

Re: Dynamic Firewall/IDS System

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-09/5596.html>

From: Karsten W. Rohrbach (karsten@rohrbach.de)

Date: 09/17/01

Date: Mon, 17 Sep 2001 15:19:45 +0200
From: "Karsten W. Rohrbach" <karsten@rohrbach.de>
To: ark@eltex.ru

ark@eltex.ru(ark@eltex.ru)@2001.09.17 16:39:40 +0000:

- > *Ok, some thoughts about event handling software.*
- >
- > *First to say i am definitely against any "super-duper-dynamic-countermeasures".*

that's the same with me, but i see the need for a system to automate some of the daily net/abuse/system admins tasks.

- > *No policy change should appear without manual review and approval.*
- > *I am the person that controls my firewall directly and there should be no*
- > *ways of indirect control.*

policies won't change themselves. i rather mean to employ policies defining what measures the output handlers are allowed to take and what input conditions have to be met to trigger a reaction. thus, prevent self-blocking the whole system and so on...

- >
- > *It sounds extermely cool, i know, but it simply does not worth problems that*
- > *appear. I mean there are many known and even more unknown yet ways to cause*
- > *'false positive' and DoS vital or just important things for you and many ways*
- > *to obtain information bad guys need regardless of if such a system is installed.*

it is the intent to set certain thresholds, combinations or whole scenarios for triggering a countermeasure. i do not want to create a stupid dumbfire firewall remote controller. i could have done this in a perl script, already, if i wanted it so badly ;-). scifi firewalls on linux also had this feature, but for me it appears too limited (just one host) and it also had several other (operational) problems in the field.

- >
- > *There are some other things to do, though. A small network gets tens of*
- > *security-related events daily, the number for big one is thousands, which*
- > *is almost impossible to handle manually just reading logs. But we have to.*

FreeBSD–Security: Re: Dynamic Firewall/IDS System

yup and joining the logs into an event handling engine, correlating them, perhaps using templates or the like and putting them into a categorized log storage (whatever it may be) strongly helps you with that task. a small network (one ip address) 194.162.162.209/32 sometimes gets several thousands of alerts a day.

- >
- > *Requirements for tool that should be able to do the job are simple:*
- >
- > *the thing should not be too complex. get offender's ip address, some mnemonic*
- > *event type as command line – and detailed info like log lines from stdin.*
- > *Do whois lookup then and record network owner and administrative contacts.*
- > *This is how we fill our database.*

these are different processing steps which should be done in a modularized setup therefor. this cuts down complexity of each module to a minimum while giving us the most flexibility.

- >
- > *What can we do than? Retrieve useful information.*
- >
- > *"automatic mode": when event occurs, send an _informative_ notification to admin,*
- > *including:*
- >
- > *all details for this event*
- > *last n similar or relevant events*
- > *last n events recorded for this host*
- > *last n events recorded for networks owned by the same organization*

this is logging, way like acid does with snort logs.

- >
- > *providing a good template for a message to abuse service*

this is also logging based.

- >
- > *"manual mode": any kind of information retrieval on demand.*

this would be some kind of query interface for the logging database, then. i am thinking about separating event priorities in handling right at the beginning. this creates a certain scalability. i just had a discussion with yoann from the prelude project, and it appears to me that separating several alert 'classes' into different priority queues on a processing node makes sense. alerts that need to be transformed for database storage and so on could spill over to another node which does the conversion to idmef or similar formats for incident storage. timeliness in reacting to what ever events come in is a premium.

- >
- > *Someone can even write a fancy (say, tk ;) GUI for that to update database,*

FreeBSD-Security: Re: Dynamic Firewall/IDS System

- > *keep track on abuse responses and tickets and to help you know if you*
- > *really did perform any actions on this or that incident or you just were too*
- > *lazy that day.*

a built-in ticketing system would rock for the categorized logging database, yes.

- >
- > *Anyone willing to implement? I'm afraid i am too busy now to write code for*
- > *that thing :(*

oh, i would be happy to have you on board with those ideas.

/k

--
> Sex is one of the nine reasons for reincarnation ... the other eight
> are unimportant. --Henry Miller
KR433/KR11-RIPE -- WebMonster Community Founder -- nGENn GmbH Senior Techie
<http://www.webmonster.de/> -- <ftp://ftp.webmonster.de/> -- <http://www.ngenn.net/>
karsten&rohrbach.de -- alpha&ngenn.net -- alpha&scene.org -- catch@spam.de
GnuPG 0x2964BF46 2001-03-15 42F9 9FFF 50D4 2F38 DBEE DF22 3340 4F4E 2964 BF46
Please do not remove my address from To: and Cc: fields in mailing lists. 10x

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message

- application/pgp-signature attachment: stored