|  |  |  |  |
| --- | --- | --- | --- |
| S05 T04 | | | Network Security |
| Securing network protocols (SSH) | | |
| Disabling unnecessary network services | | Caret Right with solid fill | یکی از جنبه‌های مهم در سخت‌کردن سرورهای لینوکس، امن‌سازی پروتکل‌های شبکه است. پروتکل SSH (Secure Shell) یکی از مهم‌ترین و پرکاربردترین پروتکل‌ها برای دسترسی امن به سرورها و مدیریت آن‌ها از راه دور است. در این مقاله به معرفی SSH، اهمیت امن‌سازی آن و ابزارها و تنظیمات مرتبط برای افزایش امنیت آن می‌پردازیم. |
| بعد از |
| Network monitoring and intrusion detection systems | | Caret Left with solid fill |
| قبل از |
| راهنمای عملی: بله | پژوهشی: **خیر** | | پیاده سازی عملی: **بله** |

## امن‌سازی پروتکل‌های شبکه (SSH) در لینوکس

یکی از جنبه‌های مهم در سخت‌کردن سرورهای لینوکس، امن‌سازی پروتکل‌های شبکه است. پروتکل SSH (Secure Shell) یکی از مهم‌ترین و پرکاربردترین پروتکل‌ها برای دسترسی امن به سرورها و مدیریت آن‌ها از راه دور است. در این مقاله به معرفی SSH، اهمیت امن‌سازی آن و ابزارها و تنظیمات مرتبط برای افزایش امنیت آن می‌پردازیم.

## SSH چیست؟

SSH یا Secure Shell یک پروتکل شبکه‌ای است که برای دسترسی امن به سرورها و دستگاه‌های شبکه‌ای از طریق یک کانال رمزگذاری شده استفاده می‌شود. SSH به کاربران این امکان را می‌دهد تا به صورت ایمن وارد سیستم شوند، دستورات را اجرا کنند و فایل‌ها را منتقل نمایند. این پروتکل جایگزین امنی برای پروتکل‌های قدیمی‌تری مانند Telnet است که به صورت متن‌واضح (Plaintext) داده‌ها را منتقل می‌کردند.

## اهمیت امن‌سازی SSH

با توجه به اهمیت و کاربرد گسترده SSH در مدیریت سرورها، امن‌سازی این پروتکل از اهمیت ویژه‌ای برخوردار است. حملات بر روی سرویس SSH، مانند حملات Brute Force و تلاش‌های متعدد برای دسترسی غیرمجاز، می‌توانند منجر به نفوذ و دسترسی غیرمجاز به سیستم شوند. بنابراین، باید اقداماتی برای افزایش امنیت SSH انجام شود.

## روش‌های امن‌سازی SSH

1. **تغییر پورت پیش‌فرض SSH**

پورت پیش‌فرض SSH، پورت 22 است. تغییر این پورت به یک پورت غیرمتداول می‌تواند تا حدودی از حملات خودکار جلوگیری کند.

sudo vi /etc/ssh/sshd\_config

مقدار Port را به پورت دلخواه خود تغییر دهید و سپس سرویس SSH را مجدداً راه‌اندازی کنید:

sudo systemctl restart sshd

1. **غیرفعال کردن ورود با کاربر root**

ورود مستقیم به عنوان کاربر root می‌تواند خطرناک باشد. بهتر است این دسترسی غیرفعال شود و کاربران از طریق یک حساب کاربری معمولی وارد شوند و سپس با استفاده از sudo دسترسی root را بدست آورند.

sudo vi /etc/ssh/sshd\_config

مقدار PermitRootLogin را به no تغییر دهید:

PermitRootLogin no

سپس سرویس SSH را مجدداً راه‌اندازی کنید:

sudo systemctl restart sshd

1. **استفاده از کلیدهای SSH به جای کلمه‌عبور**: استفاده از کلیدهای عمومی و خصوصی SSH به جای کلمه‌عبور می‌تواند امنیت را به میزان قابل توجهی افزایش دهد. کلید عمومی بر روی سرور قرار می‌گیرد و کلید خصوصی در سیستم کاربر ذخیره می‌شود.

ssh-keygen -t rsa -b 4096

ssh-copy-id user@server

سپس ورود با کلمه‌عبور را غیرفعال کنید:

sudo vi /etc/ssh/sshd\_config

مقدار PasswordAuthentication را به no تغییر دهید:

PasswordAuthentication no

سرویس SSH را مجدداً راه‌اندازی کنید:

sudo systemctl restart sshd

1. **محدود کردن دسترسی با استفاده از AllowUsers و AllowGroups**:

می‌توان دسترسی به سرویس SSH را برای کاربران و گروه‌های خاص محدود کرد.

sudo vi /etc/ssh/sshd\_config

کاربران و گروه‌های مجاز را اضافه کنید:

AllowUsers user1 user2

AllowGroups group1 group2

سرویس SSH را مجدداً راه‌اندازی کنید:

sudo systemctl restart sshd

1. **استفاده از فایروال**: استفاده از فایروال برای محدود کردن دسترسی به پورت SSH نیز می‌تواند کمک کننده باشد. به عنوان مثال، با استفاده از iptables یا ufw می‌توان دسترسی به پورت SSH را فقط برای آدرس‌های IP خاص مجاز کرد.

sudo ufw allow from 192.168.1.0/24 to any port 22

sudo ufw enable

1. **فعال‌سازی احراز هویت دو مرحله‌ای (2FA)**

استفاده از احراز هویت دو مرحله‌ای یک لایه امنیتی اضافی است که از کدهای موقتی یا پیامک برای تأیید هویت کاربر استفاده می‌کند.

sudo apt-get install libpam-google-authenticator

سپس دستور زیر را برای پیکربندی Google Authenticator اجرا کنید:

google-authenticator

## ابزارها و برنامه‌های مفید

* **fail2ban:**

ابزاری برای جلوگیری از حملات Brute Force بر روی سرویس SSH. این ابزار با مانیتورینگ لاگ‌های سرویس SSH، تلاش‌های ناموفق متعدد را شناسایی کرده و آدرس‌های IP مهاجم را به صورت موقت مسدود می‌کند.

sudo apt-get install fail2ban

sudo systemctl enable fail2ban

sudo systemctl start fail2ban

* **sshguard:**

ابزاری مشابه fail2ban که برای محافظت از سرویس SSH در برابر حملات استفاده می‌شود.

sudo apt-get install sshguard

sudo systemctl enable sshguard

sudo systemctl start sshguard

**نتیجه‌گیری**

امن‌سازی پروتکل SSH یکی از مهم‌ترین اقدامات در جهت افزایش امنیت شبکه در سیستم‌های لینوکسی است. با انجام تنظیمات مناسب و استفاده از ابزارهای امنیتی می‌توان از دسترسی‌های غیرمجاز جلوگیری کرده و سیستم را در برابر حملات مختلف محافظت کرد. آشنایی و استفاده صحیح از این روش‌ها به مدیران سیستم کمک می‌کند تا امنیت سرورهای خود را بهبود بخشند و از داده‌های حساس خود به بهترین نحو ممکن محافظت کنند.

Top of Form

Bottom of Form

## منابع و ارجاعات

* <https://roadmap.sh/linux>
* <https://roadmap.sh/r/general-linux-server-hardening>
* <https://hiddify.com/fa/manager/basic-concepts-and-troubleshooting/How-to-change-SSH-port-on-your-server/>
* <https://hiddify.com/fa/manager/basic-concepts-and-troubleshooting/Disable-SSH-Password-Authentication/>
* <https://xaas.ir/blog/fail2ban-2/>
* <https://youtu.be/0QgUPK24NNE?si=4_lTRANTnvOcLIAf&t=909>