

Script to check for Banned IPs

If you want to save yourself the trouble of checking every Fail2Ban jail yourself, you can use the following script, which moreover, runs a whois check, to tell you to whom the IP belongs. With some tweaks, you can also include this script in your monitoring (e.g. Nagios, Icinga).

```
#!/bin/bash

if [ $( id -u ) -ne 0 ]; then echo "$0 needs root to run"; exit 1; fi

LOG=fail2ban-whois.log
BOLD=$( tput bold )
SGR0=$( tput sgr0 )
SMUL=$( tput smul )
RMUL=$( tput rmul )

LIST=0
if [ $( echo $* | grep '\-h' ) ]; then echo -e "\n$0 [-h] help\n$0 [-s] output short listing (default)\n$0 [-l] output long listing\n"; exit 0; fi
if [ $( echo $* | grep '\-s' ) ]; then LIST=0; fi
if [ $( echo $* | grep '\-l' ) ]; then LIST=1; fi
echo "$( date +%F %T ) running ${BOLD}$0${SGR0} and logging to ${SMUL}$LOG${RMUL}..." | tee -a $LOG
for j in $( fail2ban-client status | grep --color=never "Jail list:" | sed -e 's/.*:.*\(.*/\1/g' -e 's/,//g' ); do
    for ip in $( fail2ban-client status $j | grep "IP list:" ); do
        if [ "$( echo $ip | grep -E [0-9a-fA-F.:]{4} )" ]; then
            echo -e "[JAIL] $j [IP] ${BOLD}$ip${SGR0} [WHOIS]\n$( whois $ip | \
                sed '0,/descr:/{s/descr:/descr_1:/}' | \
                grep -E '^((% Abuse contact for|abuse-mailbox:))|(inetnum:|CIDR:|IPv4 Address))|([nN]et[nN]ame:|Service Name|ownerid:)|([cC]ountry:|# KOREAN(UTF8))|(descr_1:|Organization Name|owner:))' | \
                sed -e 's/^ */g' -e 's/ */ /g' | sed -e 's/ - /- /g' \
                -e 's/% Abuse contact for.*is '\''\(.*/\1'\''/abuse-c: \1/g' -e "s/(abuse-c:|abuse-mailbox:)/${SMUL}abuse:${RMUL}/g" \
                -e "s/(inetnum:|CIDR:|IPv4 Address :)/${SMUL}inetnum:${RMUL}/g" -e "s/([nN]et[nN]ame:|Service Name :|ownerid:)/${SMUL}netname:${RMUL}/g" \
                -e "s/# KOREAN(UTF8)/${SMUL}country:${RMUL} ${BOLD}KR${SGR0}/" -e "s/[cC]ountry: \[a-zA-Z][a-
```

```

zA-Z])\)(.*\)/${SMUL}country:${RMUL} ${BOLD}\U\1\E${SGR0}\2/g" \
    -e "s/(Organization Name :\\owner:)/${SMUL}descr:${RMUL}/g" | \
    sort -f | uniq -i | sed "s/descr_1:/${SMUL}descr:${RMUL}/g"
)" | ( [ $LIST -eq 0 ] && sed ':a;N;$!ba;s/(\\n\\|\\r\\n\\)/ /g' || cat )
fi
done
done | tee -a $LOG

```

You can download it [here](#), or for more convenience, just run the below command

```
curl -f TODO -o ${HOME}/fail2banwhois.sh && chmod +x ${HOME}/fail2banwhois.sh
```

You have to run the script with Sudo privileges. It will show you all currently banned IPs. The output looks like this (IP's are masked):

```

[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: info@starcrecium.com country: RU inetnum:
100.100.100.100.0-100.100.100.100.255 netname: CY-STARCRECIUM descr: HOSTWAY route object
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] country: GB country: US inetnum: 100.100.100.100/13,
100.100.100.100.0.0/13, 100.100.100.100/12 inetnum: 100.100.100.100/15 netname: AMAZON-LHR netname:
AT-88-Z
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@ito.gov.ir country: IR inetnum: 100.100.100.100-
100.100.100.100 netname: TBZ-MED descr: Tabriz University of Medical Sciences
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@xyz.de country: DE inetnum: 100.100.100.100-
100.100.100.100 netname: Science-LAN descr: Some Science Institution
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@versatel.de country: DE inetnum:
100.100.100.100-100.100.100.100 netname: DE-VERSATEL-20080807 descr: VT-Customer
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@xyz.de country: DE inetnum: 100.100.100.100-
100.100.100.100 netname: Science-LAN descr: Some Science Institution
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@cdn77.com country: AT country: GB inetnum:
100.100.100.100-100.100.100.100 netname: CDN77-VIE descr: CDN77-VIE POP
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@contabo.de country: DE inetnum:
100.100.100.100-100.100.100.100 netname: CONTABO
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@contabo.de country: DE inetnum:
100.100.100.100-100.100.100.100 netname: CONTABO descr: Contabo GmbH
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@pindc.ru country: RU inetnum: 100.100.100.100-
100.100.100.100 netname: PINDC-public-vlans descr: PIN DC
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@contabo.de country: DE inetnum:
100.100.100.100-100.100.100.100 netname: CONTABO
[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@telekom.de country: DE inetnum:
100.100.100.100-100.100.100.100 netname: DTAG-DIAL28 descr: Deutsche Telekom AG

```

[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: ipas@cnnic.cn country: CN inetnum: 100.100.100.100-100.100.100.100 netname: TencentCloud descr: Tencent cloud computing (Beijing) Co., Ltd.

[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: qcloud_net_duty@tencent.com country: AU country: CN country: ZZ inetnum: 100.100.100.100-100.100.100.100 inetnum: 100.100.100.100/16 netname: APNIC netname: TENCENT-CN descr: Tencent Cloud Computing (Beijing) Co., Ltd

[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] country: US inetnum: 100.100.100.100/12, 100.100.100.100/14, 100.100.100.100/14, 100.100.100.100/17, 100.100.100.100/12, 100.100.100.100/15, 100.100.100.100/13, 100.100.100.100/16 netname: MSFT

[JAIL] nginx-dos [IP] 100.100.100.100 [WHOIS] abuse: abuse@versatel.de country: DE inetnum: 100.100.100.100-100.100.100.100 netname: VT-Customer-POOL descr: Versatel Deutschland

Revision #2

Created 24 November 2024 17:12:32 by Nicolas

Updated 16 December 2024 10:42:28 by Nicolas