

Re: Some new SSH exploit script?

Re: Some new SSH exploit script?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-06/msg00182.html>

- *From:* "Adam.Chesnutt" <icetre@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 09 Jun 2006 10:23:15 -0400
-

You see, rather than do all this, I think it's much much smarter to turn over the logs more, and write a script that outputs the log – without the script kiddies if it really bothers you. You could make the script also write a report and call it 'lame ssh hacktards' or something and contain only ip, username and number of attempts..

This is a piss poor solution to a real problem. If you have cruft, correlate. Ignoring what are genuine (albeit lame) attempts to penetrate your security is dumb.

If 3 people connect to this port, by all means, but just moving the port to decrease your viability of hacktards isn't smart. Your not decreasing your access, your moving the door. Firewall them for god's sake. Instead of ignoring the problem, **DO SOMETHING**

This is why I said something about my killapnic script. My killapnic script is a much better solution than moving the port. Why? Because it actually does something to disallow network access from the attacker, rather than continuing to allow them access, and ignoring the signs of them trying to break in.

Consider zombies.. your in a house, and zombies are outside. Do you, move the windows and doors to a new location, or board them up where they are? There's enough traffic, there's enough zombies, and the scripts are mostly smart enough **already** to find nonstandard ports. Can we please join the future here in good ole 2002?

This script is for FreeBSD, but feel free to correct it, call me an ass, or adapt it for any means needed, so long as my name appears as the original source of the idea. If you do make changes, please mail me, I'd love to hear about it and see your script.

```
#!/usr/local/bin/bash
#-----
#killapnic
#by IcE tRe
#-----
#I am sick to death of apnic trying to login as root on my server,
#even though root logins aren't allowed
#
#Deletes policy 666-699 by default, hope that doesn't clobber your crap
#
#If so, edit the following variables

IPFWCMD="/sbin/ipfw"
LYNXCMD="/usr/local/bin/lynx"
```

Re: Some new SSH exploit script?

Re: Some new SSH exploit script?

```
LYNXFLAGS=" -source"
URL="http://www.iana.org/assignments/ipv4-address-space"
STARTIPFW=665
RANGE="666-699"
MIDDLE=".0.0.0/"
#end variables
SCORE=`$IPFWCMD show $RANGE`
CURRENTRULES=`echo "$SCORE" | awk '{ print $7 }'`
for DELETE in ` $IPFWCMD show $RANGE | awk '{ print $1 }'`
do
$IPFWCMD delete $DELETE
done
echo "Deleted all rules numbered $RANGE and added the following rules:"

for EACH in ` $LYNXCMD $LYNXFLAGS $URL | grep -i apnic | awk '{ print $1 }'`
do

START=`echo $EACH | awk -F/ '{ print $1 }' | bc`
END=`echo $EACH | awk -F/ '{ print $2 }' | awk '{ print $1 }'`
IP=$START$MIDDLE$END
ENDIPFW=$(echo "$STARTIPFW + 1 " | bc)
STARTIPFW=$ENDIPFW
CMDTEMP=`echo "$IPFWCMD add $ENDIPFW deny ip from $IP to any"`
# CMDTEMP2=$CMD$CMDTEMP
# CMD=$CMDTEMP2
$CMDTEMP
done
#$CMD
echo $CMD
echo "Old counts were:"
echo "$SCORE"
echo "Old IP's:"
echo "$CURRENTRULES"
#end script
```

I usually run it in cron with stdout piped to /dev/null, but here's the output if your curious.

```
digitalfreezer# /etc/killapnic
Deleted all rules numbered 666-699 and added the following rules:
00666 deny ip from 58.0.0.0/8 to any
00667 deny ip from 59.0.0.0/8 to any
00668 deny ip from 60.0.0.0/8 to any
00669 deny ip from 61.0.0.0/8 to any
00670 deny ip from 121.0.0.0/8 to any
00671 deny ip from 122.0.0.0/8 to any
00672 deny ip from 123.0.0.0/8 to any
00673 deny ip from 124.0.0.0/8 to any
00674 deny ip from 125.0.0.0/8 to any
00675 deny ip from 126.0.0.0/8 to any
00676 deny ip from 202.0.0.0/8 to any
```

Re: Some new SSH exploit script?

Re: Some new SSH exploit script?

00677 deny ip from 203.0.0.0/8 to any
00678 deny ip from 210.0.0.0/8 to any
00679 deny ip from 211.0.0.0/8 to any
00680 deny ip from 218.0.0.0/8 to any
00681 deny ip from 219.0.0.0/8 to any
00682 deny ip from 220.0.0.0/8 to any
00683 deny ip from 221.0.0.0/8 to any
00684 deny ip from 222.0.0.0/8 to any

Old counts were:

00666 5 202 deny ip from 58.0.0.0/8 to any
00667 53 3022 deny ip from 59.0.0.0/8 to any
00668 23 1085 deny ip from 60.0.0.0/8 to any
00669 27 1282 deny ip from 61.0.0.0/8 to any
00670 0 0 deny ip from 121.0.0.0/8 to any
00671 1 408 deny ip from 122.0.0.0/8 to any
00672 0 0 deny ip from 123.0.0.0/8 to any
00673 8 394 deny ip from 124.0.0.0/8 to any
00674 6 312 deny ip from 125.0.0.0/8 to any
00675 0 0 deny ip from 126.0.0.0/8 to any
00676 9 1500 deny ip from 202.0.0.0/8 to any
00677 23 1152 deny ip from 203.0.0.0/8 to any
00678 14 653 deny ip from 210.0.0.0/8 to any
00679 12 1504 deny ip from 211.0.0.0/8 to any
00680 27 1970 deny ip from 218.0.0.0/8 to any
00681 20 973 deny ip from 219.0.0.0/8 to any
00682 30 1809 deny ip from 220.0.0.0/8 to any
00683 43 2413 deny ip from 221.0.0.0/8 to any
00684 50 3161 deny ip from 222.0.0.0/8 to any

Old IP's:

58.0.0.0/8
59.0.0.0/8
60.0.0.0/8
61.0.0.0/8
121.0.0.0/8
122.0.0.0/8
123.0.0.0/8
124.0.0.0/8
125.0.0.0/8
126.0.0.0/8
202.0.0.0/8
203.0.0.0/8
210.0.0.0/8
211.0.0.0/8
218.0.0.0/8
219.0.0.0/8
220.0.0.0/8
221.0.0.0/8
222.0.0.0/8

digitalfreezer#

Re: Some new SSH exploit script?

Re: Some new SSH exploit script?

I used to reset the connections, but in the interest in making the scripts run slower, I let em hang.

Anyways, enough from me. :)

Adam

Paul Barrette wrote:

I totally agree the the last statement.

Full port scan + a banner grab... you then know it's an SSH server... whatever the port it is running on

Paul

This List Sponsored by: Cenzic

Concerned about Web Application Security? Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.
