

Processing time and IDS traffic

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2003-08/0046.html>

From: Eric Knight (eric_at_swordsoft.com)

Date: 08/11/03

To: <focus-ids@securityfocus.com>

Date: Mon, 11 Aug 2003 15:10:44 -0600

Greetings,

I've been working on a 'universal framework' application for collecting, analyzing, charting, log management, control, etc. for "anything goes" (forensics, anti-virus, IDS, firewalls, etc.) in a client/multi-tiered server environment. At the moment, its all for Microsoft Windows. The project has gone wonderfully, and I've been working on expanding the horizons of my programs to include the majority of popular tools as it was intended.

One of the external applications I've been integrating is Snort, mostly because its reviews were outstanding and readily available to work with. I created a test environment using Snort that generates about 1 error every second and I've let it collect 75,000 reported elements (roughly 20 megabytes of logs.)

What I did was parse the logs into XML records and arranged them into a nice pleasant tree sorted by error type, origin, destination, protocol, port, etc. and collected totals by severity, time, total attacks, traffic, etc. Then displayed them in a tree structure that's easy to search through and make digested reports with. Not sure if its the best arrangement for all uses, but it seems to be certainly friendlier than the flat lists I normally see.

The problem is, 75,000 records takes about 10 minutes for my test computer to parse, sort and process. It isn't a fast box (Duron 750/256meg ram) and its mostly overburdened anyway running Snort + development environment in debug, but it raised my eyebrow because the code is fairly optimized (for Java.) However, I'm disappointed that it isn't next-to-instant (because, well, I'm -always- disappointed when something isn't next to instant. *grins*) I'm already considering re-doing the whole process in C++, but I'm wondering what the process time other people have for similar calculations, how many records people usually get on average/day from a typical, strategically placed IDS system and what people get from a IDS system located on an exposed workstation (personal firewall?) I really have no idea what performance I'm targeting for.

SecurityFocus IDS: Processing time and IDS traffic

Thanks for your time,

Eric Knight

Captus Networks – Integrated Intrusion Prevention and Traffic Shaping

- Instantly Stop DoS/DDoS Attacks, Worms & Port Scans

- Automatically Control P2P, IM and Spam Traffic

- Ensure Reliable Performance of Mission Critical Applications

Precisely Define and Implement Network Security and Performance Policies

**FREE Vulnerability Assessment Toolkit – WhitePapers – Live Demo

Visit us at: <http://www.captusnetworks.com/ads/31.htm>
