Attack detector

The «Attack detector» module is placed in the «Security» menu. This module is designed to enabling, setting up and configuring the open source IPS/IDS system - Suricata that is used in the ICS. The system was designed by Open Information Security Foundation in 2009 year. Intrusion Prevention System (IPS) is a network security system, that can detect security breaches and attacks. IPS is monitoring network traffic in real time and can use different methods to prevent breaches - connection hangout, logging of known signatures and let it pass. IPS can also deframent packages, remixing packages to protect system from packages with altered SEQ and ACK numbers. The Suricata system is multitask, so it is high-load and can manage up to 10Gbit traffic channel at the regular hardware and other, including the Snort rules format. At the main page of the module you can see it's status, the «Disable» button (or «Enable», if it's already disabled) and last log messages.

Settings

For using the attack detector signature database correctly in this tab you should locate objects (networks, servers and ports) that should be examined. Here you can specify internal and external networks, servers network addresses ranges, and also the ports that are in use. By default, there are values that allow attack detector to launch properly. To change the default configuration you should open the drop-down list in the cell and choose values from the address ranges, that is known to ICS. Or you can type the required value manually in the cell. You can use domain names (like host.ru), ip-addresses (like 192.168.1.1), ip-address with prefix (like 192.168.1.1/24), ip-address:mask (like 192.168.1.1:255.255.255.0), ip-address range (like 192.168.1.1-192.168.1.254), user, group, internal, external, VPN, OpenVPN, Wi-Fi networks and other object that ICS can manage in the cells «networks» and «servers». For the «ports» cell port number (like 25, 100), port ranges (like 1000-2000) and object defined into ICS are allowed. You can also use ports excluding, for example, «!80» for the «SHELLCODE-ports» cell. You must add the object «Local networks» in the «External networks» field for traffic to be analyzed.

Rules

In this tab you can see possible database for attack detector module. There are three rule databases: the rules from the snort.org site, recompiled rules from the snort.org and Emerging Threats rules. Each base contains a set of downloadable files, and each file contains a set of rules, grouped according to the security target. For a rule set to work, it is necessary that the base would be downloaded (you can read about this in the «setting up updates»), if the base wasn't downloaded, next to every file you would see the «Isn't downloaded» sign. If the base was downloaded, you can choose either to use all the base entirely, marking the «apply» checkbox. Or, if you want to apply a specific file, or exclude a specific file, you can mark it with «apply» flag itself. Next to every file you can see the amount of rules that it contains. In the right top corner you can see search - it works both with names and amount of rules in a file. To look through the rules and to choose an action you should click on the filename, and the new window with a table will be open. The table contains rule id

- the rule number; priority - the value of a threat; warning - the description of an attack; classification - contains information about what class that attack is in; action - defines what would be done is the attack is detected (alert - to log an event and let it pass by, drop - to drop package, allow - let it pass; reject - destroy a package and notify sender about the event); turning the rule on/off fields.

Update settings

There are 2 companies that are active developing attack prevention systems - Sourcefire and Emerging Threats. To download bases «Rules from the snort.org» and «Recompiled rules from the snort.org», you should:

- Sign up in the Snort.org site (and to subscribe to rules update if necessary),
- Get the Oinkcode for rules download (is placed in the private dashboard at the snort.org site),
- Enter this code in the «Oinkmaster code» field,
- Sign the flag that is next to this field, if you really had subscribed to the rules updates),
- Save.

You can download rules using this code only. Pay attention to the difference between the privileges of the regular signed up user from the one who subscribed to updates. After successful downloading of the rules of this developer, they will be shown in the «Rules» without «Isn't download» sign.

For downloading the «Emerging Threats rules» database you can just sigh the «Install Emerging Threats rules» flag and save changes. Another parameter that can be set up in this tab is an opportunity to check rules updates that was downloaded every day. By default it is signed, but you can change this if necessary. After everything is set, you can push the «Update now» button.

Log

It shows all system messages of the module with date and time. The log is divided to pages, you can navigate it using «next» and «previous» buttons, or you can enter page number manually. Log entries are colored depending on the message type. Regular messages are white, system status messages (turning on/off, user login) are green, warnings are yellow and errors are red. In the right top corner you can see the search line, and also a calendar to choose a period of time to show messages of. By default the log is showing events of the current date. You can save the log into a file if necessary, using the «Export» button or delete log entries of the specified period of time, using the «Delete log» button.