Fail2Ban: Proteja já o seu Raspberry PI

Date : 5 de Maio de 2017

A ferramenta Fail2Ban pode ser considerada como um agente que monitoriza regularmente os logs dos mais diversos serviços do seu sistema Linux. No caso de encontrar tentativas de acesso indevidas a um determinado serviço (ex. ssh, pam, xinetd, apache, vsftpd, proftpd, wuftpd, postfix, named, etc), o Fail2Ban adiciona dinamicamente uma regra na firewall do sistema que bloqueia de imediato as sessões/comunicações do suposto atacante.

Aprenda da instalar e configurar o Fail2Ban no seu Raspberry PI.

Com instalar o Fail2Ban no Raspberry PI?

Este tutorial tem como base o sistema operativo PiPplware, no entanto deverá funcionar em outras distribuições que têm como base o Ubuntu.

A instalação do Fail2Ban é bastante simples. Para tal basta executar o seguinte comando:

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

Em seguida vamos ao ficheiro de configuração (**/etc/fail2ban/jail.conf)** e adaptamos de acordo com o que pretendemos. Vamos por exemplo considerar o serviço SSH.

```
nano -w /etc/fail2ban/jail.local
```

Próximo passo é ir à secção **[Default]** onde podemos fazer algumas configurações. Para este exemplo vamos considerar que devem ser ignorados os endereços IP da gama 192.168.0.0/16, que o número de segundos que uma máquina deve ficar banida deve ser de 15 minutos (900 segundos) e que o Fail2Ban apenas atua após 3 tentativas falhadas de autenticação.

```
# SSH  # 3 tentativas falhadas: Ban por 15 minutos  [ssh]  enabled = t
rue  port = ssh  filter = sshd  action = iptables[name=SSH, port=ssh,
protocol=tcp]  mail-whois-lines[name=%(__name__)s, dest=%(destemail)s,
 logpath=%(logpath)s]  logpath = /var/log/auth.log  maxretry = 3  bant
ime = 900  ignoreip = 192.168.0.0/16
```

Feita a configuração geral, vamos agora indicar o serviço. O Fail2Ban tem já alguns filtros pré-definidos para vários serviços. Assim basta fazer algumas adaptações.

Aqui vai um exemplo:

```
[ssh-ddos]  enabled = true  port = ssh  filter = sshd-ddos  action = i
ptables[name=SSH, port=ssh, protocol=tcp]  logpath = /var/log/auth.log
  maxretry = 10  ignoreip = 192.168.0.0/16
```

Nota: Não se esqueçam de indicar o caminho correto do log do SSH do vosso sistema.

Por fim reiniciem o serviço Fail2Ban usando o seguinte comando:

```
sudo /etc/init.d/fail2ban restart
```

Verifique se o Fail2Ban está a funcionar acedendo ao ficheiro de log.

```
sudo tail -f /var/log/fail2ban.log
```

Já conhece a nossa promoção do Raspberry PI? Vejam aqui a nossa promoção (agora com o PiPplware 6).