<table>
<tr><td rowspan="2">File System Hardening</td><td colspan="3">S04 T02</td></tr>
<tr><td colspan="3">Mount options for system file systems</td></tr>
<tr><td rowspan="2">تنظیمات Mount به مدیر سیستم این امکان را می‌دهد که نحوه دسترسی و استفاده از سیستم فایل‌ها را کنترل کند و با اعمال محدودیت‌های مناسب، امنیت سیستم را افزایش دهد.</td><td>بعد از</td><td colspan="2">File permissions and ownership</td></tr>
<tr><td>قبل از</td><td colspan="2">Sticky bit, SUID, SGID</td></tr>
<tr><td>پیاده سازی عملی: خیر</td><td>پژوهشی: بله</td><td>راهنمای عملی: خیر</td></tr>
</table>

تنظیمات Mount برای سیستم فایل‌های سیستم در لینوکس

یکی از جنبه‌های مهم امنیت سرورهای لینوکس، سخت‌کردن سیستم فایل است. در این زمینه، تنظیمات Mount برای سیستم فایل‌های سیستم از اهمیت ویژه‌ای برخوردار است. تنظیمات Mount به مدیر سیستم این امکان را می‌دهد که نحوه دسترسی و استفاده از سیستم فایل‌ها را کنترل کند و با اعمال محدودیت‌های مناسب، امنیت سیستم را افزایش دهد.

مقدمه‌ای بر تنظیماتMount

هنگامی که یک سیستم فایل در لینوکس Mount می‌شود، می‌توان با استفاده از گزینه‌های مختلف، سطح دسترسی و ویژگی‌های آن را تنظیم کرد. این تنظیمات می‌توانند از سوء استفاده‌های احتمالی جلوگیری کنند و سیستم را در برابر حملات مختلف محافظت نمایند. برخی از این گزینه‌ها شامل noexec, nosuid, nodevو roهستند.

گزینه‌های مهمMount

۱. **noexec**: این گزینه اجرای فایل‌های باینری را از روی سیستم فایل منع می‌کند. با استفاده از این گزینه، حتی اگر یک فایل اجرایی روی سیستم فایل قرار داده شود، نمی‌توان آن را اجرا کرد.

۲. **nosuid**: این گزینه از استفاده از بیت‌های setuid و setgid در فایل‌های موجود روی سیستم فایل جلوگیری می‌کند. به این معنی که فایل‌ها نمی‌توانند با سطح دسترسی کاربر مالک فایل اجرا شوند، بلکه تنها با سطح دسترسی کاربر فعلی اجرا می‌شوند.

۳. **nodev**: این گزینه ایجاد دستگاه‌های خاص (device files) را روی سیستم فایل منع می‌کند. این امر از سوء استفاده‌هایی که ممکن است با استفاده از دستگاه‌های خاص صورت گیرد، جلوگیری می‌کند.

۴. **ro**: این گزینه سیستم فایل را به صورت فقط‌خواندنی Mount (read-only) می‌کند. این تنظیم می‌تواند برای جلوگیری از تغییرات ناخواسته در سیستم فایل‌های حساس مورد استفاده قرار گیرد.

ابزارها و برنامه‌های مفید

برای پیاده‌سازی و مدیریت تنظیماتMount ، می‌توان از ابزارها و برنامه‌های مختلفی استفاده کرد:

۱. **fstab**: فایل پیکربندی /etc/fstab یکی از مهم‌ترین ابزارها برای مدیریت تنظیمات Mount است. با ویرایش این فایل می‌توان تنظیمات مختلفی را برای سیستم فایل‌های مختلف تعریف کرد تا به صورت خودکار در هنگام بوت سیستم اعمال شوند.

۲. **mount**: فرمان mount به مدیر سیستم این امکان را می‌دهد که سیستم فایل‌ها را به صورت دستی Mount یا Unmount کند و تنظیمات مختلفی را در زمان Mount اعمال نماید.

۳. **auditd**: برنامه auditd برای مانیتورینگ و ثبت رخدادهای مربوط به سیستم فایل‌ها استفاده می‌شود. با استفاده از این برنامه می‌توان تغییرات و دسترسی‌های غیرمجاز را شناسایی و ثبت کرد.

۴. **SELinux**: سیاست‌های امنیتی SELinux می‌توانند برای محدود کردن دسترسی به سیستم فایل‌ها استفاده شوند. با تنظیم مناسب سیاست‌ها، می‌توان دسترسی‌های غیرمجاز را مسدود کرد و امنیت سیستم را افزایش داد.

نتیجه‌گیری

تنظیمات Mount برای سیستم فایل‌های سیستم یکی از ابزارهای مهم در سخت‌کردن سیستم‌های لینوکسی است. با استفاده از گزینه‌های مناسب و ابزارهای مدیریتی، می‌توان دسترسی‌ها را بهینه‌سازی و امنیت سیستم را بهبود بخشید. هر مدیر سیستمی باید با این تنظیمات و ابزارها آشنا باشد تا بتواند از سیستم‌های خود به بهترین نحو ممکن محافظت کند.

منابع و ارجاعات

- https://roadmap.sh/linux
- http://sokanac.ir/hI8
- https://youtu.be/HahSq4lYS3I?si=ASr4kYuHm7T5iIvG
- https://www.youtube.com/results?search_query=mounts%20for%20linux