Fail2Ban Helper Script für Netcup vServer

Firewall Regeln über den VCP Webservice anlegen

Script & Doku by Christian Blechert – Stand: 2012-09-18 – Lizenz: http://üäx.de/eP

1. Inhaltsverzeichnis

2. Einleitung

Da es auf vServern von Netcup nicht möglich ist kernelnahe Funktionen wie iptables zu nutzen, soll dieses Script die Nutzung von fail2ban über den Netcup VCP Webservice ermöglichen.

3. Das VCP vorbereiten

Das Webservice Feature muss über die Optionen des VCPs aktiviert werden. Nach der Aktivierung kann hier ein Passwort extra für den Webservice festgelegt werden.

Das Passwort muss dann später in dem Script hinterlegt werden.

Abbildung 1: Webservice freischalten

4. Download

Das Script und einige Zusatzdateien befinden sich in einem GIT Repository.

4.1. Zugagdaten in eine separate Datei auslagern

Um das Update auf eine neuere Version zu vereinfachen, kann man die Zugangsdaten zum VCP in eine separate Datei auslagern.

Das Hauptscript prüft zuerst ob es diese Datei im selben Ordner gibt. Erst wenn es diese Datei nicht gibt, werden die internen Zugangsdaten verwendet.

http://gitweb.fiae.ws/scripts.git/blob/master:/linux/fail2ban/nc_vcp_settings_example.php

4.2. Das eigentliche Script

http://gitweb.fiae.ws/scripts.git/blob/master:/linux/fail2ban/nc_firewallapi_beta.php

4.3. Beispiel Einrichtung

Eine Beispiel action.d Konfiguration für Fail2Ban.

http://gitweb.fiae.ws/scripts.git/blob/master:/linux/fail2ban/example.conf

5. System Voraussetzungen

- PHP5 CLI
- PHP SOAP Libary

5.1. Pakete auf Debian installieren

```
apt-get install php5-cli
```

5.2. Zeitzone konfigurieren

Bei einigen vServer Betreibern scheint die Standard Zeitzone nicht konfiguriert worden zu sein. Da diese Einstellung nichts in einem Script zu suchen hat, sollte man dies selbst in der php.ini der CLI einstellen.

Unter Debian findet man die Datei unter /etc/php5/cli/php.ini.

Vorher

```
[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
;date.timezone =
```

Nacher

```
[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
date.timezone = Europe/Berlin
```

Der Neustart von Diensten ist nicht notwendig.

6. Konfiguration des Scripts ausfüllen

Hier hat man die Wahl die Zugangsdaten direkt in das Script oder in eine separate Datei einzutragen. Die separate Datei hat den Vorteil, dass man das Script bei einem Update einfach austauschen muss. Die Zugangsdaten bleiben dann erhalten.

```
//--> enable/disable debug output
define("DEBUG_OUTPUT", true);

//--> API URL
define("SOAP_URL", "https://www.vservercontrolpanel.de/WSEndUser?
wsdl");

//--> VCP logindata
define("VCP_USERNAME", "kundennummer");
define("VCP_PASSWORD", "webservicepw");

//--> vServer name (vXXXXXXXXXXXXXXX)
define("VCP_SERVERNAME", "v220120522199999");

//--> Blacklisted IPs will not blocked
define("IP_BLACKLIST", "0.0.0.0,127.0.0.1");
```

6.1. DEBUG_OUTPUT

Legt fest, ob das Script Informationen zu den ausgeführten Aktionen Ausgeben soll.

Mögliche Werte: `true`, `false`

6.2. SOAP_URL

Legt fest, unter welcher URL der Webservice zu erreichen ist. Diese URL sollte für alle vServer gleich sein und sich nicht ändern.

6.3. VCP_USERNAME

Im normalfall die Netcup Kundennummer. Bei einigen alten Kunden kann es auch noch ein Benutzername bestehend aus den ersten drei Buchenstaben des Vornamens und des kompletten Nachnamens sein.

6.4. VCP_PASSWORD

Das Passwort welches in den Optionen für den Webservice angelegt wurde. Hierbei handelt es sich **NICHT** um das Passwort mit man sich in das VCP einloggt.

6.5. VCP_SERVERNAME

Der Name des vServers auf dem das Script läuft. Dieser Name besteht **IMMER** aus einem „v“ und einer langen Nummer. Ohne Leerzeichen.

6.6. IP_BLACKLIST

Hier können Komma separiert IP Adressen definiert werden, die von dem Scrript ignoriert werden. Diese Option bitte mit äußerster Vorsicht benutzen!

7. Beispielaufrufe

```
php -f script.php add|delete INPUT|OUTPUT sourceIP ACCEPT|REJECT|DROP
```

7.1. Firewall Regel hinzufügen

```
php -f nc_firewallapi_beta.php add INPUT 42.42.42.42 DROP
```

Hier wird eine Regel angelegt, welche jeglichen Datenverkehr von der IP 42.42.42.42 verhindert.

```
php -f nc_firewallapi_beta.php add INPUT 42.42.42.42 DROP "a comment"
```

Hier wird zusätzlich der Kommentar um den angegebenen Text erweitert.

7.2. Firewall Regel löschen

```
php -f nc_firewallapi_beta.php delete INPUT 42.42.42.42 DROP
```

8. In Fail2Ban einbinden

Der einfachste Weg das Script in Fail2Ban einzubinden ist die Vorhandene action.d Konfiguration für iptables-multiport anzupassen.

Es müssen nur die Optionen `actionban` und `actionunban` angepasst werden. Die Optionen `actionstart`, `actionstop` und `actioncheck` können auskommentiert werden.

Fail2Ban neu starten und Jails Konfigurieren nicht vergessen! Nun sollten im Log entsprechende Ban/Unban Meldungen auftauchen, wenn jemand zu oft versucht sich einzuloggen.