<table>
<tr><td rowspan="2">Secure Remote Administration</td><td colspan="3">S06 T03</td></tr>
<tr><td colspan="3">Fail2ban</td></tr>
<tr><td rowspan="2">یکی از ابزارهای موثر برای افزایش امنیت سرورهای لینوکسی و جلوگیری از حملات مخرب مانند حملات Brute Force، استفاده از Fail2ban است Fail2ban .یک نرم‌افزار امنیتی است که لاگ‌های سیستم را مانیتور می‌کند و در صورت شناسایی تلاش‌های ناموفق متعدد برای ورود به سیستم، آدرس‌های IP مشکوک را به طور موقت مسدود می‌کند.</td><td> 
بعد از</td><td colspan="2">Two-factor authentication</td></tr>
<tr><td> 
قبل از</td><td colspan="2">Damaging consequences of insecure remote administration</td></tr>
<tr><td>پیاده سازی عملی: بله</td><td>پژوهشی: خیر</td><td>راهنمای عملی: بله</td></tr>
</table>

معرفی Fail2ban و کاربرد آن در مدیریت ایمن راه دور

یکی از ابزارهای موثر برای افزایش امنیت سرورهای لینوکسی و جلوگیری از حملات مخرب مانند حملات Brute Force، استفاده از Fail2ban است Fail2ban .یک نرم‌افزار امنیتی است که لاگ‌های سیستم را مانیتور می‌کند و در صورت شناسایی تلاش‌های ناموفق متعدد برای ورود به سیستم، آدرس‌های IP مشکوک را به طور موقت مسدود می‌کند. در این مقاله به معرفیFail2ban ، اهمیت آن و مراحل عملی پیاده‌سازی آن در لینوکس می‌پردازیم.

اهمیت استفاده ازFail2ban

۱. **جلوگیری از حملاتBrute Force:** به طور موثری تلاش‌های ناموفق مکرر برای ورود به سیستم را شناسایی کرده و آدرس‌های IP مهاجم را مسدود می‌کند.

۲. **افزایش امنیت سیستم** :با مسدود کردن آدرس‌های IP مشکوک، Fail2banبه طور قابل توجهی امنیت سیستم را افزایش می‌دهد و از نفوذهای غیرمجاز جلوگیری می‌کند.

۳. **مدیریت آسان**: به راحتی قابل نصب و پیکربندی است و به مدیران سیستم امکان می‌دهد تا سیاست‌های امنیتی خود را به طور موثری اعمال کنند.

مراحل عملی پیاده‌سازیFail2ban

۱. **نصب :Fail2ban** برای نصب Fail2ban در توزیع‌های مبتنی بر Debian وUbuntu ، از دستور زیر استفاده کنید:

```
sudo apt-get install fail2ban
```

در توزیع‌های مبتنی بر Red Hat وCentOS:

```
sudo yum install epel-release

sudo yum install fail2ban
```

۲. **پیکربندی Fail2ban**: فایل پیکربندی اصلی Fail2ban در مسیر /etc/fail2ban/jail.conf قرار دارد، اما توصیه می‌شود که تنظیمات خود را در فایل /etc/fail2ban/jail.local اعمال کنید تا از بازنویسی تنظیمات در به‌روزرسانی‌های بعدی جلوگیری شود.

یک فایل پیکربندی نمونه:

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

sudo nano /etc/fail2ban/jail.local
```

۳. **تنظیم Jail برای SSH**: برای تنظیم Fail2ban جهت محافظت از سرویس SSH ، بخش [sshd] را در فایل jail.local ویرایش کنید:

```
[sshd]

enabled  = true

port     = ssh

logpath  = /var/log/auth.log

maxretry = 5
```

٤. **تعریف اقدامات (Actions) :** از اقدامات مختلفی برای مسدود کردن آدرس‌های IP استفاده می‌کند. می‌توانید از اقدامات پیش‌فرض استفاده کنید یا اقدامات خود را تعریف کنید. به عنوان مثال، برای مسدود کردن آدرس IP با استفاده از iptables:

```
banaction = iptables-multiport
```

۵. **راه‌اندازی و فعال‌سازی Fail2ban:** پس از پیکربندی، سرویس Fail2ban را راه‌اندازی و فعال کنید:

```
sudo systemctl start fail2ban

sudo systemctl enable fail2ban
```

٦. **بررسی وضعیت Fail2ban:** برای بررسی وضعیت Fail2ban و مشاهده آدرس‌های IP مسدود شده، از دستورات زیر استفاده کنید:

```
sudo fail2ban-client status

sudo fail2ban-client status sshd
```

نتیجه‌گیری

استفاده از Fail2ban یکی از موثرترین روش‌ها برای افزایش امنیت سرورهای لینوکسی و محافظت در برابر حملات Brute Force است. با نصب و پیکربندی صحیح این ابزار، می‌توان به طور قابل توجهی امنیت سیستم را افزایش داد و از نفوذهای غیرمجاز جلوگیری کرد. آشنایی و پیاده‌سازی صحیح Fail2banبه مدیران سیستم کمک می‌کند تا از داده‌های حساس خود محافظت کرده و از عملکرد بهینه سرورهای خود اطمینان حاصل کنند.

منابع و ارجاعات

- https://roadmap.sh/linux
- https://roadmap.sh/r/general-linux-server-hardening
- https://youtu.be/0QgUPK24NNE?si=RQE9ecRdtYI-vGX_&t=1253
- https://xaas.ir/blog/fail2ban-2/
- https://xaas.ir/blog/fail2ban/