<table>
<tr><td rowspan="2">Understanding of Basic Linux Systems</td><td colspan="2">S01 T07</td></tr>
<tr><td colspan="2">Linux system logs</td></tr>
<tr><td rowspan="2">لینوکس، مانند سایر سیستم‌عامل‌ها، لاگ‌ها را برای کمک به مدیران در درک آنچه که در سیستم اتفاق می‌افتد، نگهداری می‌کند. این لاگ‌ها همه چیز را مستند می‌کنند، از جمله فعالیت‌های کاربران، خطاهای سیستم و پیام‌های هسته. زمان بسیار مهمی برای پیام‌های لاگ مفید، فرآیند بوت سیستم است، زمانی که اجزای کلیدی سیستم بارگذاری و راه‌اندازی می‌شوند.</td><td>بعد از ›</td><td>Linux user and group management</td></tr>
<tr><td>قبل از ‹</td><td>---</td></tr>
<tr><td>راهنمای عملی: بله</td><td>پژوهشی: بله</td><td>پیاده سازی عملی: خیر</td></tr>
</table>

مقدمه‌ای بر لاگ‌ها

"لاگ‌ها در هنگام بوت" در لینوکس به پیام‌ها و اطلاعاتی اشاره دارد که در طول فرآیند بوت تولید می‌شوند. این لاگ‌ها تمام عملیات و رویدادهایی که در حین بوت شدن سیستم رخ می‌دهد را ثبت می‌کنند که ممکن است در تشخیص مشکل سیستم یا درک رفتار سیستم مفید باشد.

لینوکس از سطوح مختلف پیام‌های لاگ از emerg (سیستم غیرقابل استفاده است) تا debug (پیام‌های سطح اشکال‌زدایی) استفاده می‌کند. در طول فرآیند بوت، پیام‌هایی از اجزای مختلف سیستم مانند هسته، init، خدمات و غیره ذخیره می‌شوند. بسیاری از توزیع‌های لینوکس از سیستم لاگینگ systemd، یعنی journalctl، استفاده می‌کنند که لاگ‌های فرآیند بوت را نگهداری می‌کند.

مشاهده پیام‌های بوت می‌تواند در زمان واقعی با دستور dmesg انجام شود. این دستور برای خواندن و چاپ بافر حلقه‌ای هسته استفاده می‌شود. یا می‌توان آن‌ها را از طریق تنظیمات لاگینگ سیستم که اغلب شامل فایل‌های متنی در /var/log است، دسترسی داشت.

```
dmesg | less
```

این دستور لاگ‌های بوت را در قالبی کمتر مستقیم با قابلیت اسکرول به بالا و پایین نمایش می‌دهد. بافر حلقه‌ای هسته تنها اندازه مشخصی دارد، بنابراین پیام‌های قدیمی پس از مدتی حذف خواهند شد.

بررسی لاگ‌ها

بررسی لاگ‌ها در مدیریت سرویس‌ها در لینوکس نقش مهمی در مدیریت سیستم‌ها و روش‌های عیب‌یابی ایفا می‌کند. لاگ‌ها برای درک عمیق از آنچه که در داخل یک سیستم لینوکس اتفاق می‌افتد، اساسی هستند. این رکوردها یک سابقه زمانی از رویدادهای مرتبط با سیستم شما برای استفاده در اشکال‌زدایی و عیب‌یابی مشکلات فراهم می‌کنند.

چندین لاگ اساسی که توسط فرآیندهای سیستم، کاربران و اقدامات مدیران تولید می‌شوند را می‌توان در دایرکتوری /var/log یافت. لاگ‌ها را می‌توان با استفاده از چندین دستور دسترسی و مشاهده کرد. برای مثال، دستور dmesg می‌تواند برای نمایش بافر حلقه‌ای هسته استفاده شود. بیشتر لاگ‌های سیستم توسط systemd مدیریت می‌شوند و می‌توان با استفاده از دستور journalctl آن‌ها را بررسی کرد.

```
journalctl
```

این دستور کل لاگ سیستم را از زمان بوت تا لحظه‌ای که دستور journal فراخوانی می‌شود، نشان می‌دهد.

برای نمایش لاگ‌های یک سرویس خاص، می‌توان از گزینه u- استفاده کرد و نام سرویس را دنبال کرد.

```
journalctl -u service_name
```

به یاد داشته باشید، درک و نظارت بر لاگ‌های سیستم شما نمای روشنی از آنچه که در محیط لینوکس شما اتفاق می‌افتد، فراهم می‌کند. این یک مهارت حیاتی است که ارزش توسعه دارد تا به طور موثر سیستم‌ها را مدیریت و عیب‌یابی کنید.

لاگ‌های احراز هویت

هنگام کار با یک سرور لینوکس و نگهداری آن، یکی از اجزای بسیار مهم که باید به طور منظم بررسی شود، لاگ‌های احراز هویت است. این لاگ‌ها که معمولاً در /var/log/auth.log (برای توزیع‌های مبتنی بر دبیان) یا /var/log/secure برای Red Hat و CentOS قرار دارند، تمامی رویدادها و فعالیت‌های مربوط به احراز هویت که روی سرور رخ داده است را ثبت می‌کنند. این شامل، از جمله دیگر، ورود به سیستم، تغییر رمز عبور و دستورات صادر شده sudo است.

لاگ‌های احراز هویت یک ابزار بسیار ارزشمند برای نظارت و تحلیل امنیت سرور لینوکس شما هستند. آن‌ها می‌توانند حملات ورود به سیستم به روشbrute force ، تلاش‌های دسترسی غیرمجاز و هرگونه رفتار مشکوک را نشان دهند. تحلیل منظم این لاگ‌ها یک وظیفه اساسی در تضمین امنیت سرور و یکپارچگی داده‌ها است.

در اینجا یک مثال از چگونگی استفاده از دستور tail برای مشاهده آخرین ورودی‌های لاگ احراز هویت آورده شده است:

```
tail /var/log/auth.log
```

با خواندن و درک لاگ‌های احراز هویت آشنا شوید، زیرا این یکی از راه‌های اساسی برای حفظ امنیت سرور شماست.

منابع و ارجاعات

- https://youtu.be/vBDgTA-VYXo?si=IMl9Erxjmh65C-bg
- https://youtu.be/T-ut4oQfJI8?si=-eLSCkfqBH7M0x6t
- https://youtu.be/1_wf9O9QHCA?si=qRn53ekFNG78fEnv
- https://www.youtube.com/results?search_query=checking%20logs%20for%20linux

- https://www.youtube.com/results?search_query=auth%20logs%20for%20linux
- https://www.youtube.com/results?search_query=introduction%20to%20logs%20for%20linux
- https://roadmap.sh/linux