Fail2Ban

written by archi | 24 października 2019

Uruchamiany usługę blokowania dostępu do usług. Jej celem jest blokowanie nieautoryzowanych dostępów do usług poprzez wyszukiwanie w logach systemowych informacji o np. błędnym haśle itp.

1. Aktualizuj bazę dostępnego oprogramowania

```
apt-get update
```

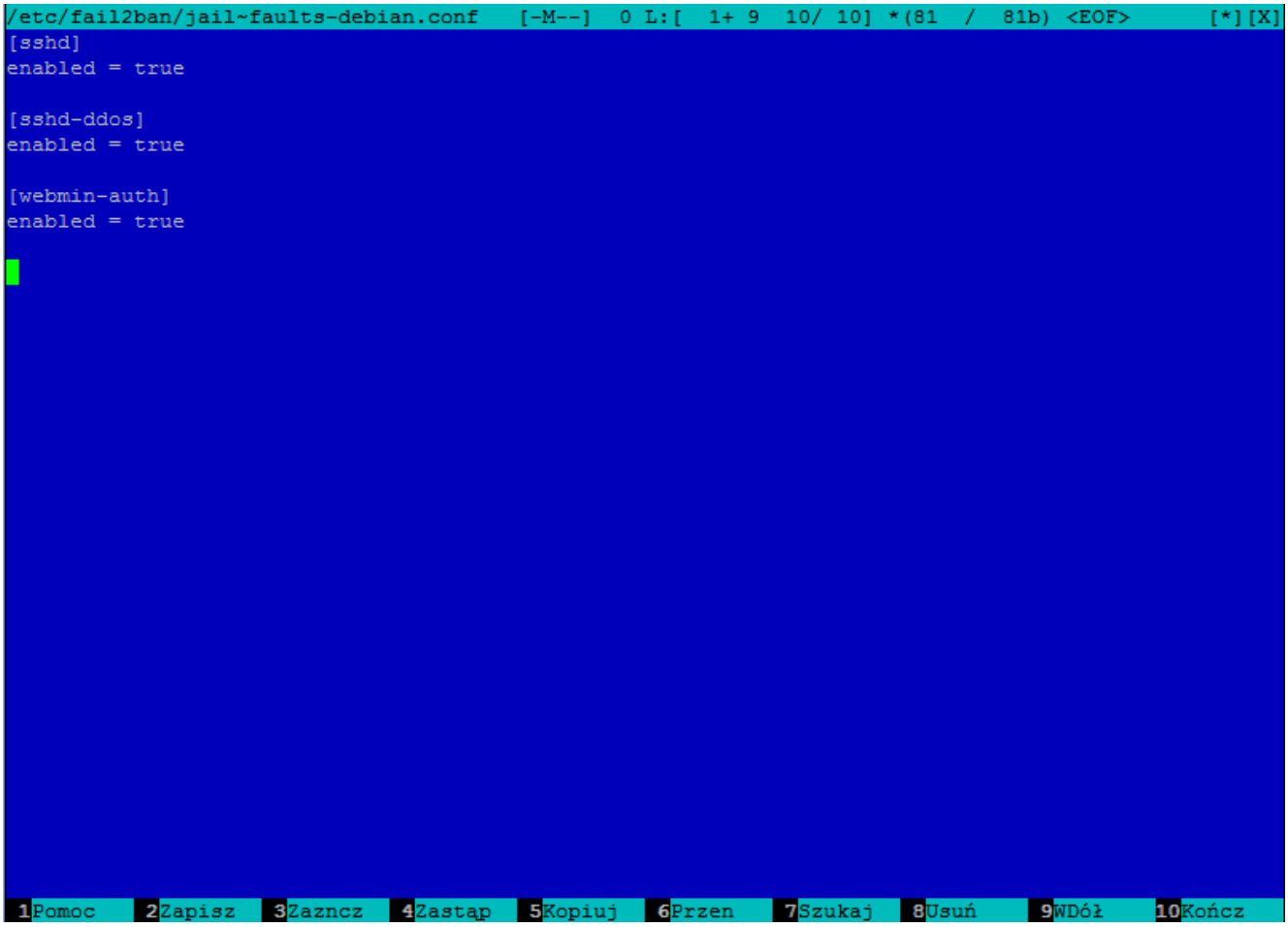
2. Zainstaluj pakiet „fail2ban”

```
apt-get install fail2ban
```

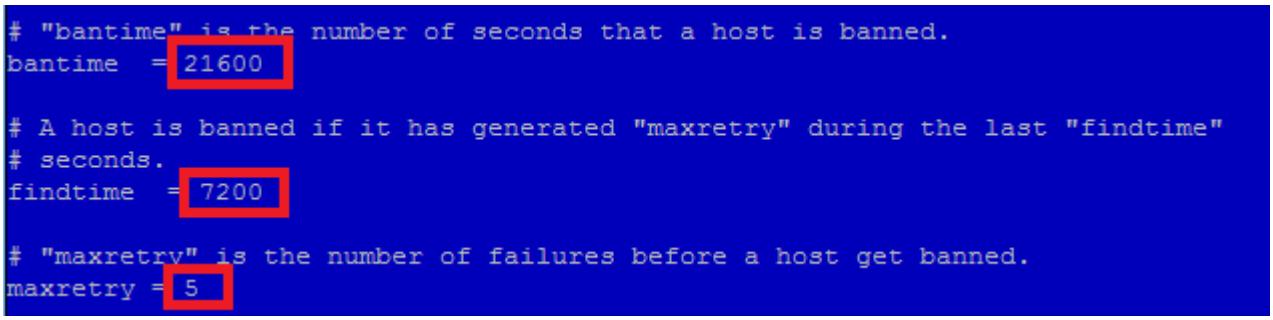
3. W katalogu „`/etc/fail2ban`” zostały zgromadzone pliki konfiguracyjne tego pakietu. *(widok dla Ubuntu 16.04)*

```
fail2ban
├ /action.d
│    ├ apf.conf
│    │  [...]
│    └ -xarf-login-attack.conf
├ /fail2ban.d
├ /filter.d
│    ├ /ignorecommands
│    ├ 3proxy.conf
│    │  [...]
│    └ xinetd-fail.conf
├ /jail.d
│    └ defaults-debian.conf
├ fail2ban.conf
├ jail.conf
├ paths-common.conf
└ paths-debian.conf
```

4. Należy włączyć sprawdzanie dla „**sshd**„, „**sshd-ddos**„, „**webmin-auth**” w pliku „`/etc/fail2ban/jail.d/defaults-debian.conf`„



5. W pliku „`/etc/fail2ban/jail.conf`” należy zmienić wartości domyślne dla: bantime = 60, findtime = 3600 i maxretry = 3 – wartości na obrazku w czerwonych ramkach



W tym samym pliku podane są domyślnie parametry dla kolejnych włączonych wcześniej więzień (jail)

```
[sshd]

port    = ssh
logpath = %(sshd_log)s


[sshd-ddos]
# This jail corresponds to the standard configuration in Fail2ban.
# The mail-whois action send a notification e-mail with a whois request
# in the body.
port    = ssh
logpath = %(sshd_log)s
```

```
[webmin-auth]

port    = 10000
logpath = %(syslog_authpriv)s
```

6. Po wprowadzeniu wszystkich zmian restartujemy usługę:

```
services fail2ban restart
```

7. Sprawdzimy czy usługa działa poprawnie:

`fail2ban-client`

8. Wykonamy test sprawdzający czy więzienie dla Webmin-Auth działa:

– wykonaj polecenie dla sprawdzenia wpisów

```
fail2ban-client status
```

– w wyniku powinieneś zobaczyć odpowiedź systemu

```
Status
|- Number of jail:      3
`- Jail list:   sshd, sshd-ddos, webmin-auth
```

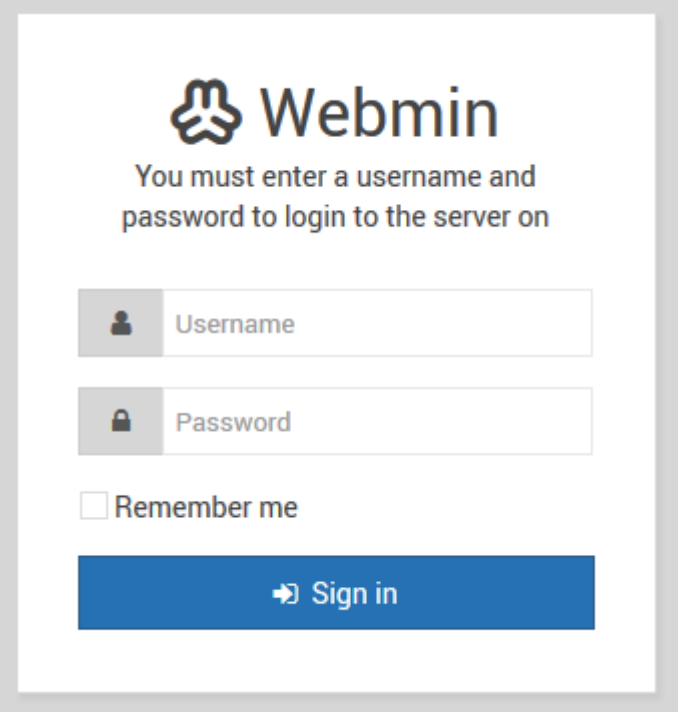
– sprawdzimy wpisy w Firewall

```
iptables -L -n
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-webmin-auth  tcp  --  0.0.0.0/0      0.0.0.0/0
```

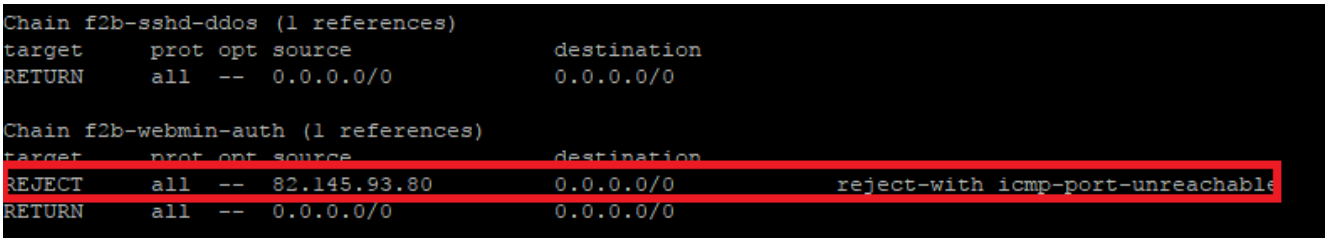
```
multiport dports 10000
f2b-sshd-ddos    tcp  --  0.0.0.0/0      0.0.0.0/0
multiport dports 22
f2b-sshd         tcp  --  0.0.0.0/0      0.0.0.0/0
multiport dports 22
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
Chain f2b-sshd (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
Chain f2b-sshd-ddos (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
Chain f2b-webmin-auth (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

– zaloguj się na stronie „`https://192.168.x.x:10000/`” do konsoli Webmin w sposób prawidłowy oraz następnie wykonaj 3x błędne logowanie



– gdy zalogujemy się niepoprawnie po raz trzeci (3) to nastąpi zablokowanie dostępu dla adresu IP z którego się logowaliśmy i dostęp do strony Webmin

będzie zablokowany na ustawiony wcześniej czas 60s.



Jeśli uzyskasz taki efekt to usługa została skonfigurowana poprawnie...