<table>
<tr><td rowspan="2">Secure Remote Administration</td><td colspan="3">S06 T02</td></tr>
<tr><td colspan="3">Two-factor authentication</td></tr>
<tr><td rowspan="2">یکی از مهم‌ترین جنبه‌های مدیریت ایمن راه دور (Secure Remote Administration)در سرورهای لینوکس، استفاده از احراز هویت دو مرحله‌ای (Two-Factor Authentication)است. این روش امنیت اتصالات SSH را به طور قابل توجهی افزایش می‌دهد و از نفوذهای غیرمجاز جلوگیری می‌کند. در این مقاله به معرفی احراز هویت دو مرحله‌ای، مزایای آن و نحوه پیاده‌سازی آن در لینوکس می‌پردازیم.</td><td>بعد از</td><td colspan="2">Public key authentication</td></tr>
<tr><td>قبل از</td><td colspan="2">Fail2ban</td></tr>
<tr><td>پیاده سازی عملی: بله</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

احراز هویت دو مرحله‌ای در لینوکس

یکی از مهم‌ترین جنبه‌های مدیریت ایمن راه دور (Secure Remote Administration) در سرورهای لینوکس، استفاده از احراز هویت دو مرحله‌ای (Two-Factor Authentication) یا ۲FA است. این روش امنیت اتصالات SSH را به طور قابل توجهی افزایش می‌دهد و از نفوذهای غیرمجاز جلوگیری می‌کند. در این مقاله به معرفی احراز هویت دو مرحله‌ای، مزایای آن و نحوه پیاده‌سازی آن در لینوکس می‌پردازیم.

احراز هویت دو مرحله‌ای چیست؟

احراز هویت دو مرحله‌ای (2FA) یک لایه امنیتی اضافی است که علاوه بر کلمه‌عبور، نیاز به یک عامل دیگر برای تأیید هویت کاربر دارد. این عامل دوم می‌تواند یک کد موقتی باشد که از طریق یک نرم‌افزار احراز هویت تولید می‌شود. با این روش، حتی اگر کلمه‌عبور کاربر به دست مهاجم بیفتد، دسترسی به سیستم بدون عامل دوم امکان‌پذیر نخواهد بود.

مزایای احراز هویت دو مرحله‌ای

۱. **افزایش امنیت** :با افزودن یک لایه امنیتی اضافی، احتمال نفوذ غیرمجاز به سیستم کاهش می‌یابد.

۲. **محافظت در برابر حملات فیشینگ و Brute Force:** حتی اگر کلمه‌عبور کاربر به سرقت برود، مهاجم بدون کد موقتی نمی‌تواند به سیستم دسترسی پیدا کند.

۳. **سهولت در پیاده‌سازی** :ابزارها و نرم‌افزارهای مختلفی برای پیاده‌سازی ۲FA در لینوکس وجود دارد که کار را برای مدیران سیستم ساده می‌کند.

ابزارها و برنامه‌های مفید

1. **Google Authenticator**:

ابزاری برای تولید کدهای موقتی جهت احراز هویت دو مرحله‌ای.

2. **FreeOTP**:

یک نرم‌افزار منبع‌باز برای تولید کدهای موقتی که به عنوان جایگزینی برای Google Authenticator می‌تواند استفاده شود.

3. **Duo Security**:

سرویس احراز هویت دو مرحله‌ای پیشرفته که امکانات بیشتری مانند ارسال کدهای موقتی از طریق پیامک یا تماس تلفنی ارائه می‌دهد.

نتیجه‌گیری

احراز هویت دو مرحله‌ای یکی از موثرترین روش‌ها برای افزایش امنیت اتصـــالات SSH و جلوگیری از نفوذهای غیرمجاز به سـرورهای لینوکس اسـت. با پیاده‌سـازی این روش و اسـتفاده از ابزارهای مناسـب، می‌توان به طور قابل توجهی امنیت سـیسـتم را بهبود بخشـید و از داده‌های حسـاس خود محافظت کرد. آشنایی و استفاده صحیح از احراز هویت دو مرحله‌ای به مدیران سیستم کمک می‌کند تا به بهترین نحو ممکن امنیت دسترسی‌های راه دور خود را تضمین کنند.

منابع و ارجاعات

- https://roadmap.sh/linux
- https://roadmap.sh/r/general-linux-server-hardening
- https://youtu.be/wrx2cm3qDNI?si=n8PWX1aRjuG6peVc
- https://youtu.be/vOy46lGBZoQ?si=KuuJHpQL563z93n4
- https://youtu.be/z34VFH91Gd0?si=lBE4A3FJr1z-Wu3x
- https://github.com/google/google-authenticator-libpam

- https://youtu.be/f-lw-w3cXeA?si=8aQ5Gyo9kqLOFUvW