

## Other possible protection against RST/SYN attacks (was Re: TCP RST attack)

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-04/0126.html>

---

*From:* Mike Tanca (*mike\_at\_sentex.net*)

*Date:* 04/21/04

Date: Wed, 21 Apr 2004 12:30:40 -0400

To: freebsd-security@FreeBSD.org

One other technique that might help with respect to this attack is what Cisco implemented, commonly known as the "TTL hack"

<http://www.nanog.org/mtg-0302/hack.html>

I have not tried it yet, and I am not sure of the implications. But on bgp speaking hosts, what if the following were done.

Assuming these are directly connected peers,

```
sysctl -w net.inet.ip.ttl=255
```

```
ipfw add 500 allow tcp from any to me 179 ipttl 255
```

```
ipfw add 600 deny log tcp from any to me 179
```

You would also need to cover the source ports. Not sure what the cleanest looking rule for that would be.

What nasty side effects would this cause ? If the attacker were on the same subnet this would not do anything, but you have larger problems if this is the case.

---Mike

At 07:10 AM 21/04/2004, Jacques A. Vidrine wrote:

> On Tue, Apr 20, 2004 at 01:32:40PM -0700, Dragos Ruiu wrote:

> > Also keep in mind ports are predictable to varying degrees depending on  
> > the vendor or OS, which further reduces the brute force space you have to  
> > go though without sniffing.

>

> This is exactly why I ported OpenBSD's TCP ephemeral port allocation

> randomization to FreeBSD-CURRENT (although I asked Mike Silby to commit

> it for me and take the blame if it broke :-). It will also be MFC'd

> shortly in time for 4.10-RELEASE.

>

FreeBSD-Security: Other possible protection against RST/SYN attacks (was Re: TCP RST attack)

> *Cheers,*

> ---

> *Jacques Vidrine / nectar@celabo.org / jvidrine@verio.net / nectar@freebsd.org*

---

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"