



File System Hardening	S04 T05	
	File integrity checkers (AIDE, Tripwire)	
<p>یکی از مهم‌ترین جنبه‌های سخت‌کردن سرورهای لینوکس، اطمینان از یکپارچگی فایل‌های سیستم است. ابزارهای بررسی یکپارچگی فایل‌ها، مانند AIDE و Tripwire، به مدیران سیستم کمک می‌کنند تا تغییرات غیرمجاز در فایل‌ها و پوشه‌ها را شناسایی کرده و از سلامت و امنیت سیستم اطمینان حاصل کنند.</p>		ACL (access control lists)
	بعد از	
		Encryption of sensitive data
	قبل از	
پیاده سازی عملی: خیر	پژوهشی: خیر	راهنمای عملی: بله

بررسی کننده‌های یکپارچگی فایل در لینوکس

یکی از مهم‌ترین جنبه‌های سخت‌کردن سرورهای لینوکس، اطمینان از یکپارچگی فایل‌های سیستم است. ابزارهای بررسی یکپارچگی فایل‌ها، مانند AIDE و Tripwire، به مدیران سیستم کمک می‌کنند تا تغییرات غیرمجاز در فایل‌ها و پوشه‌ها را شناسایی کرده و از سلامت و امنیت سیستم اطمینان حاصل کنند.

AIDE چیست؟

AIDE (Advanced Intrusion Detection Environment) یک ابزار متن‌باز برای بررسی یکپارچگی فایل‌ها در سیستم‌های لینوکسی است. این ابزار با ایجاد پایگاه داده‌ای از فایل‌های سیستم و ویژگی‌های آن‌ها (مانند مجوزها، مالکیت، هش‌ها و غیره)، در هنگام اجرای مجدد می‌تواند تغییرات را شناسایی کند.

ویژگی‌های AIDE

- **متن‌باز و رایگان** AIDE: به صورت رایگان در دسترس است و می‌توان آن را به آسانی نصب و پیکربندی کرد.
- **پشتیبانی از الگوریتم‌های هش مختلف** AIDE: از الگوریتم‌های هش مختلفی مانند MD5، SHA1 و غیره پشتیبانی می‌کند.
- **قابلیت پیکربندی بالا**: می‌توان تنظیمات AIDE را به گونه‌ای سفارشی‌سازی کرد که نیازهای خاص سیستم را برآورده کند.

نحوه نصب و استفاده از AIDE

برای نصب AIDE در سیستم‌های مبتنی بر Debian/Ubuntu، می‌توان از فرمان زیر استفاده کرد:

```
sudo apt-get install aide
```

پس از نصب، می‌توان با فرمان زیر پایگاه داده اولیه را ایجاد کرد:

```
sudo aideinit
```

برای اجرای بررسی یکپارچگی فایل‌ها، می‌توان از فرمان زیر استفاده کرد:

```
sudo aide --check
```

Tripwire چیست؟

Tripwire یکی دیگر از ابزارهای مشهور برای بررسی یکپارچگی فایل‌ها است. این ابزار، مانند AIDE، تغییرات در فایل‌های سیستم را شناسایی می‌کند و به مدیران سیستم هشدار می‌دهد. نسخه‌های تجاری و رایگان Tripwire موجود است و نسخه رایگان آن معمولاً برای محیط‌های کوچک تا متوسط مناسب است.

ویژگی‌های Tripwire

- **پشتیبانی از سیستم‌عامل‌های مختلف** Tripwire: بر روی سیستم‌عامل‌های مختلفی از جمله لینوکس و یونیکس اجرا می‌شود.
- **قابلیت هشداردهی**: می‌توان Tripwire را طوری تنظیم کرد که در صورت شناسایی تغییرات غیرمجاز، به مدیر سیستم هشدار دهد.
- **پشتیبانی از الگوریتم‌های هش مختلف**: مانند AIDE، Tripwire نیز از الگوریتم‌های هش مختلف پشتیبانی می‌کند.

نحوه نصب و استفاده از Tripwire

برای نصب Tripwire در سیستم‌های مبتنی بر Debian/Ubuntu، می‌توان از فرمان زیر استفاده کرد:

```
sudo apt-get install tripwire
```

پس از نصب، باید پایگاه داده اولیه را ایجاد و تنظیمات اولیه را انجام داد:

```
sudo twadmin --init
```

```
sudo tripwire -check
```

نتیجه‌گیری

استفاده از ابزارهای بررسی یکپارچگی فایل مانند AIDE و Tripwire یکی از بهترین روش‌ها برای اطمینان از امنیت و سلامت سیستم‌های لینوکسی است. این ابزارها با شناسایی تغییرات غیرمجاز در فایل‌ها و پوشه‌ها، به مدیران سیستم کمک می‌کنند تا به موقع اقدام‌های لازم را انجام دهند و از حملات و نفوذهای احتمالی جلوگیری کنند. هر مدیر سیستمی باید با این ابزارها آشنا باشد و بتواند آن‌ها را به درستی پیکربندی و استفاده کند تا امنیت سیستم‌های خود را تضمین نماید.

منابع و ارجاعات

- <https://roadmap.sh/linux>