

RE: IPS vs Firewall

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-04/0385.html>

From: Steven Trewick (STrewick_at_joplings.co.uk)

Date: 04/28/04

To: 'Benny Late' <lvmygop@hotmail.com>, security-basics@securityfocus.com

Date: Wed, 28 Apr 2004 09:32:33 +0100

Might I suggest using the witty worm as an example ?

http://www.theregister.co.uk/2004/04/07/witty_evil_firsts/

The CAIDA analysis linked by the above story is well worth a look.

In case you have been holidaying in tibet, or a cave, the witty worm was a recent UDP borne worm that specifically targeted ISS firewall appliances and software (both corporate and personal).

When it hit a vulnerable system, it spammed 20k copies of itself to random IP addresses and then dumped 64k of random data to a random area on the hard disk of the host machine, then it repeated this cycle until the host crashed.

Now admittedly, this is most likely a 'fail closed' scenario, but it illustrates the point that firewalls are open to attack.

A long list of cisco router/firewall security related things can be found here <http://snipurl.com/608w> (securityfocus search)

Not to mention the recent kerfuffle about aincet and fairly well known TCP RST DoS vulns, some links to which can be found here :

http://www.theregister.co.uk/2004/04/21/tcp_vuln/

HTH ;-)

> *List,*

>

> *I am to give a presentation concerning IPS vs. IDS and why we*

> *have decided*

> *to implement an IPS solution. I have stuff about each of*

SecurityFocus BASICS: RE: IPS vs Firewall

- > *those, but my big*
- > *problem is going to come from my LAN/WAN group. Because I've*
- > *decided to*
- > *place the IPS outside the firewall, they have already moaned*
- > *about it and I*
- > *know they're going to bring up why we need IPS vs. Firewall.*
- > *I have stuff*
- > *about what firewalls don't look for or do compared to IPS.*
- >
- > *My question is, how would you go about showing that firewalls*
- > *or BigIP*
- > *routers can be attacked directly? For those of you*
- > *conidering IPS, can you*
- > *impart any of the knowledge gained by implementing your solutions?*
- >
- > *Many thanks,*
- > *Benny*
- >

</code>

The information contained in this e-mail is confidential and may be privileged, it is intended for the addressee only. If you have received this e-mail in error please delete it from your system. The statements and opinions expressed in this message are those of the author and do not necessarily reflect those of the company. Whilst Joplings Group operates an e-mail anti-virus program it does not accept responsibility for any damage whatsoever that is caused by viruses being passed.

joplings.co.uk

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors.

Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization.

Visit us at:

http://www.infosecinstitute.com/courses/ethical_hacking_training.html
