Iptables를 이용한SSH brute force 공격방어

작성자 : 넥스트라인 고객기술지원부 백철현
작성일 : 2009년 03월 19일

SSH brute force 공격은 사전적 계정이름과 단순한 패스워드의 문제를 이용한 대입공격 입니다. Ssh brute force 공격은 하나의 아이디에 여러 개의 패스워드를 대입시켜 보아서 일치되는 경우에 시스템의 사용자 계정을 획득하게 됩니다. 계정이 뚫렸다면, 시스템에 문제를 일으키는 일 뿐만 아니라, 다른 시스템을 해킹하는 또 다른 문제가 발생할 소지가 되기도 합니다. 심한 경우 한 아이피에서 몇 천번이 넘는 시도가 이루어지기도 합니다. 가장 훌륭한 방법은 각 **계정의 패스워드를 매우 복잡하게 영문, 숫자, 특수문자**를 골고루 썩어서 12자 이상으로 만들어 쓰시면 매우 좋습니다. 다른 방법으로는 아래의 iptables 룰셋을 이용해도 대입공격은 막아낼 수 있습니다. 이 룰셋은 아이디와 패스워드를 지속적으로 대입하지 못하도록 하는 룰셋입니다. 대입공격이 아이디와 패스워드를 변경해 가면서 대입하는 것이기 때문에 로긴이 실패했을 경우 다시 시도를 해야하는데 그 시간이 다음 대입시도를 할 때까지 시간을 늘려놓는 것이 이번 룰셋의 핵심입니다. 테스트 결과 과다한 접속시도가 거의 이루어지지 않았습니다. 룰셋은 iptables의 recent, LOG 모듈을 활용한 방법입니다.

1. SSH 공격방어 Flow

1) 22번 포트에 접속시도 한 모든 패킷을 SSH_BLACK 테이블의 리스트에 넣습니다.
2) 이 리스트에서 60초간 6번 이상의 시도가 이루어질 경우에 BLACK 리스트에 올립니다.
3) BLACK 리스트에 오르면 60초간 접속이 차단됩니다.
4) 60초가 지나면 SSH_BLACK 테이블이 갱신되면서 접속시도가 가능해집니다.
   따라서, 자신이 6번 이상 실패했다면 60초 동안 기다렸다가 해야합니다.

2. SSH 공격방어를 위한 룰셋

```
1 #!/bin/sh
2
3 IPT=/sbin/iptables
4
5 $IPT -A INPUT -p tcp --dport 22 -m state --state NEW ₩
6         -m recent --set --name SSH_BLACK
7 $IPT -A INPUT -p tcp --dport 22 -m state --state NEW ₩
8         -m recent --update --seconds 60 --hitcount 6 ₩
9         --rttl --name SSH_BLACK -j LOG --log-prefix "SSH BLACK: "
10 $IPT -A INPUT -p tcp --dport 22 -m state --state NEW ₩
11         -m recent --update --seconds 60 --hitcount 6 ₩
12         --rttl --name SSH_BLACK -j DROP
13
```

첫줄은 iptables 를 짧게 IPT 변수로 만든 것입니다. Iptables 의 위치를 지정해주면 됩니다.

두번째 , 세번째 줄의

$IPT –A INPUT –p tcp –dport 22 –m state –state NEW –m recent -–set -–name SSH_BLACK

위 명령은 22번 SSH 포트로 오는 모든 "새로운 연결" 패킷은 SSH_BLACK 라는 이름으로 정의합니다.

네번째, 다섯째, 여섯번짼 줄의

$IPT –A INPUT –p tcp –dport 22 –m state –state NEW –m recent -–update -–seconds 60 -–hitcount 6 –rttl –name SSHSCAN –j LOG –log-prefix SSH_SCAN:

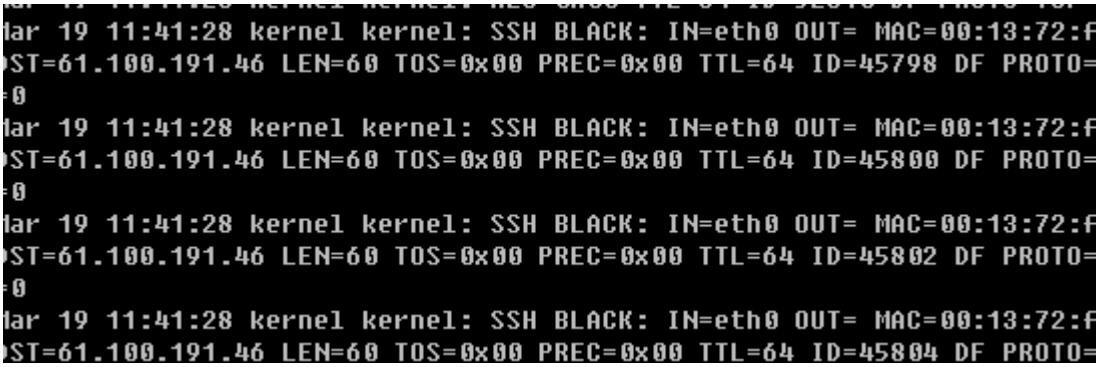
위 줄은 6번의 연결시도를 한 것을 로그로 기록한 것이고 60초 동안 6번의 접속 시도를 하는 아이피를 로그로 남기게 됩니다.

마지막 줄은

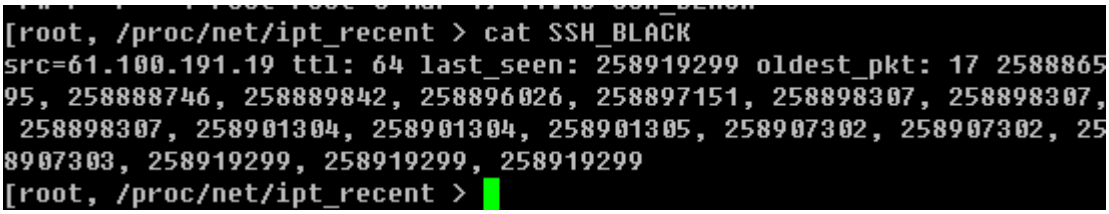
$IPT –A INPUT –p tcp –dport 22 –m state –state NEW –m recent –update –seconds 60 –hitcount 6 -–rttl -–name SSH_BLACK –j DROP

이 마지막줄은 6번 이상을 시도한 접속을 60초 동안 막았다가 60초 후에 다시 black 리스트를 갱신하여 접속이 가능하게 해줍니다.

로그에 기록된 화면입니다. 위치는 /var/log/messages 에서 볼수가 있습니다.



실시간으로 확인 가능한 화면을 보실수 있습니다. 위치는
/proc/net/ipt_recent/SSH_BLACK 파일입니다.



위 스크립트를 적용하실 경우 현재 서버의 IPTABLES의 룰셋에 적용시키는 방법을 소개합니다. 위의 스크립트의 경우는 단독으로 쓰실 경우를 위해서 만든 것 입니다.
만일 현재의 룰셋에 추가 하고 싶으시다면 아래와 같이 해주세요.

```
#!/bin/sh

IPT=/sbin/iptables

$IPT -I INPUT 1 -p tcp --dport 22 -m state --state NEW ₩
        -m recent --set --name SSH_BLACK
$IPT -I INPUT 2 -p tcp --dport 22 -m state --state NEW ₩
        -m recent --update --seconds 60 --hitcount 6 ₩
        --rttl --name SSH_BLACK -j LOG --log-prefix "SSH BLACK: "
$IPT -I INPUT 3 -p tcp --dport 22 -m state --state NEW ₩
        -m recent --update --seconds 60 --hitcount 6 ₩
        --rttl --name SSH_BLACK -j DROP
```

일단, -A 대신 –I 로 현재 룰셋에 삽입을 하였습니다. 그리고, 룰셋의 1,2,3 라인에 추가를 시키도록 $IPT –I INPUT 1 , $IPT –I INPUT 2, $IPT –I INPUT 3 로 설정하였습니다.
저부분은 자신의 사정에 맞게 고치시면 되지만 그냥 저렇게 넣어도 지장은 없습니다.

감사합니다.