CSF telepítése

Ebben a cikkben elmagyarázzuk, hogyan telepíthető és konfigurálható a ConfigServer Security & Firewall-t (rövidítve a CSF). A CSF egy teljes körű biztonsági csomag, amit használhat tűzfal és behatolás / bejelentkezési hiba észlelő rendszerként.

A CSF TELEPÍTÉSE ÉS BEÁLLÍTÁSA LINUX RENDSZEREN

Ahhoz, hogy a CSF telepíthető legyen és normális módon fusson a Perl és a libwww csomagoknak telepítve kell lenniük a szerveren. A CSF-et jelenleg bármelyik RHEL, CentOS, openSUSE, Debian és Ubuntu disztribúció alá lehet telepíteni.

```
yum install perl-libwww-perl
apt install libwww-perl
```

1. **CSF letöltése**

   ```
   cd /usr/src
   wget https://download.configserver.com/csf.tgz
   ```

2. **A letöltött csomag kitömörítése**

   ```
   tar xzf csf.tgz
   cd csf
   ```

3. **a CSF telepítő futtatása**A folyamat ezen része ellenőrzi, hogy az összes függőség telepítve van-e, létre hozza a webes felülethez szükséges könyvtárstruktúrákat és fájlokat, észleli az éppen megnyitott portokat, valamint figyelmezteti Önt arra, hogy a csf és az lfd démonokat újra kell indítani, miután elvégezte a kezdeti beállítást.

   ```
   sh install.sh
   perl /usr/local/csf/bin/csftest.pl
   ```

   A fenti parancs várható kimenete a következő:

```
Testing ip_tables/iptable_filter...OK
Testing ipt_LOG...OK
Testing ipt_multiport/xt_multiport...OK
Testing ipt_REJECT...OK
Testing ipt_state/xt_state...OK
Testing ipt_limit/xt_limit...OK
Testing ipt_recent...OK
Testing xt_connlimit...OK
Testing ipt_owner/xt_owner...OK
Testing iptable_nat/ipt_REDIRECT...OK
Testing iptable_nat/ipt_DNAT...OK

RESULT: csf should function on this server
```

4. **Az éppen futó tűzfal letiltása, a CSF beállítása**Állítsa le, majd tiltsa le a firewalld-t a következő parancsok kiadásával, ezt követően állítsa be a CSF-et.

```
systemctl stop firewalld
systemctl disable firewalld
```

Az `/etc/csf/csf.conf` fájlban módosítsa a `TESTING = "1"` változó értékét `TESTING = "0"`-ra különben az lfd démon nem indul el), ezt követően állítsa be a vesszővel elválasztva a bejövő és kimenő portokat (TCP_IN és TCP_OUT). A fájl tartalma megközelítőlegesen így kell hogy kinézzen:

```
# Testing flag - enables a CRON job that clears iptables incase of
# configuration problems when you start csf. This should be enabled until you
# are sure that the firewall works - i.e. incase you get locked out of your
# server! Then do remember to set it to 0 and restart csf when you're sure
# everything is OK. Stopping csf will remove the line from /etc/crontab
#
# lfd will not start while this is enabled
TESTING = "0"

# Allow incoming TCP ports
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"

# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,53,80,110,113,443,587,993,995"
```

A megfelelő beállítások megadását követően mentse el a fájlt, majd lépjen ki a szerkesztőből.

5. **A CSF újraindítása és tesztelése**

```
# systemctl restart {csf,lfd}
# systemctl enable {csf,lfd}
# systemctl is-active {csf,lfd}
# csf -v
```

Innentől a CSF már használatra kész, azonban a tűzfal és behatolásérzékelés szabályait még célszerű beállítani.

A CSF HASZNÁLATÁHOZ SZÜKSÉGES FONTOSABB PARANCSOK

A jelenlegi tűzfal szabályok kilistázásához adjuk ki a következő parancsot:

```
# csf -l
```

A tűzfal szabályokat a következő parancs segítségével törölheti:

```
# csf -f
```

A tűzfal szabályokat a következő parancs segítségével töltheti újra:

```
# csf -r
```

A fenti parancsokat lehetőség szerint jegyezze meg mert a későbbiek során szüksége lehet rájuk amikor a **csf** és az **lfd** újraindításra kerül.

IP-CÍMEK ENGEDÉLYEZÉSE ÉS TILTÁSA, AZ ENGEDÉLYEZETT ÉS TILTOTT ELEMEK ELTÁVOLÍTÁSA

A bejövő kapcsolatok engedélyezése 192.168.0.10-től.

```
# csf -a 192.168.0.10
```

Hasonlóképpen megtagadhatja a 192.168.0.11-ből származó kapcsolatokat.

```
# csf -d 192.168.0.11
```

Eltávolíthatja a fenti szabályokat, ha ezt szeretné.

```
# csf -ar 192.168.0.10
# csf -dr 192.168.0.11
```

A `-ar` illetve a `-dr` kapcsolók használata a fenti IP-címmel társított meglévő engedélyezési és megtagadási szabályokat eltávolítja.

BEJÖVŐ KAPCSOLATOK KORLÁTOZÁSA FORRÁS SZERINT

A kiszolgáló tervezett felhasználásától függően a kapcsolatokat korlátozhatja port alapon, és a beérkező próbálkozások száma szerint. Ehhez nyissa meg az `/etc/csf/csf.conf` fájlt, és keresse meg a `CONNLIMIT` részt. Megadható több port, a portokat `;` elválasztva adja meg. Például:

```
CONNLIMIT = "22; 2,80; 10"
```

a fenti példában csak 2 bejövő kapcsolatot engedélyez ugyanabból a forrásból a 22-es portra, míg a 80-as TCP port esetén egy IP címről maximum 10 kapcsolatot engedélyez.

EMAIL ÉRTESÍTÉSEK

Számos riasztási típus beállítható, ehhez keresse meg az `EMAIL_ALERT` részt a `/etc/csf/csf.conf` fájlban, majd ellenőrizze le hogy az értéke `1`-re van e állítva. Például:

```
LF_SSH_EMAIL_ALERT = "1"
LF_SU_EMAIL_ALERT = "1"
```

az `LF_ALERT_TO` résznél megadott email címre küldi minden egyes alkalommal, amikor valaki sikeresen bejelentkezik az SSH-n keresztül, vagy átvált egy másik fiókra a `su` parancs segítségével.

A CSF KONFIGURÁCIÓS FÁJLOK HELYE

A következő fájlok segítségével módosítható a `csf` működése. A `csf` összes konfigurációs fájlja a `/etc/csf` könyvtár alatt található. Az alábbi fájlok módosítása esetén a `csf démont újra kell indítani.`

- **csf.conf**: A CSF fő konfigurációs állománya.
- **csf.allow**: A tűzfalon engedélyezett IP és CIDR címek listája.
- **csf.deny**: A tűzfalon található tiltott IP és CIDR címek listája.
- **csf.ignore**: A tűzfalon a figyelmen kívül hagyott IP és CIDR címek listája.
- **csf.*ignore**: A tűzfalon a figyelmen kívül hagyott egyéb felhasználók, fájlok, IP címek listája.

A CSF ELTÁVOLÍTÁSA

Ha teljesen el szeretné távolítani a CSF-et, akkor futtassa a `/etc/csf/uninstall.sh`

```
#/etc/csf/uninstall.sh
```

A fenti parancs teljesen törli a CSF-et az összes fájlt és mappát.

Változat #1
DotRoll Tudásbázis hozta létre 2023-09-21 09:15:53 CEST
DotRoll Tudásbázis frissítette 2023-09-21 09:17:08 CEST