسیر `/etc/rsyslog.conf` قرار دارد. می‌توانید تنظیمات مربوط به لاگ‌گیری فعالیت‌های کاربران را در این فایل تعریف کنید:

```
auth.* /var/log/auth.log
```

## 3. lastlog استفاده از ابزار:

این ابزارها برای مشاهده آخرین ورودهای کاربران به سیستم و لاگ‌های مربوط به آن‌ها استفاده می‌شوند.

- مشاهده آخرین ورودهای کاربران:

```
last
```

- مشاهده لاگ‌های ورود کاربران

```
lastlog
```

#### 4. `bash_history` استفاده از:

فایل `bash_history` در دایرکتوری خانه هر کاربر، تاریخچه دستورات اجرا شده توسط آن کاربر را ذخیره می‌کند. می‌توانید این فایل را بررسی کنید تا فعالیت‌های کاربران را مشاهده کنید.

- مشاهده تاریخچه دستورات

```
cat ~/.bash_history
```

#### 5. `acct` استفاده از ابزار:

ابزار `acct` برای مانیتورینگ و لاگ‌گیری فعالیت‌های کاربران در سطح سیستم استفاده می‌شود.

- نصب `acct`:

```
sudo apt-get install acct

sudo systemctl enable acct

sudo systemctl start acct
```

- مشاهده گزارش‌های فعالیت‌های کاربران:

```
ac
```

```
lastcomm
```

## نتیجه‌گیری

لاگ‌گیری فعالیت‌های کاربران یکی از اصول اساسی در افزایش امنیت حساب‌های کاربری و سیستم‌های لینوکسی است. با استفاده از ابزارها و روش‌های مناسب، می‌توان فعالیت‌های کاربران را مانیتور کرد و از دسترسی‌های غیرمجاز و رفتارهای مشکوک جلوگیری کرد. آشنایی و پیاده‌سازی صحیح این ابزارها 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>