



Linux Kernel Hardening	S03 T05	
	Linux kernel vulnerability scanning	
یکی از مهم‌ترین جنبه‌های امنیت سرورهای لینوکسی، سخت‌کردن کرنل لینوکس است. کرنل به‌عنوان هسته سیستم‌عامل، نقش حیاتی در مدیریت منابع سیستم و ارتباط با سخت‌افزار ایفا می‌کند. بنابراین، وجود آسیب‌پذیری در کرنل می‌تواند تهدیدهای جدی به امنیت سیستم وارد کند. در این مقاله، به توضیح و روش‌های عملی برای اسکن آسیب‌پذیری‌های کرنل لینوکس می‌پردازیم.		Linux kernel security updates
	بعد از	
		---
	قبل از	
پیاده سازی عملی:	پژوهشی: خیر	راهنمای عملی: بله

اهمیت اسکن آسیب‌پذیری‌های کرنل

آسیب‌پذیری‌های کرنل می‌توانند توسط مهاجمان مورد سوءاستفاده قرار گیرند تا به سیستم دسترسی غیرمجاز پیدا کنند، داده‌ها را سرقت کنند یا به سیستم آسیب بزنند. اسکن منظم آسیب‌پذیری‌های کرنل می‌تواند به شناسایی و رفع مشکلات امنیتی پیش از بهره‌برداری مهاجمان کمک کند.

ابزارهای اسکن آسیب‌پذیری‌های کرنل

برای اسکن آسیب‌پذیری‌های کرنل لینوکس، ابزارهای مختلفی وجود دارد. در ادامه، چند ابزار معروف را معرفی می‌کنیم:

• Lynis:

Lynis یک ابزار ارزیابی امنیتی و حسابرسی برای سیستم‌های لینوکسی است که می‌تواند کرنل را برای آسیب‌پذیری‌ها و پیکربندی‌های نادرست بررسی کند.

• Chkrootkit:

Chkrootkit یک ابزار شناسایی rootkit‌ها است که می‌تواند برخی از آسیب‌پذیری‌های کرنل را نیز شناسایی کند.

• OpenVAS:

OpenVAS یک ابزار کامل اسکن آسیب‌پذیری است که می‌تواند کرنل و سایر اجزای سیستم را اسکن کند.

مراحل عملی اسکن آسیب‌پذیری‌های کرنل

در این بخش، مراحل عملی برای استفاده از ابزار Lynis به‌عنوان نمونه برای اسکن آسیب‌پذیری‌های کرنل را شرح می‌دهیم.

نصب Lynis

ابتدا باید Lynis را نصب کنیم. در توزیع‌های مختلف لینوکس، می‌توان از دستورات زیر استفاده کرد:

Debian/Ubuntu:

```
sudo apt update  
  
sudo apt install lynis
```

Red Hat/CentOS:

```
sudo yum install epel-release  
  
sudo yum install lynis
```

اجرای اسکن با Lynis

پس از نصب Lynis، می‌توانیم اسکن سیستم را شروع کنیم. برای اسکن کامل سیستم، از دستور زیر استفاده کنید:

```
sudo lynis audit system
```

این دستور یک اسکن کامل روی سیستم اجرا می‌کند و گزارشی از آسیب‌پذیری‌ها و نقاط ضعف سیستم را ارائه می‌دهد. در این گزارش، به موارد مربوط به کرنل نیز اشاره خواهد شد.

بررسی گزارش و رفع آسیب‌پذیری‌ها

پس از اتمام اسکن، Lynis گزارشی جامع ارائه می‌دهد که شامل نقاط ضعف و توصیه‌های امنیتی است. برای مشاهده گزارش، می‌توانید فایل گزارش را که معمولاً در مسیر `/var/log/lynis.log` قرار دارد، بررسی کنید:

```
less /var/log/lynis.log
```

در این گزارش، به بخش‌هایی که مربوط به کرنل است توجه کنید و توصیه‌های ارائه شده را برای رفع آسیب‌پذیری‌ها دنبال کنید.

نتیجه‌گیری

سخت‌کردن کرنل لینوکس و اسکن منظم آسیب‌پذیری‌های آن از جمله مهم‌ترین اقدامات برای افزایش امنیت سیستم‌های لینوکسی است. با استفاده از ابزارهایی مانند Lynis، می‌توان به‌طور مؤثر آسیب‌پذیری‌های کرنل را شناسایی و رفع کرد. این مقاله راهنمایی جامع برای شروع کار با اسکن آسیب‌پذیری‌های کرنل ارائه می‌دهد.

منابع و ارجاعات

- <https://linuxsecurity.expert/security-tools/linux-vulnerability-scanning-tools>
- <https://www.youtube.com/watch?v=gj25vE62aaE>
- <https://chatwith.tools/youtube-summarizer/secure-rhel-slay-vulnerabilities-like-a-pro-with-scapy>
- <https://manpages.ubuntu.com/manpages/oracular/en/man8/lynis.8.html>