

Re: NIPS Vendors explicit answer

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2004-04/0029.html>

From: christian graf (*chr.graf_at_gmx.de*)

Date: 04/19/04

To: focus-ids <focus-ids@securityfocus.com>, Toby Kohlenberg <toby.kohlenberg@intel.com>
Date: Mon, 19 Apr 2004 17:10:45 +0200

Hi,

its amazing. Normally each vendor cries "hello me" if he thinks his product can do anything quite well.

However, it seemed that no vendor is able to speak clearly regarding "anomaly detection".

Below is the mail I have sent a few days ago.

If still no vendor will answer, what should I think? That the products are weak in anomaly detection or not even one guy is capable in answering it?

Is only Toby interested in HOW the products of today really use anomaly detection? No one else?

christian

Am Mi, den 07.04.2004 schrieb christian graf um 16:07:

> *Hi all,*

>

> *there are many "imaginable" ways for a NIPS to detect traffic, which should be blocked. Patternbased, data-mining-methods (to even guess into encrypted traffic – see <http://www.phrack.org/show.php?p=61&a=9>, RFC-anomaly, protocol-based anomaly (layer 4 flows, new listening services, new protocols,..), statistical methods, ... Those methods will most-likely combined with neuronal-networks, back-propagation-networks, state-machines and at least with some voodoo called heuristic.*

>

> *My goal is here, do get a feeling for "unknown / zero day" exploits. One of the best places to stop them is probably the host itself (lids-project or one of many HIPS, AV-products and even some nice HIDS with IPS functionality). But here I want the NIPS functionality only. And I absolutely do not want to start a discussion IDS versus IPS. Those are two separate functions and can't be replaced against each together.*

>

> *My questions is, how the vendors would have detected and blocked a prior unseen SINGLE successful attempt which exploits <http://www.cert.org/advisories/CA-2001-06.html> (Automatic Execution of Embedded MIME Types) and a SINGLE successful hack*

SecurityFocus IDS: Re: NIPS Vendors explicit answer

- > using <http://www.cert.org/advisories/CA-2001-12.html>
- > (Superfluous Decoding Vulnerability in IIS) . Both are
- > nimda-related and are just a generic example.
- >
- > Please do not highlight, that your product would have captured the tftp
- > (69/UDP) traffic to the IIS-Server NOR that the infected clients will
- > start scanning for vulnerable IIS-Servers! This traffic is all
- > worm-related and thats easy to detect anyway.
- > I do want to checkout how clever the systems may handle an unknown,
- > single but successful exploit. Most important when (at which step) the
- > exploit is detected and stopped (when the backdoor triggers, shellcode
- > seen, new ports are listening, unseen new traffic, ...)
- > Even target-based intelligence will not really help in my question, as
- > I'm talking to the unseen exploit ONLY -and targetbased are all already
- > seen vulnerabilities. Ups, and checking for RFC-Compliance wont't help
- > either (hm, is declaring a binary-executable as audio/x-wav against the
- > RFC..)
- >
- > In the answer I would like to see the following points included:
- > 1) would the system have captured/blocked a "unique, prior unseen"
- > infection by a user who's mail-system was rendering the malicious mail?
- >
- > 1a) you may include the behaviour regarding the
- > directory-traversal-exploit for IIS.
- >
- > 2) if the system could block/detect it, how was the system teached to
- > get aware of the exploits?
- >
- > 3) how long took it to teach the system?
- >
- > 3a) Once the first successful exploit was done (and not blocked), the
- > system will detect "malicious" traffic or even a newly installed
- > backdoor.
- > How fast can the system be configured to block further similar hacks?
- > Is this reconfiguration done automatically?
- > How can the system be sure that no legacy traffic is blocked
- > automatically?
- >
- > 4) what will happen, if during the teaching-phase the infection will
- > happen? (So the exploit got learned and maybe classified as normal)
- >
- > 5)How will the anomaly IDS/IPS act during the absolutely normal drift of
- > any network (new servers, new services, new FW-rules, ..)?
- >
- > 6) As anytime, the system may be tuned to extreme: If measured by
- > ROC-graphs (as seen and discussed in the papers from C.C. Micael, Anup
- > Ghosh "Two-state approaches to Program-based anomaly detection" or in
- > the paper from Stefanie Forrest and Thomas A. Langstaff "A Sense of Self
- > for Unix Processes". The ROC-graph in general shows the relationship
- > between the false-positives-rate and the successfully-detected rate.
- > I'm interested if the system is tuned to report minimum false positives,

