<table>
<tr><td rowspan="2">Linux Kernel Hardening</td><td colspan="3">S03 T01</td></tr>
<tr><td colspan="3">Kernel modules</td></tr>
<tr><td rowspan="3">ماژول‌های کرنل، قطعاتی از کد هستند که می‌توانند به صورت پویا به هسته لینوکس اضافه یا از آن حذف شوند. این ماژول‌ها قابلیت‌های اضافی به هسته اضافه می‌کنند بدون اینکه نیاز به کام ایل مجدد هسته باشد.</td><td>›
بعد از</td><td colspan="2">---</td></tr>
<tr><td>‹
قبل از</td><td colspan="2">Kernel parameter tuning</td></tr>
<tr><td>پیاده سازی عملی: خیر</td><td>پژوهشی: بله</td><td>راهنمای عملی: بله</td></tr>
</table>

Kernel Modulesچیست؟

Kernel Modulesیا ماژول‌های کرنل، قطعاتی از کد هستند که می‌توانند به صورت پویا به هسته لینوکس اضافه یا از آن حذف شوند. این ماژول‌ها قابلیت‌های اضافی به هسته اضافه می‌کنند بدون اینکه نیاز به کامپایل مجدد هسته باشد. این ویژگی به مدیران سیستم اجازه می‌دهد تا قابلیت‌ها را بر اساس نیازهای جاری سیستم مدیریت کنند.

امنیتKernel Modules

امن‌سازی ماژول‌های کرنل از اهمیت بالایی برخوردار است زیرا ماژول‌های کرنل می‌توانند به صورت مستقیم به هسته سیستم دسترسی داشته باشند و در صورت وجود ضعف یا نقص امنیتی، این دسترسی می‌تواند به آسیب‌پذیری‌های جدی منجر شود.

راهکارهای امن‌سازیKernel Modules

۱. **محدود کردن ماژول‌های بارگذاری شده:**

- فقط ماژول‌های مورد نیاز را بارگذاری کنید و ماژول‌های غیرضروری را حذف کنید.
- استفاده از ابزارهایی مانند **lsmod** برای بررسی ماژول‌های بارگذاری شده و **modprobe** یا **rmmod** برای مدیریت آنها.

۲. **کنترل دسترسی به ماژول‌ها:**

- استفاده از فایل **/etc/modprobe.d/** برای تنظیمات و محدودیت‌های ماژول‌ها.
- تنظیم **blacklist**برای جلوگیری از بارگذاری ماژول‌های ناخواسته.

۳. **بارگذاری ماژول‌ها با امضای دیجیتال:**

- استفاده از ماژول‌های کرنل با امضای دیجیتال برای اطمینان از اینکه ماژول‌های بارگذاری شده معتبر و دستکاری نشده‌اند.
- فعال کردن گزینه CONFIG_MODULE_SIG در کرنل و تنظیم کلیدهای عمومی و خصوصی برای امضای ماژول‌ها.

۴. **استفاده از SELinux و AppArmor:**

- پیاده‌سازی سیاست‌های امنیتی با استفاده از SELinux یا AppArmor برای محدود کردن دسترسی‌های ماژول‌های کرنل به منابع سیستم.

۵. **بروز نگه‌داشتن سیستم:**

- بروز رسانی مرتب هسته و ماژول‌های کرنل برای رفع آسیب‌پذیری‌های امنیتی شناخته شده.

مراحل عملی

۱. **مشاهده ماژول‌های فعال:**

```
lsmod
```

۲. **بارگذاری ماژول:**

```
modprobe <module_name>
```

۳. **حذف ماژول:**

```
rmmod <module_name>
```

۴. **ایجاد فایل پیکربندی برای جلوگیری از بارگذاری ماژول‌های ناخواسته:**

- ایجاد فایل در **/etc/modprobe.d/** به نام دلخواه، مثلاً **blacklist.conf**
- افزودن خط زیر برای جلوگیری از بارگذاری ماژول **usb-storage**:

```
blacklist usb-storage
```

نتیجه‌گیری

امن‌سازی ماژول‌های کرنل یک جزء کلیدی از فرایند سخت‌سازی هسته لینوکس است. با استفاده از روش‌های ذکر شده، می‌توانید ریسک‌های امنیتی مرتبط با ماژول‌های کرنل را کاهش داده و سیستم خود را امن‌تر کنید.

منابع و ارجاعات

- https://manpages.ubuntu.com/manpages/noble/en/man8/lsmod.8.html
- https://www.youtube.com/watch?v=AqVEnLIqeI8
- https://virgool.io/@randomhex/kernel-and-module-in-linux-uqptytl2mw6c
- https://www.youtube.com/watch?v=kdJsJ1wCUD4