<table>
<tr><td rowspan="2">File System Hardening</td><td colspan="2">S04 T06</td></tr>
<tr><td colspan="2">Encryption of sensitive data</td></tr>
<tr><td rowspan="2">یکی از اصول اساسی در سخت‌کردن سرورهای لینوکس، حفاظت از داده‌های حساس است. رمزنگاری یکی از بهترین روش‌ها برای حفاظت از این داده‌ها در برابر دسترسی‌های غیرمجاز و حملات مختلف است. در این مقاله به معرفی رمزنگاری داده‌های حساس در لینوکس و ابزارهای مرتبط با آن می‌پردازیم.</td><td>بعد از</td><td>File integrity checkers (AIDE, Tripwire)</td></tr>
<tr><td>قبل از</td><td>---</td></tr>
<tr><td>پیاده سازی عملی: بله</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

رمزنگاری داده‌های حساس در لینوکس

یکی از اصول اساسی در سخت‌کردن سرورهای لینوکس، حفاظت از داده‌های حساس است. رمزنگاری یکی از بهترین روش‌ها برای حفاظت از این داده‌ها در برابر دسترسی‌های غیرمجاز و حملات مختلف است. در این مقاله به معرفی رمزنگاری داده‌های حساس در لینوکس و ابزارهای مرتبط با آن می‌پردازیم.

رمزنگاری چیست؟

رمزنگاری فرآیندی است که طی آن داده‌ها به شکلی تغییر می‌کنند که تنها افراد مجاز قادر به خواندن آن‌ها باشند. این فرآیند شامل استفاده از الگوریتم‌ها و کلیدهای رمزنگاری برای تبدیل داده‌های قابل خواندن به فرمتی غیرقابل خواندن است. تنها با داشتن کلید صحیح می‌توان این داده‌ها را دوباره به شکل اولیه و قابل خواندن تبدیل کرد.

انواع رمزنگاری

۱. **رمزنگاری متقارن** :در این نوع رمزنگاری، از یک کلید واحد برای رمزنگاری و رمزگشایی داده‌ها استفاده می‌شود. الگوریتم‌هایی مانند AES (Advanced Encryption Standard) نمونه‌هایی از رمزنگاری متقارن هستند.

۲. **رمزنگاری نامتقارن** :این نوع رمزنگاری از دو کلید مجزا استفاده می‌کند: یک کلید عمومی برای رمزنگاری و یک کلید خصوصی برای رمزگشایی. الگوریتم‌هایی مانند RSA (Rivest-Shamir-Adlemanو) ECC (Elliptic Curve Cryptography) از نمونه‌های رمزنگاری نامتقارن هستند.

ابزارها و برنامه‌های رمزنگاری در لینوکس

لینوکس دارای ابزارها و برنامه‌های متنوعی برای رمزنگاری داده‌های حساس است. برخی از این ابزارها عبارتند از:

1. **GnuPG (GPG)**:

GnuPG یک ابزار قدرتمند برای رمزنگاری و امضای دیجیتال است که از رمزنگاری نامتقارن استفاده می‌کند. این ابزار به شما امکان می‌دهد تا فایل‌ها و ایمیل‌های خود را رمزنگاری کرده و امضاهای دیجیتال را تأیید کنید.

```
gpg --encrypt --recipient recipient@example.com file.txt

gpg --decrypt file.txt.gpg
```

2. **OpenSSL**:

OpenSSL یک کتابخانه و ابزار خط فرمان برای استفاده از پروتکل‌های SSL و TLS و همچنین رمزنگاری داده‌ها است. این ابزار می‌تواند برای رمزنگاری فایل‌ها و داده‌ها با استفاده از الگوریتم‌های مختلف مورد استفاده قرار گیرد.

```
openssl enc -aes-256-cbc -salt -in file.txt -out file.txt.enc

openssl enc -d -aes-256-cbc -in file.txt.enc -out file.txt
```

3. **LUKS (Linux Unified Key Setup)**:

LUKS یک استاندارد برای رمزنگاری دیسک در لینوکس است. این ابزار برای رمزنگاری پارتیشن‌ها و دیسک‌های کامل استفاده می‌شود و از رمزنگاری متقارن برای حفاظت از داده‌ها استفاده می‌کند.

```
sudo cryptsetup luksFormat /dev/sdX

sudo cryptsetup luksOpen /dev/sdX encrypted_drive

sudo mkfs.ext4 /dev/mapper/encrypted_drive
```

4. **eCryptfs:**

eCryptfs یک سیستم فایل رمزنگاری شده در سطح فایل است که به شما امکان می‌دهد پوشه‌های خاصی را رمزنگاری کنید. این ابزار به طور خاص برای رمزنگاری پوشه‌های خانگی کاربران در لینوکس استفاده می‌شود.

```
sudo mount -t ecryptfs /path/to/source /path/to/destination
```

نکات مهم در رمزنگاری داده‌ها

- **استفاده از الگوریتم‌های قوی** :همیشه از الگوریتم‌های رمزنگاری قوی و استاندارد مانند-AES 256استفاده کنید.
- **مدیریت کلید** :اطمینان حاصل کنید که کلیدهای رمزنگاری به صورت امن مدیریت و ذخیره می‌شوند. از ذخیره کردن کلیدها در مکان‌های ناامن خودداری کنید.
- **بروزرسانی منظم** :ابزارها و کتابخانه‌های رمزنگاری باید به طور منظم بروزرسانی شوند تا از امنیت آن‌ها اطمینان حاصل شود.

نتیجه‌گیری

رمزنگاری داده‌های حساس یکی از مهم‌ترین اقدامات در جهت حفاظت از اطلاعات و افزایش امنیت سرورهای لینوکس است. با استفاده از ابزارها و تکنیک‌های مناسب، می‌توان از دسترسی غیرمجاز به داده‌ها جلوگیری کرد و امنیت سیستم را بهبود بخشید. آشنایی و استفاده صحیح از این ابزارها، به مدیران سیستم کمک می‌کند تا از داده‌های خود به بهترین نحو ممکن محافظت کنند.

منابع و ارجاعات

- https://roadmap.sh/linux