<table>
<tr><td rowspan="2">Network Security</td><td colspan="3">S05 T06</td></tr>
<tr><td colspan="3">IPv6 hardening</td></tr>
<tr><td rowspan="2">یکی از جنبه‌های مهم در سخت‌کردن سرورهای لینوکس، افزایش امنیت پروتکل IPv6 است. با توجه به افزایش استفاده از IPv6 به دلیل محدودیت‌هایIPv4 ، امن‌سازی این پروتکل اهمیت ویژه‌ای دارد. در این مقاله، به معرفی IPv6، اهمیت سخت‌کردن آن و ابزارها و روش‌های مرتبط با آن می‌پردازیم.</td><td>بعد از</td><td colspan="2">Network monitoring and intrusion detection systems</td></tr>
<tr><td>قبل از</td><td colspan="2">---</td></tr>
<tr><td>پیاده سازی عملی: بله</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

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 محدودیت‌هایIPv4 ، امن‌سازی این پروتکل اهمیت ویژه‌ای دارد. در این مقاله، به معرفیIPv6 ، اهمیت سخت‌کردن آن و ابزارها و روش‌های مرتبط با آن می‌پردازیم.

IPv6چیست؟

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 سخت‌کردنIPv6

با توجه به گستردگی فضای آدرس‌دهی و ویژگی‌های خاصIPv6 ، 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 سخت‌کردنIPv6

۱. **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
```

۲. **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
```

۳. **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
```

٤. **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.

٥. **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 سخت‌کردنIPv6

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

```
sudo apt-get install iptables
```

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

```
sudo apt-get install nftables
```

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

```
sudo sysctl -p
```

٤. **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.

منابع و ارجاعات

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