|  |  |  |  |
| --- | --- | --- | --- |
| S05 T06 | | | Network Security |
| IPv6 hardening | | |
| Network monitoring and intrusion detection systems | | Caret Right with solid fill | یکی از جنبه‌های مهم در سخت‌کردن سرورهای لینوکس، افزایش امنیت پروتکل IPv6 است. با توجه به افزایش استفاده از IPv6 به دلیل محدودیت‌های IPv4، امن‌سازی این پروتکل اهمیت ویژه‌ای دارد. در این مقاله، به معرفی IPv6، اهمیت سخت‌کردن آن و ابزارها و روش‌های مرتبط با آن می‌پردازیم. |
| بعد از |
| --- | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **خیر** | | پیاده سازی عملی: **بله** |

## سخت‌کردن IPv6 در لینوکس

یکی از جنبه‌های مهم در سخت‌کردن سرورهای لینوکس، افزایش امنیت پروتکل IPv6 است. با توجه به افزایش استفاده از IPv6 به دلیل محدودیت‌های IPv4، امن‌سازی این پروتکل اهمیت ویژه‌ای دارد. در این مقاله، به معرفی IPv6، اهمیت سخت‌کردن آن و ابزارها و روش‌های مرتبط با آن می‌پردازیم.

## IPv6 چیست؟

IPv6 (Internet Protocol version 6) نسخه جدیدتر پروتکل اینترنت است که با هدف حل مشکلات و محدودیت‌های IPv4 طراحی شده است. IPv6 از فضای آدرس‌دهی بسیار بزرگتری نسبت به IPv4 برخوردار است و دارای ویژگی‌ها و بهبودهای امنیتی و کارایی بیشتری می‌باشد.

## اهمیت سخت‌کردن IPv6

با توجه به گستردگی فضای آدرس‌دهی و ویژگی‌های خاص IPv6، امن‌سازی آن از اهمیت ویژه‌ای برخوردار است. مهاجمان می‌توانند از نقاط ضعف موجود در پیکربندی‌های پیش‌فرض IPv6 بهره‌برداری کرده و به شبکه و سیستم‌های شما نفوذ کنند. بنابراین، سخت‌کردن IPv6 می‌تواند به کاهش سطح حملات و افزایش امنیت شبکه کمک کند.

## روش‌های سخت‌کردن IPv6

1. **غیرفعال کردن IPv6 در صورت عدم نیاز**: اگر نیازی به استفاده از IPv6 ندارید، بهتر است آن را غیرفعال کنید تا سطح حملات را کاهش دهید.

sudo sysctl -w net.ipv6.conf.all.disable\_ipv6=1

sudo sysctl -w net.ipv6.conf.default.disable\_ipv6=1

برای غیرفعال کردن دائمی، این خطوط را به فایل /etc/sysctl.conf اضافه کنید:

net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.default.disable\_ipv6 = 1

1. **استفاده از فایروال برای IPv6**: استفاده از فایروال می‌تواند به محدود کردن ترافیک IPv6 و جلوگیری از حملات کمک کند.
   * **iptables**:

sudo ip6tables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo ip6tables -A INPUT -j DROP

* + **nftables**:

sudo nft add table inet my\_filter

sudo nft add chain inet my\_filter input { type filter hook input priority 0 \; }

sudo nft add rule inet my\_filter input tcp dport 22 accept

sudo nft add rule inet my\_filter input drop

1. **پیکربندی امن برای شبکه‌های محلی (RA و DHCPv6)**: تنظیمات روتر تبلیغات (Router Advertisements) و DHCPv6 باید به درستی پیکربندی شوند تا از نفوذ و حملات جلوگیری شود.
   * غیرفعال کردن پذیرش RA در صورت عدم نیاز:

sudo sysctl -w net.ipv6.conf.all.accept\_ra=0

sudo sysctl -w net.ipv6.conf.default.accept\_ra=0

برای غیرفعال کردن دائمی، این خطوط را به فایل /etc/sysctl.conf اضافه کنید:

net.ipv6.conf.all.accept\_ra = 0

net.ipv6.conf.default.accept\_ra = 0

1. **استفاده از آدرس‌های خصوصی IPv6 (ULA)**: برای ارتباطات داخلی و خصوصی، استفاده از آدرس‌های ULA (Unique Local Address) به جای آدرس‌های عمومی می‌تواند به امنیت کمک کند.
2. **پیکربندی صحیح DNS برای IPv6**: اطمینان حاصل کنید که DNS سرورهای شما به درستی پیکربندی شده‌اند تا از نشت اطلاعات جلوگیری شود.

**ابزارها و برنامه‌های مفید برای سخت‌کردن IPv6**

1. **ip6tables**: ابزار فایروال برای مدیریت ترافیک IPv6.

sudo apt-get install iptables

1. **nftables**: ابزار پیشرفته‌تر و جدیدتر برای مدیریت فایروال در لینوکس که از IPv6 نیز پشتیبانی می‌کند.

sudo apt-get install nftables

1. **sysctl**: ابزار خط فرمان برای تنظیم پارامترهای کرنل، از جمله تنظیمات مرتبط با IPv6.

sudo sysctl -p

1. **radvd**: ابزار پیکربندی تبلیغات روتر (Router Advertisement) برای IPv6.

sudo apt-get install radvd

## نتیجه‌گیری

سخت‌کردن IPv6 یکی از اقدامات مهم در جهت افزایش امنیت شبکه‌های لینوکسی است. با انجام تنظیمات صحیح و استفاده از ابزارهای مناسب، می‌توان از نفوذهای غیرمجاز جلوگیری کرد و امنیت شبکه را بهبود بخشید. آشنایی و استفاده صحیح از این روش‌ها به مدیران سیستم کمک می‌کند تا از شبکه‌های خود به بهترین نحو ممکن محافظت کنند و از داده‌های حساس خود حفظ نمایند.

Top of Form

Bottom of Form

## منابع و ارجاعات

* <https://roadmap.sh/linux>
* <https://roadmap.sh/r/general-linux-server-hardening>
* <https://linux.die.net/man/5/sshd_config>