

Re: DoS

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2002-01/0037.html>

From: Nathan W. Labadie (ab0781@wayne.edu)

Date: 01/07/02

From: "Nathan W. Labadie" <ab0781@wayne.edu>

To: <focus-linux@lists.securityfocus.com>

Date: Mon, 7 Jan 2002 14:22:22 -0500

We've been using snort with ACID as a front-end and MySQL as the back-end with great success. ACID has a feature that allows you to export the alerts as an email, along with any custom message. For us, they look something like this:

---snip---

The following logs are in the EDT timezone (GMT-5). Please investigate and report back.

Thank you.

Nathan W. Labadie
Sr. Security Specialist
C&IT Security Office
Wayne State University
<http://security.wayne.edu>

Generated by ACID v0.9.6b20 on Mon January 07, 2002 08:36:42

#1-3916] [2002-01-07 08:04:34] 216.47.152.201:722 -> xxx.xxx.xxx.xx:111

[arachNIDS/24] RPC portmap request ttdbserv

#1-3921] [2002-01-07 08:08:27] 216.47.152.201:768 -> xxx.xxx.xxx.xx:111

[arachNIDS/24] RPC portmap request ttdbserv

#1-3951] [2002-01-07 08:08:31] 216.47.152.201:769 -> xxx.xxx.xxx.xx:111

[arachNIDS/24] RPC portmap request ttdbserv

---snip---

More information can be found here:

<http://www.snort.org>

<http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html>

On Monday 07 January 2002 11:23 am, you wrote:

> *I'd like to know if there is anykind of software that can besides*
> *detecting DoS attack also report via any tool to Administrator and or*
> *ISP Abuse Email*

--

Re: DoS

SecurityFocus Linux: Re: DoS

Nathan W. Labadie | ab0781@wayne.edu
Sr. Security Specialist | 313/577.2126
Wayne State University | 313/577.1338 fax
C&IT Security Office: <http://security.wayne.edu>

- ***Previous message:*** [José Luis Domingo López: "Re: vlock with md5 password support"](#)
- ***In reply to:*** [Aleksey Domorad: "DoS"](#)
- ***Next in thread:*** [Andrew Hatfield: "RE: DoS"](#)
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)