<table>
<tr><td rowspan="2">Linux Kernel Hardening</td><td colspan="3">S03 T02</td></tr>
<tr><td colspan="3">Kernel parameter tuning</td></tr>
<tr><td rowspan="3">بخش "Kernel parameter tuning" در زمینه امن‌سازی سرور لینوکسی به تنظیم و بهینه‌سازی پارامترهای کرنل لینوکس می‌پردازد. این تنظیمات به منظور افزایش امنیت، کارایی، و پایداری سیستم انجام می‌شوند. در این بخش، شما با تغییر مقادیر پیش‌فرض برخی پارامترهای کرنل می‌توانید رفتار سیستم را متناسب با نیازهای امنیتی و عملکردی خود تغییر دهید.</td><td>›
بعد از</td><td colspan="2">Kernel modules</td></tr>
<tr><td>‹
قبل از</td><td colspan="2">SELinux or AppArmor</td></tr>
<tr><td>پیاده سازی عملی: بله</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

تنظیم پارامترهای هسته (Kernel Parameter Tuning) در لینوکس

تنظیم پارامترهای هسته (Kernel Parameter Tuning) یکی از مباحث حیاتی در افزایش امنیت و بهبود عملکرد سیستم‌های لینوکسی است. با تنظیم مناسب این پارامترها، می‌توان از سیستم در برابر تهدیدات مختلف محافظت کرد و همچنین بهره‌وری آن را افزایش داد. در این مقاله به معرفی مفهوم تنظیم پارامترهای هسته، اهمیت آن و گام‌های عملی برای انجام این کار می‌پردازیم.

اهمیت تنظیم پارامترهای هسته

۱. **افزایش امنیت سیستم** :با تنظیم پارامترهای امنیتی هسته، می‌توان از نفوذهای غیرمجاز و حملات مختلف جلوگیری کرد.

۲. **بهبود عملکرد سیستم** :تنظیم پارامترهای هسته می‌تواند به بهینه‌سازی منابع سیستم کمک کرده و عملکرد کلی را بهبود بخشد.

۳. **پایداری بیشتر** :با تنظیم صحیح پارامترهای هسته، می‌توان از بروز خطاها و کرش‌های غیرمنتظره جلوگیری کرد.

گام‌های عملی تنظیم پارامترهای هسته

۱. **بررسی پارامترهای فعلی هسته** :برای مشاهده پارامترهای فعلی هسته می‌توانید از دستور sysctl -aاستفاده کنید.

```
sysctl -a
```

2. **ویرایش فایل /etc/sysctl.conf**:

پارامترهای هسته را می‌توان در فایل /etc/sysctl.conf تنظیم کرد. این فایل شامل تنظیمات دائمی هسته است که در هر بار راه‌اندازی سیستم اعمال می‌شود.

۳. **نمونه‌ای از تنظیمات امنیتی هسته** :برخی از پارامترهای امنیتی که می‌توانید در فایل /etc/sysctl.conf تنظیم کنید عبارتند از:

```
# جلوگیری از ارسال پاسخ به پینگ‌ها

net.ipv4.icmp_echo_ignore_all = 1

# جلوگیری از ارسال بسته‌های IP معیوب

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0


# جلوگیری از بازپخش بسته‌ها

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 1


# جلوگیری از فوروارد کردن بسته‌های IP

net.ipv4.ip_forward = 0


# جلوگیری از ارسال پاسخ به درخواست‌های بازپخش

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv4.conf.all.secure_redirects = 0

net.ipv4.conf.default.secure_redirects = 0
```

۴. **اعمال تغییرات** :پس از ویرایش فایل /etc/sysctl.conf، باید تغییرات را اعمال کنید تا پارامترهای جدید به هسته اعمال شوند.

```
sudo sysctl -p
```

۵. **تنظیم پارامترهای خاص برای شبکه** :به عنوان مثال، برای بهبود عملکرد شبکه می‌توان پارامترهای زیر را تنظیم کرد:

```
# افزایش حافظه بافر ارسال و دریافت

net.core.rmem_max = 16777216

net.core.wmem_max = 16777216

net.ipv4.tcp_rmem = 4096 87380 16777216

net.ipv4.tcp_wmem = 4096 65536 16777216



# افزایش تعداد اتصالات نیمه‌باز

net.core.somaxconn = 1024

net.ipv4.tcp_max_syn_backlog = 2048
```

۶. **تنظیم پارامترهای خاص برای امنیت** :برخی از تنظیمات امنیتی دیگر که می‌توانید اعمال کنید عبارتند از:

```
# جلوگیری از بارگذاری ماژول‌های کرنل غیرضروری

kernel.modules_disabled = 1



# جلوگیری از دسترسی به فایل‌های حافظه کرنل

kernel.kptr_restrict = 2

kernel.dmesg_restrict = 1



# محدود کردن دسترسی به پروسس‌ها

kernel.yama.ptrace_scope = 1
```

۷. **تست و بررسی تنظیمات** :پس از اعمال تغییرات، باید سیستم را برای اطمینان از عملکرد صحیح تنظیمات تست کنید. این کار شامل بررسی لاگ‌های سیستم و ارزیابی عملکرد کلی سیستم است.

نتیجه‌گیری

تنظیم پارامترهای هسته یکی از مراحل حیاتی در بهبود امنیت و عملکرد سیستم‌های لینوکسی است. با اعمال تنظیمات مناسب در فایل /etc/sysctl.conf و بررسی و تست دقیق تنظیمات، می‌توان از سیستم در برابر تهدیدات مختلف محافظت کرده و بهره‌وری آن را بهبود بخشید. آشنایی و پیاده‌سازی صحیح این تنظیمات به مدیران سیستم کمک می‌کند تا از پایداری و امنیت سرورهای خود اطمینان حاصل کنند.

منابع و ارجاعات

- https://roadmap.sh/r/general-linux-server-hardening
- https://roadmap.sh/linux
- https://www.youtube.com/watch?v=0QgUPK24NNE
- https://linuxacademy.ir/?p=11710