

Re: FW1 External Ruleset validation tools?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-09/0068.html>

From: ravi pina (ravi_at_cow.org)

Date: 09/10/03

Date: Wed, 10 Sep 2003 15:17:27 -0400

To: Leif Sawyer <lsawyer@gci.com>

On Wed, Sep 10, 2003 at 09:04:07AM -0800, Leif Sawyer said at one point in time:

> Hello,

>

> I'm looking for a way to audit my firewall ruleset, in

> a very specific manner.

>

>

> I've gotten reports of packets traversing our firewall

> that should not be allowed by any of the rules currently implemented.

unpossible! :)

> What is the easiest way to find out what rule line the supposed packet

> could be traversing, without logging on every single rule? This is

> interesting because it is a random occurrence, with no way to know

> when it will happen. And I dislike the idea of full logging until

> I see the violation again -- I just don't have the disk space, for one.

well, do you know the src address? if so, you could place that at the bottom of your rule base with an explicit accept and when the inspect code is built, it'll tell you where that rule conflicts.

you could also sniff the last interface the packet traversed and check the source. could it be getting in the network some other way? how do you even know that this is occurring?

> Something like an external program that would allow a crafted packet

> to be 'virtually' sent through the ruleset would be perfect.

it would, wouldn't it?

> Does such a tool exist? Preferably supporting Checkpoint FW-1 NG

not that i am aware of.

-r

SecurityFocus Penetration: Re: FW1 External Ruleset validation tools?

--

```
echo "send pgg key" | mail ravi@cow.org  
"All the world is a stage; god is filming, how are you acting?"  
-- Spirk
```

FREE Trial!

New for security consultants and in-house pros: FOUNDSTONE PROFESSIONAL
and PROFESSIONAL TL software. Fast, reliable vulnerability assessment
technology powered by the award-winning FoundScan engine. Try it free for 21 days at: <http://www>
