Блокировка источников динамическим листом IP с UFW

Устанавливаем необходимые пакеты:

```
apt-get -y install ipset
```

Создаем блок лист:

```
ipset create "IP_ipsum4_block" hash:ip
```

Добавляем туда значения от общедоступных фидов IPsum (агрегационный фид level 4 - very low false positives) и сохраняем в файл `/etc/ipset.rules`:

```
ipset flush "IP_ipsum4_block"; for IP in $(wget -O - https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt); do ipset add "IP_ipsum4_block" $IP; done; ipset save > /etc/ipset.rules
```

Добавляем ежедневное обновление фидов с crontab (для редактирования планировщика: `crontab -e`):

```
0 0 * * * ipset flush "IP_ipsum4_block"; for IP in $(wget -O - https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt); do ipset add "IP_ipsum4_block" $IP; done; ipset save > /etc/ipset.rules
```

Создайте скрипт для восстановления ipset при перезагрузке:

```
sudo nano /etc/network/if-pre-up.d/ipset_restore
```

Добавьте следующее содержимое:

```
#!/bin/bash
ipset restore < /etc/ipset.rules
```

Сделайте скрипт исполняемым:

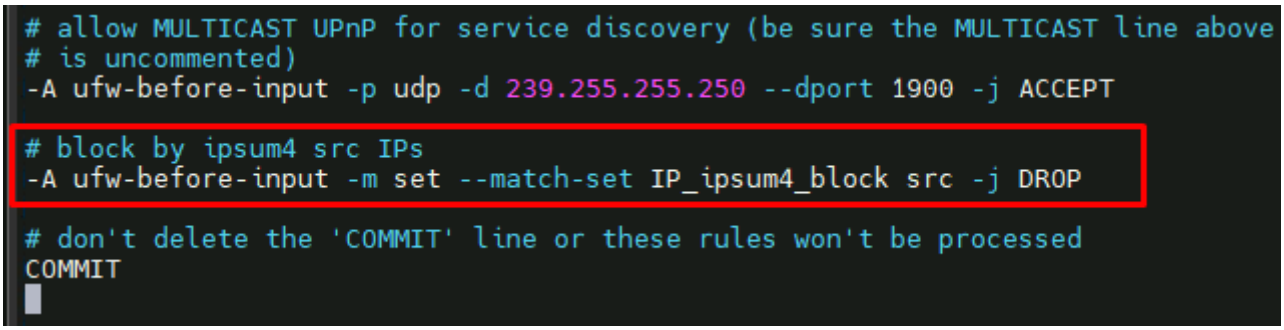
```
sudo chmod +x /etc/network/if-pre-up.d/ipset_restore
```

Далее добавим правило в UFW:

```
sudo nano /etc/ufw/before.rules
```

Добавьте следующее значение до COMMIT:

```
-A ufw-before-input -m set --match-set IP_ipsum4_block src -j DROP
```



Перезапустите UFW:

```
sudo ufw reload
```

Убедитесь, что правило применяется (добавленная запись должна появиться в списке вывода):

```
sudo iptables -S ufw-before-input
```

Revision #1
Created 20 December 2024 10:57:54 by Boris Rzr
Updated 20 December 2024 11:22:01 by Boris Rzr