Поиск и блокировка вредных IP

Продолжение той истории.

Так как на новый сервер переносилась старая база логинов и паролей (что бы максимально смягчить для пользователей шок от перезда), то попадались откровенно слабые к перебору пароли, например 123321 или qwer123. И особо ленивые их не сменили. Поэтому подобрали пароль к старой но редко пользуемой учетке. Для начала меняем пароль через postfixadmin, а потом баним разбойников.

Выясняем кто и что:

```
# cat amavis_open_relay.sh
#!/bin/sh

# 2.2.2.2 - my IP или надежные IP

cat /var/log/amavisd-new.log | grep "OpenRelay" | grep -v -e 2.2.2.2 > /var/log/z_open_relay.`date +%Y-%m-%d`
```

Парсим IP (если добавим к uniq *-c* — получим количество вхождений):

```
# cat z_open_relay.2019-07-16 | grep "user_name" | awk '{print $11}' | uniq > /home/admin/ip_ban_20190716.txt
```

Получился такой список:

```
[191.240.84.96]
[191.36.154.138]
[95.182.120.38]
[95.182.120.36]
[185.231.245.42]
[185.231.245.41]
[185.231.245.46]
[95.182.120.38]
[185.231.245.46]
[95.182.120.38]
[94.242.206.124]
```

```
[185.231.245.40]
[185.231.245.44]
[94.242.206.127]
[185.231.245.48]
[5.44.45.137]
[94.242.206.124]
[185.231.245.43]
[5.44.45.143]
[5.44.45.139]
```

Чистим от скобок:

```
# sed -i -e 's/\[//g' ip_ban_20190716.txt && sed -i -e 's/\]//g' ip_ban_20190716.txt

# cat ip_ban_20190716.txt
191.240.84.96
191.36.154.138
95.182.120.38
95.182.120.36
185.231.245.42
185.231.245.41
185.231.245.46
95.182.120.38
185.231.245.46
95.182.120.38
94.242.206.124
185.231.245.40
185.231.245.44
94.242.206.127
185.231.245.48
5.44.45.137
94.242.206.124
185.231.245.43
5.44.45.143
5.44.45.139
```

С помощью скрипта загоняем их в таблицу на “вечный” бан:

```
# cat add_ip_to_ipfw.sh
#!/bin/sh
# IPFW table 3, 4
cat /home/admin/ip_ban_20190716.txt | { while read ip;
```

```
do
        /sbin/ipfw table 3 add $ip;
done;
}
```