

Re: What is this Very Stupid DOS Attack Script?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-04/0030.html>

From: John Davis (linux0642_at_sbcglobal.net)

Date: 04/06/05

Date: Wed, 06 Apr 2005 09:35:17 -0700

To: freebsd-security@freebsd.org

Martin McCormick wrote:

- > *We have been noticing flurries of sshd reject messages in*
- > *which some system out there in the hinterlands hits us with a flood of*
- > *ssh login attempts. An example:*
- >
- > *Other than spewing lots of entries in to syslog, what is the*
- > *purpose of the attack? Are they just hoping to luck in to an open*
- > *account? The odds of guessing the right account name and then guessing*
- > *the correct password are astronomical to say the least.*
- > *Direct root logins are not possible so there is another roadblock.*
- > *<snipped for speed>*

This is probably a variant of a worm that infects the server and then spends all its time trying to log into other servers by guessing the ssh password. Once it succeeds, it attempts a compromise, and if successful, tries to break into other machines. I have read some interesting analyses on this. Apparently there are multiple variations of the worm, but they all do essentially the same thing. About the only real defense you have is to enforce a good password policy. I have taken to dropping everthing that comes from the pacific rim at the firewall. This has been helpful in reducing some attacks, though in my case, it seems like about a quarter of them come from inside the USA.

Here's a list of pacific rim IP ranges:

<http://www.okean.com/iptables/rc.firewall.sinokorea>

Here's an interesting read on one of the worm variants:

<http://www.security.org.sg/gtec/honeynet/viewdiary.php?diary=20041102>

Personally, it think people who write malicious software should be treated like terrorists because it seems to me, they are. I know it's a common defense to claim that publishing exploits is useful to IT (perhaps it is in some twisted way), but that's like saying defendants in foiled murder plots should be forgiven because they helped to expose flaws in one's personal security. It's nonsense.

--

-linux_lad

FreeBSD-Security: Re: What is this Very Stupid DOS Attack Script?

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"