<table>
<tr><td rowspan="2">Network Security</td><td colspan="2">S05 T02</td></tr>
<tr><td colspan="2">KnockD</td></tr>
<tr><td rowspan="2">یکی از روش‌های پیشرفته و موثر برای افزایش امنیت شبکه در سرورهای لینوکسی، استفاده از KnockD است . KnockDیک 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.</td><td>بعد از</td><td>Host firewall (iptables, nftables)</td></tr>
<tr><td>قبل از</td><td>Disabling unnecessary network services</td></tr>
<tr><td>پیاده سازی عملی: بله</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

معرفی KnockD و کاربرد آن در امنیت شبکه

یکی از روش‌های پیشرفته و موثر برای افزایش امنیت شبکه در سرورهای لینوکسی، استفاده از KnockDاست 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 معرفیKnockD ، اهمیت آن و مراحل عملی پیاده‌سازی آن در لینوکس می‌پردازیم.

اهمیت استفاده ازKnockD

۱. **افزایش امنیت** :با استفاده ازKnockD ، 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.

۲. **مخفی‌سازی پورت‌ها:** KnockD به مخفی‌سازی پورت‌های باز کمک می‌کند و از شناسایی آن‌ها توسط اسکنرهای شبکه جلوگیری می‌کند.

۳. **کنترل دسترسی** :با استفاده ازKnockD ، می‌توانید دسترسی به پورت‌های خاص را تنها به کاربران مجاز محدود کنید.

مراحل عملی پیاده‌سازیKnockD

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

```
sudo apt-get install knockd
```

۲. **پیکربندی KnockD:** پس از نصب، فایل پیکربندی KnockD را ویرایش کنید. این فایل معمولاً در مسیر /etc/knockd.confقرار 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
```

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

```
sudo systemctl enable knockd

sudo systemctl start knockd
```

٤. **ارسال توالی پورت‌ها برای باز کردن پورت SSH:** برای باز کردن پورتSSH ، 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
```

٥. **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