<table>
<tr><td rowspan="2">Secure Remote Administration</td><td colspan="3">S06 T01</td></tr>
<tr><td colspan="3">Public key authentication</td></tr>
<tr><td rowspan="3">یکی از مهم‌ترین موضوعات در زمینه مدیریت ایمن راه دور (Secure Remote Administration)در سرورهای لینوکس، استفاده از احراز هویت با کلید عمومی است. این روش به طور قابل توجهی امنیت اتصالات SSH را افزایش می‌دهد و از حملات متداولی مانند حملات Brute Forceجلوگیری می‌کند. در این مقاله به معرفی احراز هویت با کلید عمومی، مزایای آن و روش پیاده‌سازی آن می‌پردازیم.</td><td>›
بعد از</td><td>---</td><td></td></tr>
<tr><td>‹
قبل از</td><td>Two-factor authentication</td><td></td></tr>
<tr><td colspan="2">پیاده سازی عملی: بله</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

احراز هویت با کلید عمومی در لینوکس

یکی از مهم‌ترین موضوعات در زمینه مدیریت ایمن راه دور (Secure Remote Administration) در سرورهای لینوکس، استفاده از احراز هویت با کلید عمومی است. این روش به طور قابل توجهی امنیت اتصالات SSH را افزایش می‌دهد و از حملات متداولی مانند حملات Brute Force جلوگیری می‌کند. در این مقاله به معرفی احراز هویت با کلید عمومی، مزایای آن و روش پیاده‌سازی آن می‌پردازیم.

احراز هویت با کلید عمومی چیست؟

احراز هویت با کلید عمومی (Public Key Authentication) روشی برای تأیید هویت کاربران است که از یک جفت کلید عمومی و خصوصی استفاده می‌کند. کلید عمومی بر روی سرور ذخیره می‌شود و کلید خصوصی در اختیار کاربر قرار دارد. هنگامی که کاربر تلاش می‌کند به سرور متصل شود، سرور از کلید عمومی برای تأیید کلید خصوصی کاربر استفاده می‌کند.

مزایای احراز هویت با کلید عمومی

۱. **امنیت بیشتر** :این روش بسیار امن‌تر از استفاده از کلمه‌عبور است، زیرا کلیدهای خصوصی به راحتی قابل حدس زدن یا شکستن نیستند.

۲. **جلوگیری از حملات Brute Force**: با استفاده از کلیدهای عمومی و خصوصی، حملات Brute Forceبه کلمه‌عبور بی‌اثر می‌شوند.

۳. **راحتی در استفاده** :کاربران می‌توانند بدون نیاز به وارد کردن کلمه‌عبور، به سرورها متصل شوند، که این کار را برای اتصال‌های مکرر راحت‌تر می‌کند.

نحوه پیاده‌سازی احراز هویت با کلید عمومی

۱. تولید جفت کلید

برای تولید یک جفت کلید عمومی و خصوصی، از ابزار ssh-keygenاستفاده می‌شود:

```
ssh-keygen -t rsa -b 4096 -C your_email@example.com
```

این فرمان یک جفت کلید RSA با طول ٤٠٩٦ بیت ایجاد می‌کند. پس از اجرای فرمان، شما می‌توانید مسیر ذخیره‌سازی کلیدها را مشخص کنید (به طور پیش‌فرض در ~/.ssh/id_rsa).

۲. کپی کردن کلید عمومی به سرور

برای کپی کردن کلید عمومی به سرور، از ابزار ssh-copy-idاستفاده کنید:

```
ssh-copy-id user@server
```

این فرمان کلید عمومی شما را به فایل ssh/authorized_keys/.~در سرور اضافه می‌کند.

۳. تنظیمات سرورSSH

برای اطمینان از اینکه سرور SSH احراز هویت با کلید عمومی را قبول می‌کند، فایل پیکربندی SSH را بررسی و ویرایش کنید:

```
sudo vi /etc/ssh/sshd_config
```

مقادیر زیر را در این فایل تنظیم کنید:

```
PubkeyAuthentication yes

PasswordAuthentication no
```

پس از اعمال تغییرات، سرویس SSH را مجدداً راه‌اندازی کنید:

```
sudo systemctl restart sshd
```

ابزارها و برنامه‌های مفید

۱. **ssh-keygen**: ابزاری برای تولید جفت کلیدهای SSH.

```
ssh-keygen
```

۲. **ssh-copy-id**: ابزاری برای کپی کردن کلید عمومی به سرور.

```
ssh-copy-id user@server
```

۳. **sshd**: سرویس SSH که برای مدیریت اتصالات SSH استفاده می‌شود.

٤. **puttygen**: ابزاری برای تولید کلیدهای SSH در سیستم‌های ویندوز. این ابزار بخشی از مجموعه Putty است.

نتیجه‌گیری

استفاده از احراز هویت با کلید عمومی یکی از بهترین روش‌ها برای افزایش امنیت اتصالات SSH در سرورهای لینوکس است. با پیاده‌سازی این روش، می‌توان از حملات متداول جلوگیری کرد و امنیت سیستم را به طور قابل توجهی افزایش داد. آشنایی و استفاده صحیح از ابزارهای مربوط به احراز هویت با کلید عمومی به مدیران سیستم کمک می‌کند تا امنیت دسترسی‌های راه دور خود را بهبود بخشند و از داده‌های حساس خود 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/Disable-SSH-Password-Authentication/
- https://youtu.be/vu53J6wyOII?si=wItecyM7gHmZhaCi&t=758
- https://youtu.be/qfARNLChgpE?si=m3ZoXVs2KRfiwFNf
- https://youtu.be/YYm3U8hnszo?si=DmK7ZMUorAaaRbaa