



Network Security	S05 T04	
	Securing network protocols (SSH)	
<p>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.</p>		Disabling unnecessary network services
	بعد از	
		Network monitoring and intrusion detection systems
	قبل از	
پیاده سازی عملی: بله	پژوهشی: خیر	راهنمای عملی: بله

امن سازی پروتکل های شبکه (SSH) در لینوکس

یکی از جنبه های مهم در سخت کردن سرورهای لینوکس، امن سازی پروتکل های شبکه است. پروتکل SSH (Secure Shell) یکی از مهم ترین و پرکاربردترین پروتکل ها برای دسترسی امن به سرورها و مدیریت آن ها از راه دور است. در این مقاله به معرفی SSH، اهمیت امن سازی آن و ابزارها و تنظیمات مرتبط برای افزایش امنیت آن می پردازیم.

SSH چیست؟

SSH یا Secure Shell یک پروتکل شبکه ای است که برای دسترسی امن به سرورها و دستگاه های شبکه ای از طریق یک کانال رمزگذاری شده استفاده می شود. به کاربران این امکان را می دهد تا به صورت ایمن وارد سیستم شوند، دستورات را اجرا کنند و فایل ها را منتقل نمایند. این پروتکل جایگزین امنی برای پروتکل های قدیمی تری مانند Telnet است که به صورت متن واضح (Plaintext) داده ها را منتقل می کردند.

اهمیت امن سازی SSH

با توجه به اهمیت و کاربرد گسترده SSH در مدیریت سرورها، امن سازی این پروتکل از اهمیت ویژه ای برخوردار است. حملات بر روی سرویس SSH، مانند حملات Brute Force و تلاش های متعدد برای دسترسی غیرمجاز، می توانند منجر به نفوذ و دسترسی غیرمجاز به سیستم شوند. بنابراین، باید اقداماتی برای افزایش امنیت SSH انجام شود.

روش‌های امن‌سازی SSH

۱. تغییر پورت پیش‌فرض SSH

پورت پیش‌فرض SSH ، پورت ۲۲ 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
```

۲. 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
```

۳. استفاده از کلیدهای SSH به جای کلمه عبور: استفاده از کلیدهای عمومی و خصوصی SSH به جای کلمه عبور 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 کلمه عبور 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
```

۴. 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
```

۵. **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
```

۶. 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.

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_lTRANtvOcLIAf&t=909

