Instalace a nastavení Fail2ban

Co je to Fail2ban?

Fail2ban je open-source nástroj, který pomáhá chránit server před útoky typu "brute force" (útok hrubou sílou), kdy útočník pokouší prolomit heslo pomocí opakovaných neúspěšných pokusů. Fail2ban monitoruje logovací soubory různých služeb (např. SSH, Apache, Nginx) a zablokuje přístup pro IP adresy, které se pokoušejí přihlásit se s nesprávnými údaji vícekrát než je stanoveno v konfiguraci. V návodu si ukážeme nastavení Fail2ban pro blokaci neúspěšných přihlášení na SSH.

Instalace Fail2ban

- Otevřete si SSH.
- Nainstalujte Fail2ban příkazem:

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

- Aktivujte si fail2ban

```
sudo systemctl enable fail2ban-client
```

- Po dokončení instalace můžete ověřit, zda je Fail2ban správně nainstalován, spuštěním následujícího příkazu:

```
sudo fail2ban-client status
```

- Pokud byla instalace úspěšná, měli byste vidět něco podobného:

```
Status
|- Number of jail:      1
```

```
`- Jail list:   sshd
```

Nastavení Fail2ban pro SSH

- Otevřete konfigurační soubor Fail2banu pro SSH příkazem:

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

- Přidejte následující obsah do souboru:

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
```

- Uložte soubor a restartujte Fail2ban příkazem:

```
sudo systemctl restart fail2ban
```

Kontrola funkčnosti Fail2ban pomocí IPTables

- Pomocí následujícího příkazu můžete zkontrolovat, zda je Fail2ban aktivní a blokuje přístup pro potencionálně nebezpečné IP adresy:

```
sudo iptables -L
```

- Za předpokladu, že Fail2ban již nějakou IP adresu, byste měl vidět něco podobného tomuto:

```
Chain f2b-sshd (1 references)
target     prot opt source               destination
```

```
REJECT     all  --  192.168.1.100        anywhere             reject-with icmp-port-
unreachable
RETURN     all  --  anywhere             anywhere
```

Odstranění Fail2ban banu

- Pokud chcete odstranit blokaci pro všechny IP adresy, použijte následující příkaz:

```
sudo fail2ban-client unban --all
```

- Pokud chcete odstranit specifickou IP adresu použijte následující příkaz:

```
sudo fail2ban-client set f2b-sshd unbanip IP_K_ODBLOKACI
```

Tím jsme dokončili návod na instalaci a nastavení Fail2banu na Ubuntu. Nezapomeňte, že je důležité pravidelně kontrolovat logovací soubory a upravovat nastavení Fail2banu podle vašich potřeb.

Revision #3
Created 15 February 2023 21:32:09 by Petr Kývala
Updated 15 February 2023 21:54:32 by Petr Kývala