|  |  |  |  |
| --- | --- | --- | --- |
| S05 T05 | | | Network Security |
| Network monitoring and intrusion detection systems | | |
| Securing network protocols (SSH) | | Caret Right with solid fill | یکی از بخش‌های اساسی در سخت‌کردن سرورهای لینوکس، نظارت بر شبکه و استفاده از سیستم‌های تشخیص نفوذ (IDS) است. این فرآیندها به مدیران سیستم کمک می‌کنند تا به طور فعال از حملات و نفوذهای احتمالی جلوگیری کنند و امنیت کلی شبکه را افزایش دهند. در این مقاله، به معرفی مفهوم نظارت بر شبکه و سیستم‌های تشخیص نفوذ، اهمیت آن‌ها و ابزارهای مرتبط با آن‌ها می‌پردازیم. |
| بعد از |
| IPv6 hardening | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **بله** | | پیاده سازی عملی: **خیر** |

## نظارت بر شبکه و سیستم‌های تشخیص نفوذ در لینوکس

یکی از بخش‌های اساسی در سخت‌کردن سرورهای لینوکس، نظارت بر شبکه و استفاده از سیستم‌های تشخیص نفوذ (IDS) است. این فرآیندها به مدیران سیستم کمک می‌کنند تا به طور فعال از حملات و نفوذهای احتمالی جلوگیری کنند و امنیت کلی شبکه را افزایش دهند. در این مقاله، به معرفی مفهوم نظارت بر شبکه و سیستم‌های تشخیص نفوذ، اهمیت آن‌ها و ابزارهای مرتبط با آن‌ها می‌پردازیم.

## نظارت بر شبکه چیست؟

نظارت بر شبکه فرآیندی است که در آن ترافیک شبکه به طور مستمر بررسی و تحلیل می‌شود تا هرگونه فعالیت مشکوک یا غیرمعمول شناسایی شود. این کار به مدیران سیستم اجازه می‌دهد تا به سرعت به تهدیدات و مشکلات پاسخ دهند و از بروز حملات جدی‌تر جلوگیری کنند.

## سیستم‌های تشخیص نفوذ (IDS) چیست؟

سیستم‌های تشخیص نفوذ (IDS) ابزارهایی هستند که ترافیک شبکه و فعالیت‌های سیستم را مانیتور کرده و تلاش می‌کنند تا نشانه‌های نفوذ یا حمله را شناسایی کنند. IDS‌ها می‌توانند به دو دسته اصلی تقسیم شوند:

1. **سیستم‌های تشخیص نفوذ شبکه (NIDS)**: این سیستم‌ها ترافیک شبکه را مانیتور می‌کنند و هرگونه فعالیت مشکوک یا غیرمجاز را شناسایی می‌کنند.
2. **سیستم‌های تشخیص نفوذ میزبان (HIDS)**: این سیستم‌ها فعالیت‌های داخلی سیستم را بررسی می‌کنند و تلاش می‌کنند تا نشانه‌های نفوذ یا سوءاستفاده را شناسایی کنند.

### اهمیت نظارت بر شبکه و IDS

* **شناسایی سریع تهدیدات**: با نظارت مستمر بر شبکه و استفاده از IDS، می‌توان تهدیدات را به سرعت شناسایی کرد و از بروز خسارات جدی‌تر جلوگیری کرد.
* **پاسخ سریع به حملات**: با داشتن اطلاعات دقیق و به‌روز از وضعیت شبکه، مدیران سیستم می‌توانند به سرعت به حملات پاسخ دهند و اقدامات لازم را انجام دهند.
* **افزایش امنیت شبکه**: نظارت بر شبکه و استفاده از IDS‌ها به مدیران سیستم کمک می‌کند تا از نفوذهای غیرمجاز جلوگیری کرده و امنیت کلی شبکه را افزایش دهند.

## ابزارها و برنامه‌های مفید برای نظارت بر شبکه و IDS

1. **Wireshark**:

Wireshark یکی از ابزارهای قدرتمند و پرکاربرد برای تحلیل ترافیک شبکه است. این ابزار به مدیران سیستم اجازه می‌دهد تا بسته‌های شبکه را به طور دقیق بررسی کرده و فعالیت‌های مشکوک را شناسایی کنند.

sudo apt-get install wireshark

1. **Snort**:

Snortیکی از مشهورترین ابزارهای NIDS است که برای شناسایی و جلوگیری از نفوذهای شبکه‌ای استفاده می‌شود. این ابزار می‌تواند ترافیک شبکه را تحلیل کرده و بر اساس قواعد تعریف شده، فعالیت‌های مشکوک را شناسایی کند.

sudo apt-get install snort

1. **Suricata**:

Suricataیک IDS/IPS (سیستم پیشگیری از نفوذ) قدرتمند و متن‌باز است که می‌تواند ترافیک شبکه را به صورت واقعی زمان (real-time) تحلیل کند و تهدیدات را شناسایی کند.

sudo apt-get install suricata

1. **Tripwire**:

Tripwireیک ابزار HIDS است که برای شناسایی تغییرات غیرمجاز در فایل‌های سیستم استفاده می‌شود. این ابزار به مدیران سیستم کمک می‌کند تا فعالیت‌های مشکوک را در سطح فایل‌ها و دایرکتوری‌ها شناسایی کنند.

sudo apt-get install tripwire

1. **OSSEC**:

OSSECیک سیستم HIDS قدرتمند و متن‌باز است که می‌تواند فعالیت‌های سیستم را مانیتور کرده و تهدیدات را شناسایی کند. این ابزار همچنین قابلیت‌های دیگری مانند مانیتورینگ لاگ‌ها و یکپارچگی فایل‌ها را ارائه می‌دهد.

sudo apt-get install ossec-hids

## نتیجه‌گیری

نظارت بر شبکه و استفاده از سیستم‌های تشخیص نفوذ (IDS) یکی از مهم‌ترین اقداماتی است که می‌تواند امنیت شبکه‌های لینوکسی را بهبود بخشد. با استفاده از ابزارهای مناسب و پیاده‌سازی روش‌های موثر، می‌توان تهدیدات را به سرعت شناسایی و از نفوذهای غیرمجاز جلوگیری کرد. آشنایی و استفاده صحیح از این ابزارها به مدیران سیستم کمک می‌کند تا امنیت شبکه‌های خود را به بهترین نحو ممکن تضمین کنند و از داده‌های حساس خود محافظت کنند.

Top of Form

Bottom of Form

## منابع و ارجاعات

* <https://roadmap.sh/linux>
* <https://roadmap.sh/r/general-linux-server-hardening>