

Re: improve ipfw rules

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-02/0131.html>

From: Matthew George (*mdg_at_secureworks.net*)

Date: 02/25/04

Date: Wed, 25 Feb 2004 12:29:07 -0500 (EST)

To: Borja Marcos <borjamar@sarenet.es>

On Wed, 25 Feb 2004, Borja Marcos wrote:

> > *It is my hope that someday someone will step in and implement a similar*
> > *system under FreeBSD. But i think it requires quite a lot of work and*
> > *possibly*
> > *major rebuilding of ipfw if it needs to be integrated (which would be*
> > *great)*
>
> *¿Perhaps Snort with Flexresp? It should be able to close a connection*
> *upon detection of a signature.*
>

The difference is that snort is still packet based. You'd need to have the concept of data stream analysis in order to really implement an effective application layer protocol analysis engine.

--

Matthew George
SecureWorks Technical Operations
404.327.6339

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"