

## RE: intrusion detection system

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-10/0033.html>

---

**From:** Ozdemircili Ozgur NMI Civ TR 425 ABS/SGST (*Ozgur.Ozdemircili\_at\_izmir.af.mil*)

**Date:** 10/19/04

To: "'Tomas Pluskal'" <plusik@pohoda.cz>

Date: Tue, 19 Oct 2004 15:46:52 +0300

Great job Thomas,

I am reading and at the same time making a news out of it for the Turkish FreeBSD scene ;).

By the way I have discovered the relation where you got all your "inspiration" for your project ;P Legos of course.

Keep up the good work.

Ozgur Ozdemircili

425 SG M.A.S

DSN: 675-3236

-----Original Message-----

From: owner-freebsd-security@freebsd.org

[mailto:owner-freebsd-security@freebsd.org] On Behalf Of Tomas Pluskal

Sent: Monday, October 18, 2004 4:19 PM

To: freebsd-security@freebsd.org; freebsd-hackers@freebsd.org

Subject: intrusion detection system

Hello to all,

I have implemented a new type of intrusion detection system for my Master thesis. I would like to announce this information, in case anyone would be interested in this research.

The IDS system is designed as a kernel module for FreeBSD 5.2. It is inspired by the SpamAssassin program, which detects spam by applying a set of tests to every email message and counting a sum of point score generated by each test. My IDS system applies a set of tests to every running process in the OS and counts its score generated by the tests. Therefore, the purpose of the IDS is not to monitor the network traffic, but rather to monitor the process activity.

The current system status is a "working prototype" – it is more a research than a real IDS.

FreeBSD–Security: RE: intrusion detection system

If you are interested in this, please read the details here:

<http://plusik.pohoda.cz/thesis/>

Thanks,

Tomas

---

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"

---

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"