|  |  |  |  |
| --- | --- | --- | --- |
| S05 T02 | | | Network Security |
| KnockD | | |
| Host firewall (iptables, nftables) | | Caret Right with solid fill | یکی از روش‌های پیشرفته و موثر برای افزایش امنیت شبکه در سرورهای لینوکسی، استفاده از KnockD است. KnockD یک سرویس مخفی‌سازی پورت‌ها (Port Knocking) است که به مدیران سیستم اجازه می‌دهد تا با استفاده از توالی‌های مشخصی از درخواست‌ها، پورت‌های بسته را به‌صورت موقت باز کنند. |
| بعد از |
| Disabling unnecessary network services | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **خیر** | | پیاده سازی عملی: **بله** |

## معرفی KnockD و کاربرد آن در امنیت شبکه

یکی از روش‌های پیشرفته و موثر برای افزایش امنیت شبکه در سرورهای لینوکسی، استفاده از KnockD است. KnockD یک سرویس مخفی‌سازی پورت‌ها (Port Knocking) است که به مدیران سیستم اجازه می‌دهد تا با استفاده از توالی‌های مشخصی از درخواست‌ها، پورت‌های بسته را به‌صورت موقت باز کنند. این روش به‌ویژه برای مخفی‌سازی پورت‌های حساس مانند SSH بسیار مفید است. در این مقاله به معرفی KnockD، اهمیت آن و مراحل عملی پیاده‌سازی آن در لینوکس می‌پردازیم.

## اهمیت استفاده از KnockD

1. **افزایش امنیت**: با استفاده از KnockD، پورت‌های حساس سیستم شما به‌صورت پیش‌فرض بسته هستند و تنها در صورت دریافت توالی خاصی از درخواست‌ها باز می‌شوند، که این امر امنیت سیستم را افزایش می‌دهد.
2. **مخفی‌سازی پورت‌ها:** KnockD به مخفی‌سازی پورت‌های باز کمک می‌کند و از شناسایی آن‌ها توسط اسکنرهای شبکه جلوگیری می‌کند.
3. **کنترل دسترسی**: با استفاده از KnockD، می‌توانید دسترسی به پورت‌های خاص را تنها به کاربران مجاز محدود کنید.

## مراحل عملی پیاده‌سازی KnockD

1. **نصب :KnockD** ابتدا باید KnockD را نصب کنید. در توزیع‌های مبتنی بر Debian و Ubuntu، می‌توانید از دستور زیر استفاده کنید:

sudo apt-get install knockd

1. **پیکربندی :KnockD** پس از نصب، فایل پیکربندی KnockD را ویرایش کنید. این فایل معمولاً در مسیر /etc/knockd.conf قرار دارد.

sudo nano /etc/knockd.conf

در این فایل، می‌توانید توالی پورت‌های مورد نظر و اقداماتی که باید پس از دریافت توالی انجام شود را تعریف کنید. به عنوان مثال:

[options]

UseSyslog

[openSSH]

sequence = 7000,8000,9000

seq\_timeout = 15

command = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

tcpflags = syn

[closeSSH]

sequence = 9000,8000,7000

seq\_timeout = 15

command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

tcpflags = syn

1. **فعال‌سازی و راه‌اندازی سرویس :KnockD** پس از پیکربندی، سرویس KnockD را فعال و راه‌اندازی کنید:

sudo systemctl enable knockd

sudo systemctl start knockd

1. **ارسال توالی پورت‌ها برای باز کردن پورت :SSH** برای باز کردن پورت SSH، از یک سیستم دیگر، می‌توانید از ابزار knock استفاده کنید:

knock your\_server\_ip 7000 8000 9000

پس از ارسال توالی، پورت SSH برای IP شما باز می‌شود و می‌توانید به سرور متصل شوید:

ssh your\_user@your\_server\_ip

1. **بستن پورت SSH با ارسال توالی معکوس**: برای بستن پورت SSH پس از اتمام کار، توالی معکوس را ارسال کنید:

knock your\_server\_ip 9000 8000 7000

## نتیجه‌گیری

استفاده از KnockD یکی از روش‌های موثر برای افزایش امنیت شبکه در سرورهای لینوکسی است. با مخفی‌سازی و کنترل دسترسی به پورت‌های حساس، می‌توان از نفوذهای غیرمجاز جلوگیری کرد و امنیت کلی سیستم را بهبود بخشید. آشنایی و پیاده‌سازی صحیح این ابزار به مدیران سیستم کمک می‌کند تا از داده‌های حساس خود محافظت کرده و از عملکرد بهینه سرورهای خود اطمینان حاصل کنند.

## منابع و ارجاعات

* <https://roadmap.sh/linux>
* <https://roadmap.sh/r/general-linux-server-hardening>
* <https://youtube.com/watch?v=WhPHKvNUpAw>