



Network Security	S05 T05	
	Network monitoring and intrusion detection systems	
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.		Securing network protocols (SSH)
	بعد از	
		IPv6 hardening
	قبل از	
پیاده سازی عملی: خیر	پژوهشی: بله	راهنمای عملی: بله

## 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. IDS ها می‌توانند به دو دسته اصلی تقسیم شوند:

۱. **سیستم‌های تشخیص نفوذ شبکه (NIDS)** این سیستم‌ها ترافیک شبکه را مانیتور می‌کنند و هرگونه فعالیت مشکوک یا غیرمجاز را شناسایی می‌کنند.
۲. **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 IDS ها 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
```

### 2. Snort:

Snort یکی 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
```

### 3. Suricata:

Suricata یک 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
```

### 4. Tripwire:

Tripwire یک 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
```

## 5. OSSEC:

OSSEC یک سیستم HIDS قدرتمند و متن باز است که می تواند فعالیت های سیستم را مانیتور کرده و تهدیدات را شناسایی کند. این ابزار همچنین قابلیت های دیگری مانند مانیتورینگ لاگ ها و یکپارچگی فایل ها را ارائه می دهد.

```
sudo apt-get install ossec-hids
```

## نتیجه گیری

نظارت بر شبکه و استفاده از سیستم های تشخیص نفوذ (IDS) یکی از مهم ترین اقداماتی است که می تواند امنیت شبکه های لینوکسی را بهبود بخشد. با استفاده از ابزارهای مناسب و پیاده سازی روش های موثر، می توان تهدیدات را به سرعت شناسایی و از نفوذهای غیرمجاز جلوگیری کرد. آشنایی و استفاده صحیح از این ابزارها به مدیران سیستم کمک می کند تا امنیت شبکه های خود را به بهترین نحو ممکن تضمین کنند و از داده های حساس خود محافظت کنند.

## منابع و ارجاعات

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