

Re: Continuous medium traffic fake Syn packets

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2002-10/0013.html>

From: Philipp Schulte (pschulte@uni-duisburg.de)

Date: 10/11/02

Date: Fri, 11 Oct 2002 12:12:51 +0200
From: Philipp Schulte <pschulte@uni-duisburg.de>
To: focus-linux@securityfocus.com

Reinder P. Gerritsen wrote:

> At any given moment SYN packs of some 20 to 30 faked host adresses are
> flooding into my IP stack, at an alarming rate. (think in order of some
> 100 SYN packs per sec or something like that.) My server responds to
> that with the SYNACK reply, to the faked adres, which itself starts
> announcing it hasn't requested a session. This continues up to say about
> 5 minutes, then the IP drops its attempts, just to have "another IP"
> starting.

[...]

> My question is, is there anyone who might have a solution to split out
> the large quantity of fake requests, without taking down al the
> legitimate traffic?

OK, the first thing that comes to mind, is using syncookies.

<http://cr.yip.to/syncookies.html>

Basically you have to enable "CONFIG_SYN_COOKIES=y" and do a

```
$ echo "1" > /proc/sys/net/ipv4/tcp_syncookies
```

This should reduce the load on your machine, because it doesn't have to keep track of all the fake connection-attempts. Of course it doesn't reduce the load on your network-connecion.

The only way this problem could be really solved is when all ISPs start to use ingress-filtering (RFC2267) so no packets with faked IP-addresses would leave their network in the first place.

Phil

- **Previous message:** [Reinder P. Gerritsen: "Followup: Continuous medium traffic fake Syn packets"](#)
- **In reply to:** [Reinder P. Gerritsen: "Continuous medium traffic fake Syn packets"](#)
- **Next in thread:** [Seth Arnold: "Re: Continuous medium traffic fake Syn packets"](#)
- **Reply:** [Seth Arnold: "Re: Continuous medium traffic fake Syn packets"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)