



Network Security	S05 T01	
	Host firewall (iptables, nftables)	
یکی از جنبه‌های مهم در سخت‌کردن سرورهای لینوکس، امنیت شبکه است. دیوار آتش میزبان (Host Firewall) ابزاری قدرتمند برای مدیریت ترافیک ورودی و خروجی در سیستم‌های لینوکس است. دو ابزار اصلی برای این منظور iptables و nftables هستند که هر کدام ویژگی‌ها و قابلیت‌های منحصر به فرد خود را دارند.		---
	بعد از	
		KnockD
	قبل از	
پیاده سازی عملی: بله	پژوهشی: خیر	راهنمای عملی: بله

دیوار آتش میزبان (iptables, nftables) در لینوکس

یکی از جنبه‌های مهم در سخت‌کردن سرورهای لینوکس، امنیت شبکه است. دیوار آتش میزبان (Host Firewall) ابزاری قدرتمند برای مدیریت ترافیک ورودی و خروجی در سیستم‌های لینوکس است. دو ابزار اصلی برای این منظور iptables و nftables هستند که هر کدام ویژگی‌ها و قابلیت‌های منحصر به فرد خود را دارند.

معرفی iptables

iptables یکی از پرکاربردترین ابزارهای فیلترینگ بسته‌های شبکه در لینوکس است. این ابزار امکان کنترل دقیق ترافیک ورودی، خروجی و عبوری از سیستم را فراهم می‌کند. با استفاده از جداول و زنجیره‌ها (chains) برای تعریف قوانین فیلترینگ کار می‌کند.

ویژگی‌های iptables

- قابلیت پیکربندی بالا: امکان تعریف قوانین پیچیده برای مدیریت ترافیک شبکه
- پشتیبانی گسترده: مورد استفاده در بسیاری از توزیع‌های لینوکسی و پشتیبانی شده توسط جامعه‌ی بزرگ کاربران
- سازگاری با ماژول‌ها: قابلیت افزودن ماژول‌های مختلف برای افزایش عملکرد و قابلیت‌ها

نحوه استفاده از iptables

برای کار با iptables می‌توان از فرمان‌های زیر استفاده کرد:

- افزودن قانون جدید:

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

- حذف قانون:

```
sudo iptables -D INPUT -p tcp --dport 22 -j ACCEPT
```

- مشاهده قوانین فعلی:

```
sudo iptables -L
```

معرفی nftables

nftables ابزار جدیدتر و پیشرفته‌تری برای فیلترینگ بسته‌های شبکه در لینوکس است که به عنوان جایگزینی برای iptables معرفی شده است. nftables با هدف ساده‌تر کردن مدیریت دیوار آتش و افزایش عملکرد طراحی شده است.

ویژگی‌های nftables

- **سادگی و کارایی:** قوانین و جداول به صورت ساده‌تری مدیریت می‌شوند
- **عملکرد بهتر:** بهینه‌سازی‌های بیشتر در عملکرد نسبت به iptables
- **پشتیبانی از ساختارهای داده پیچیده‌تر:** امکان تعریف جداول و زنجیره‌های پیچیده‌تر و منعطف‌تر

نحوه استفاده از nftables

برای کار با nftables می‌توان از فرمان‌های زیر استفاده کرد:

- افزودن قانون جدید:

```
sudo nft add rule inet filter input tcp dport 22 accept
```

- حذف قانون:

```
sudo nft delete rule inet filter input handle <handle_number>
```

- مشاهده قوانین فعلی:

```
sudo nft list ruleset
```

ابزارها و برنامه‌های مفید

برای مدیریت و پیکربندی دیوار آتش میزبان، ابزارها و برنامه‌های متعددی وجود دارد که به مدیران سیستم کمک می‌کند:

- **ufw (Uncomplicated Firewall):**

یک ابزار ساده و کاربرپسند برای مدیریت iptables که در توزیع‌هایی مانند Ubuntu بسیار پرکاربرد است.

```
sudo ufw enable
```

```
sudo ufw allow 22/tcp
```

- **firewalld:**

یک ابزار مدیریتی برای iptables و nftables که با استفاده از مناطق (zones) و سرویس‌ها (services) مدیریت دیوار آتش را ساده‌تر می‌کند.

```
sudo firewall-cmd --add-service=ssh --permanent
```

```
sudo firewall-cmd -reload
```

نتیجه‌گیری

استفاده از دیوار آتش میزبان (iptables) و (nftables) یکی از مهم‌ترین اقدامات برای افزایش امنیت شبکه در سیستم‌های لینوکس است. با پیکربندی صحیح و مدیریت مناسب دیوار آتش، می‌توان ترافیک ورودی و خروجی را کنترل و از دسترسی‌های غیرمجاز جلوگیری کرد. آشنایی و استفاده صحیح از این ابزارها به مدیران سیستم کمک می‌کند تا امنیت شبکه‌ی خود را بهبود بخشند و از سیستم‌های خود به بهترین نحو ممکن محافظت کنند.

منابع و ارجاعات

- <https://roadmap.sh/linux>
- <https://manpages.ubuntu.com/manpages/noble/en/man8/iptables.8.html>
- <https://wiki.archlinux.org/title/nftables>
- <https://www.youtube.com/watch?v=JMHD04X7v1s>
- <https://linuxacademy.ir/ip-tables/>