

New Open Source Intrusion Detector Suricata Released



44

Posted by timothy on Thursday December 31, 2009 @05:42PM from the open-but-not-promiscuous dept.

richrubble writes

"The [OISF](#) has released the beta version of the [Suricata](#) IDS/IPS engine: The Suricata Engine is an Open Source Next Generation Intrusion Detection and Prevention Engine. This engine is not intended to just replace or emulate the existing tools in the industry, but will bring new ideas and technologies to the field. This new Engine supports Multi-Threading, Automatic Protocol Detection (IP, TCP, UDP, ICMP, HTTP, TLS, FTP and SMB!), Gzip Decompression, Fast IP Matching and coming soon hardware acceleration on CUDA and OpenCL GPU cards."



You may like to read:



[The Twelve Most Tarnished Brands In Tech](#)

[Ask Slashdot: Which Apps Aren't Available on Linux?](#)
[What the Linux Desktop Really Needs To Challenge Windows](#)
[Four More Tech Bloggers Are Switching to Linux](#)
[Rust Will Save Linux From AI, Says Greg Kroah-Hartman](#)
[Someone Forked systemd Over Its New Birth Date Field](#)
[Submission: New OpenSource IDS/IDP \(Beta\) Suricata Released](#)

[What Would Have Entered the Public Domain Tomorrow?](#)

FEATURED CONTENT

Compare the top business software of 2026



Did you know Slashdot offers the world's largest business software comparison directory?

Find the right software tools for you or your business using the Slashdot Business Software Comparison engine. Slashdot's comparison engine contains over 100,000 software products, and over 4000 categories. Filter by pricing, features, integrations, user reviews, and more.

Compare Now

New Open Source Intrusion Detector Suricata Released

Archived Discussion

Load All Comments

8 Full 20 Abbreviated 16 Hidden

Comments Filter: **All** Insightful Informative Interesting Funny

The Fine Print: The following comments are owned by whoever posted them. We are not responsible for them in any way.

Innovation (Score:5, Insightful)

by Reason58 (775044) on Thursday December 31, 2009 @05:49PM (#30610198)

This engine is not intended to just replace or emulate the existing tools in the industry, but will bring new ideas and technologies to the field.

Sweet! What are some examples of things this does that no other solution provides?

[Share](#)

7 hidden comments

Promising (Score:1) Hardware acceleration with CUDA makes this product worthwhile to watch.**Re:Promising (Score:5, Informative)**by FooAtWfu (699187) on Thursday December 31, 2009 @06:14PM (#30610438) [Homepage](#)

That is interesting to me. CUDA can easily provide parallelization of bulk mathematical operations, but it's notoriously weak with conditional logic. Are they doing a whole lot of math on the side -- perhaps with some fancy anomaly-detection algorithms that work by clustering packet attributes in multidimensional spaces, or approximate nonnegative matrix factorization, or such?

[Parent](#) [Share](#)
Re:Promising (Score:5, Informative)

by PatDev (1344467) on Thursday December 31, 2009 @06:38PM (#30610600)

Maybe I'm missing something, but as someone who has working with the techniques referenced in the parent post - I'm not sure where the funny mod came from. Both clustering packet attributes and nonnegative matrix factorizations could be used for anomaly detection. And as someone who has also worked on CUDA a good bit, I think both of those problems have solutions that fit CUDA's concurrency model.

I get the impression that the mods saw big words and assumed this was a joke about buzzwords, but in fact that's a reasonable approach to this problem.

[Parent](#) [Share](#)

Re: I get the impression that the mods saw big words and assumed this was a joke about buzzwords, but in fact that's a reasonable
1 hidden comment

Re: To be fair, I think this is from 1994. You gotta give Gibson some slack on that one.

Re: If his writing had any redeeming qualities, he'd have earned some slack... but I've just found him to kinda suck. His

Re: I suppose that ranks as "funny" because the extent of the CUDA parallelism is... probably just to accelerate the aforementioned gzip

Re: All your GPU are belong to us.

huh (Score:4, Insightful)

by dropadrop (1057046) on Thursday December 31, 2009 @05:54PM (#30610236)

While there is some information available on the site, it's still pretty sparse. Is this a whole framework? They refer to engine, but do they mean a detection engine or also a correlation engine? This area really needs more open source innovation, commercial solutions are ridiculously expensive for small / mid sized companies, and the only "complete" IDS option I know of for the moment is Ossim (which has extremely lacking documentation).

[Share](#)

1 hidden comment

Re: From the INSTALL doc: Suricata is compatible with standard Snort rulesets. A sample standard configuration file can be found in the Suricata

Dangerous (Score:2, Insightful) The features look indeed promising. On the other hand, the more complicated an IDS/IPS gets, the more likely it**On first glance (Score:4, Funny)**

by joeffies (529536) on Thursday December 31, 2009 @06:23PM (#30610504)

I thought that the "Open Source Intrusion Detector" spotted intrusions of open source software in the company. I'm sure that Microsoft would have loved to have one of those for the Windows 7 USB/DVD download tool.

[Share](#)

1 hidden comment

Re: Give them time, Maybe it will be part of SP1b.

More info (Score:4, Informative)

by methamorph (950510) on Thursday December 31, 2009 @06:47PM (#30610662)

Since the original site is slashdoted some more info can be read [here](#) [seclists.org]

[Share](#)

Are these useful yet? (Score:1, Interesting) I'm not trying to be a troll here or anything, but are IDS/IPS systems actually worth while? We started
1 hidden comment

Re:Are these useful yet? (Score:5, Interesting)

by Martin Blank (154261) on Thursday December 31, 2009 @07:08PM (#30610806) Journal

You are. Your IDS was incredibly poorly-tuned, a very common problem in IT. First guideline: turn off signatures for anything that you're not running. It makes no sense to watch your inbound traffic for Windows signatures if you run Apache on RHEL. If all you have are web servers and they do only HTTP, there's no reason to watch for SMTP.

Making the move to IPS is always tricky. You have to figure out what level of false positives you're willing to accept. If it's zero, well, you don't need an IPS. But odds are that you will come across some strange but innocuous traffic that the IPS doesn't like, and it trips a rule and blocks the traffic.

In addition, you need to get the hardware for the solution. A server-based Snort solution works well for low-bandwidth scenarios, but at most hosting providers, you need a dedicated appliance solution built on ASICs. If you like Snort, you go to Sourcefire. Otherwise, you find solutions from McAfee (Intrushield), Tipping Point, IBM, etc. They have boxes that scale into the gigabit-per-second range, with latencies under 1ms in most cases, and there are a few true-10Gbps solutions out there now. Yes, they can be quite expensive, but the low-end systems (essentially highly-tuned servers) can start at as low as a few thousand dollars.

But in any case, rule tuning is an ongoing item, and anyone that tells you that an IDS/IPS will reduce your time requirements is probably trying to get you to sign a contract. It *can* reduce overall time requirements by alerting you early in the attempt to compromise a system and save you all the time of recovery, but that is not a certain thing.

[Parent](#) [Share](#)

Re: Say it's HTTP only. What can they do for you?

Re: They can protect in situations involving unpatched vulnerabilities, actually. In many cases, once a vulnerability is publicized, a

Re: A lot of companies don't know enough to understand security, some well dressed salesman comes through the door and tells them

Re: Try the sguil console, and you'll be happier with handling alerts. It presents the data from full content pcaps, Snort alerts, and session data,

Apparently it can't stop a DoS (Score:3, Funny)

by istartedi (132515) on Thursday December 31, 2009 @07:03PM (#30610772) Journal

If it were really that good, it would sniff the referrer on all the HTTP requests and throttle Slashdot.

[Share](#)

Re: I'm sure this was meant in jest, but it doesn't work that way. They could instantly drop every packet in a DDoS attack and it wouldn't matter.

Re: I did lash out a bit there. Now that you mention it, recognizing the referrer would most likely be of marginal benefit at best. You have to
1 hidden comment

Re: No, it would help a lot... Most of the bandwidth from being hit by web requests is actually outbound traffic when the server actually

Editors? (Score:2) What's with all the caps, exclamation marks, spelling etc in the summary? As it is, it wouldn't even pass any sane spam filter:

Does it page their sysadmin... (Score:2) ...because their site is failing to load, looks like the DB server or connection is fek'd: Database Error:

Multi-Threading is evil (Score:1) Multi-threading is insecure in itself. Stop sharing, start merging.

Related LinksTop of the: [day](#), [week](#), [month](#).

- 244 Ask Slashdot: Which Apps Aren't Available on Linux?
- 231 What the Linux Desktop Really Needs To Challenge Windows
- 197 Four More Tech Bloggers Are Switching to Linux
- 171 Rust Will Save Linux From AI, Says Greg Kroah-Hartman
- 170 Someone Forked systemd Over Its New Birth Date Field

NEXT



[What Would Have
Entered the Public
Domain Tomorrow?](#)

331

PREVIOUS



[The Twelve Most Tarnished Brands In Tech](#)

430

Slashdot

Get more comments

44 of 44 loaded

Archived Discussion

Submit Story

"I may be synthetic, but I'm not stupid" -- the artificial person, from [_Aliens_](#)

[FAQ](#) [Story Archive](#) [Hall of Fame](#) [Advertising](#) [Terms](#) [Privacy](#)
[Statement](#) [About](#) [Feedback](#) [Mobile View](#) [Blog](#)

Copyright © 2026 Slashdot Media. All Rights Reserved.

[Cookie Choices](#)

☒ Do Not Sell or Share My Personal Information