<table>
<tr><td rowspan="2">Network Security</td><td colspan="2">S05 T03</td></tr>
<tr><td colspan="2">Disabling unnecessary network services</td></tr>
<tr><td rowspan="2">یکی از اصول مهم در سخت‌کردن سرورهای لینوکس، غیرفعال کردن سرویس‌های شبکه غیرضروری است. این اقدام می‌تواند سطح حملات احتمالی را کاهش داده و امنیت کلی سیستم را بهبود بخشد. در این مقاله به اهمیت غیرفعال کردن سرویس‌های غیرضروری، روش‌های انجام آن و ابزارهای مرتبط می‌پردازیم.</td><td>بعد از</td><td>KnockD</td></tr>
<tr><td>قبل از</td><td>Securing network protocols (SSH)</td></tr>
<tr><td>پیاده سازی عملی: بله</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

غیرفعال کردن سرویس‌های شبکه غیرضروری در لینوکس

یکی از اصول مهم در سخت‌کردن سرورهای لینوکس، غیرفعال کردن سرویس‌های شبکه غیرضروری است. این اقدام می‌تواند سطح حملات احتمالی را کاهش داده و امنیت کلی سیستم را بهبود بخشد. در این مقاله به اهمیت غیرفعال کردن سرویس‌های غیرضروری، روش‌های انجام آن و ابزارهای مرتبط می‌پردازیم.

اهمیت غیرفعال کردن سرویس‌های غیرضروری

هر سرویس شبکه‌ای که بر روی یک سیستم فعال باشد، می‌تواند به عنوان یک نقطه ورود بالقوه برای مهاجمان عمل کند. سرویس‌های غیرضروری که به صورت پیش‌فرض فعال هستند، می‌توانند آسیب‌پذیری‌های امنیتی ایجاد کنند و به مهاجمان امکان دسترسی به سیستم را بدهند. با غیرفعال کردن این سرویس‌ها، می‌توان سطح حملات را کاهش داده و امنیت سیستم را افزایش داد.

روش‌های شناسایی و غیرفعال کردن سرویس‌های غیرضروری

۱. **شناسایی سرویس‌های فعال** :برای شناسایی سرویس‌های شبکه‌ای که در حال اجرا هستند، می‌توان از ابزارهای مختلفی استفاده کرد. یکی از این ابزارها netstatاست:

```
sudo netstat -tuln
```

این فرمان لیستی از سرویس‌های شبکه‌ای فعال و پورت‌هایی که در حال گوش دادن هستند را نمایش می‌دهد.

۲. **بررسی سرویس‌های فعال با ss:**

```
sudo ss -tuln
```

این ابزار مشابه netstatعمل می‌کند و اطلاعات دقیقی درباره اتصالات شبکه ارائه می‌دهد.

۳. **استفاده از systemctl**: برای مدیریت سرویس‌ها در سیستم‌عامل‌های مبتنی بر Systemd مانند اکثر توزیع‌های مدرن لینوکس، می‌توان از systemctl استفاده کرد.

- **لیست سرویس‌های فعال:**

```
sudo systemctl list-units --type=service
```

- **غیرفعال کردن یک سرویس:**

```
sudo systemctl disable service_name

sudo systemctl stop service_name
```

به جای service_name، نام سرویس مورد نظر را قرار دهید.

٤. **استفاده از chkconfig**: در سیستم‌های مبتنی بر SysVinit مانند برخی از توزیع‌های قدیمی‌تر لینوکس، می‌توان از chkconfig برای مدیریت سرویس‌ها استفاده کرد.

- **غیرفعال کردن یک سرویس:**

```
sudo chkconfig service_name off

sudo service service_name stop
```

٥. **بررسی و ویرایش اسکریپت‌های راه‌اندازی**: در برخی موارد، سرویس‌ها ممکن است از طریق اسکریپت‌های راه‌اندازی در دایرکتوری‌های /etc/rc.d/ یا /etc/init.d/ فعال شوند. بررسی و ویرایش این اسکریپت‌ها می‌تواند به غیرفعال کردن سرویس‌های غیرضروری کمک کند.

ابزارها و برنامه‌های مفید

برای مدیریت سرویس‌های شبکه‌ای و غیرفعال کردن سرویس‌های غیرضروری، ابزارها و برنامه‌های متعددی وجود دارد که به مدیران سیستم کمک می‌کند:

- **netstat**: ابزار خط فرمان برای نمایش اتصالات شبکه و پورت‌های در حال گوش دادن.
- **ss:** ابزار پیشرفته‌تر برای نمایش اطلاعات اتصالات شبکه.
- **systemctl:** ابزار مدیریتی برای سیستم‌های مبتنی بر.Systemd
- **chkconfig:** ابزار مدیریتی برای سیستم‌های مبتنی بر.SysVinit
- **nmap:** ابزار قدرتمند اسکن شبکه که می‌تواند برای شناسایی سرویس‌های فعال بر روی یک سیستم استفاده شود.

```
sudo nmap -sT -O localhost
```

نتیجه‌گیری

غیرفعال کردن سرویس‌های شبکه غیرضروری یکی از مهم‌ترین اقداماتی است که می‌تواند امنیت سیستم‌های لینوکسی را بهبود بخشد. با شناسایی و غیرفعال کردن این سرویس‌ها، می‌توان نقاط ضعف بالقوه را کاهش داده و سیستم را در برابر حملات مختلف مقاوم‌تر کرد. استفاده از ابزارهای مدیریتی مناسب و آشنایی با روش‌های مختلف غیرفعال کردن سرویس‌ها به مدیران سیستم کمک می‌کند تا امنیت شبکه‌ی خود را به بهترین نحو ممکن تضمین کنند.

منابع و ارجاعات

- https://roadmap.sh/linux
- https://roadmap.sh/r/general-linux-server-hardening
- https://youtu.be/0QgUPK24NNE?si=znhTupmVlKlirMcL&t=863