AANVAL 8 INSTALLATION AND SENSOR SET-UP GUIDE

AANVAL 8

With Aanval 8, Tactical FLEX, Inc. continues to set a new bar with performance upgrades, enhanced threat detection, and new automation features. The best performing Snort, Suricata, and Syslog Intrusion Detection, Correlation, and Threat Management console on the market is now better than ever.

While delivering complete end-to-end network visibility, Aanval 8 boasts dozens of new features including HTML5, IPv6, Direct Unified2 Support, Threat Levels Displays, Global Heat Maps, Syslog Enhancements, New Automation Systems, and a complete re-write of nearly the entire code-base to make it our most stable and advanced version of Aanval yet.

Aanval is the solution for IT security professionals demanding a proven security and network operations tool with a strong focus on intrusion detection, coupled with robust log management and SIEM capabilities.

CONTENTS

DOWNLOAD AND INSTALLATION

Aanval has been designed from its core outward to support a broad variety of installation environments and be as simple to install as possible.

Downloading and installing Aanval takes only minutes to accomplish. Designed to work with all current Linux, UNIX, and Mac OS X flavors, you can quickly be up and running.

SOFTWARE REQUIREMENTS

Each of the following requirements should be satisfied prior to starting your Aanval installation. Testing for any additional requirements will be performed during the installation process.

REQUIREMENT	REASONING	REFERENCE
		The most current versions of these packages can be found at the following links
Operating System	Aanval will install on all major Linux and UNIX distributions, including Mac OS X	Popular operating systems have been Linux-based CentOS and Ubuntu variations CentOS: http://www.centos.org/modules/tinycontent/index.php?id=15 Ubuntu: http://www.ubuntu.com/download
IDS Engine	Aanval requires an Intrusion Detection System (IDS) for monitoring and retrieving network traffic and packets	Snort: https://www.snort.org/downloads Suricata: http://oisf.net/suricata/
Apache	Aanval will require an Apache web server capable of serving PHP scripting	http://httpd.apache.org/download.cgi
PHP	Aanval will require PHP for server-side scripting	http://php.net/downloads.php
PERL	Aanval uses PERL to launch the PHP scripts in wrapper fashion	https://www.perl.org/get.html
MySQL	Aanval will require a MySQL database for event processing and storage	http://www.mysql.com/downloads/
Wget	Aanval uses Wget to download external data like console updates and signatures.	http://www.gnu.org/software/wget/ Users can also use their OS' built-in installation or update commands to obtain the utility
Unzip	Aanval uses Unzip to decompress downloaded data like console updates.	https://oss.oracle.com/el4/unzip/unzip.html Users can also use their OS' built-in installation or update commands to obtain the utility

PREPARATION

1. Users can store Aanval in the root of the web server directory. Users can also create a directory within the web root directory for Aanval; issuing the following command from the web root directory creates a directory to store Aanval:

```
mkdir aanval
```

2. Change to the new aanval directory (if you selected to create a new directory; otherwise, change to the root of the web server directory, which is generally **/var/www/html**). Issuing the following command will download Aanval:

```
wget download.aanval.com/aanval-8-latest-stable.tar.gz
```

3. Uncompress Aanval. The following command will uncompress and extract the Aanval package contents into the current directory:

```
tar -zxvf aanval-8-latest-stable.tar.gz
```

4. Create a MySQL database for Aanval. Using the MySQL administrative tools, the following command will create the database named **aanvaldb**:

```
mysqladmin create aanvaldb
```

INSTALLATION

1. Direct your web browser to the location of Aanval, where you should be presented with the Aanval End-User-License-Agreement.

2. After reading the EULA, click **I agree** to continue.

3. Aanval will then perform environmental and compatibility tests. Ensure all tests are successful; otherwise, resolve the problems listed and click **Continue**.

4. Direct Aanval to the location of the newly created Aanval database by providing values for the following:

   Database Server (IP or hostname of the database server)

   Database Name (this should be **aanvaldb**)

   Database Username

   Database Password (in some instances this value may be blank)

5. Submit the settings for testing. Once confirmed, a **Success** message will be provided if everything is correct; otherwise, return and resolve any problems. Click **Continue**.

6. The Aanval installation process will take place and is relatively quick. This process creates and loads all required database tables as well as provisions the console for initial usage. When complete, click **Continue** to proceed.

7. Once you have successfully installed Aanval, you will be presented with the default username and password of this Aanval console as well as the instructions to start the Aanval Background Processing Units (BPUs).

8. Log in to Aanval using the credentials provided on the previous screen. Typically these will be a username of **root** and a password of **specter**.

STARTING THE BPUS

1. The Aanval Background Processing Units (BPUs) are responsible for importing events, processing actions, and ensuring the console functions properly. You must start the BPUs in order for the console to operate correctly, and it should be done with root or equivalent privileges. To start the BPUs, change into the **/apps** directory of your Aanval installation and run the following command:

```
perl idsBackground.pl -start
```

ADDING AN IDS MYSQL SENSOR

An IDS MySQL sensor is an IDS engine that uses Barnyard2 to send its event logs to a local or remote MySQL database, and from which Aanval reads and imports its logs. Aanval's Sensor Management Tools (SMTs) are not necessary for this mode of event importing; however, users can continue to set up and use them for advanced sensor and signature management functions.

1. Inside the Aanval console, go to the **Configuration** menu by hovering over the user login at the top-right of the screen. Under **Event Import Options**, go to **MySQL Module** > **Settings**.

2. Check the **Enabled** box at the top and then continue to enter the location and user information of the IDS MySQL database where Barnyard2 would be sending IDS logs. Click **Update** to commit the changes. Users will receive two Success messages for the database connection and name; resolve any issues.

Note: The **Database Trimming** option, when selected, will automatically remove the oldest events from the IDS database once the threshold is met. Enabling this feature is recommended and can assist to prevent the MySQL disk from running out of disk space.

3. From the menu directory display in the upper-right of the screen, go back one menu by clicking **Configuration**, and then under **Event Import Options**, select **MySQL Module** > **Sensor Configuration**.

4. On the left of the screen will be displayed all IDS sensors that are reporting or have reported to the database to which Aanval is connected. If no sensors appear, ensure Aanval is connected to the correct database and that Barnyard2 has the permissions to access and is properly reporting to the proper database. Select the desired sensor from the left, check the **Enabled** box, enter relevant sensor information (name, description, location, etc.), and click **Update** to commit the changes. Repeat these steps for any additional sensors.

5. Ensure the **Sensor Permissions** at the bottom of the menu are enabled for each user that will be viewing and managing the events for the given sensor; otherwise, events will not display or be available on any menu.

Aanval is now connected to the IDS database and the sensor is enabled. New IDS events should be imported and displayed at the Home menu or one of the Live event menus. If events are not being displayed, check the following items:

IDS engine: ensure the engine is running in daemon mode and that network traffic is flowing to it.

IDS signatures: ensure signatures are enabled that match corresponding network traffic.

Barnyard2: ensure the process is running in daemon mode.

If events still aren't being imported and displayed, check the Aanval wiki Troubleshooting Guide for further assistance: http://wiki.aanval.com/wiki/Aanval:Troubleshooting_Guide

INSTALLING AND STARTING THE SMTS

The Sensor Management Tools (SMTs) enable the management of local or remote IDS engine services and signatures from within Aanval. They can start and stop IDS engines, auto-update and manage IDS signatures, and with Aanval 8 also allow the console to directly import Unified2 files and network events.

The SMTs are found within the **/contrib/** directory of any Aanval installation.

Note: for MySQL-based IDS sensors, utilize the SMT or **/smt** package. For Unified2-based sensors, utilize the SMT2 or **/smt2** package. Both packages are found within the **/contrib/** directory. Each package is specifically designed for its type of sensor; the SMTs designed for MySQL-based IDS sensors will not work with Unified2-based sensors, and visa versa.

1. On the same machine as the sensor(s), create a directory to store a copy of the SMTs and copy the contents of the **/contrib/{smt/ or smt2/}** directory into this location. Users commonly do this off the root directory with the following command:

   ```
   mkdir /smt
   ```

2. To then copy the SMT contents to the new directory, enter the following command:

   ```
   cp {/your/aanval/install}/contrib/{smt/ or smt2/}* /smt/
   ```

3. Edit and configure **conf.php**, adding the proper paths (**$consoleHost**, **$consoleHostPath**, etc.) and values (**$id**, **$confSnort**, **$rulesSnort**, etc.), and save the file. **Note:** for Unified2-based sensors where the SMT2s are utilized, only the values of SMT ID (**smtID**) and the location of Aanval (**aanvalURL**) are required; the additional details of the IDS sensor configuration file and rules paths are provided in the Unified2 Sensor Management menu of Aanval.

4. Test the SMTs by issuing the following command in the **/smt** directory:

   ```
   php smt.php
   ```

5. Resolve any communication or configuration errors, and then start the SMTs with the following command:

   ```
   perl idsSensor.pl -start
   ```

6. The SMTs can be stopped using the following command:

   ```
   perl idsSensor.pl -stop
   ```

ADDING AN IDS UNIFIED2 SENSOR

An IDS Unified2 sensor is an IDS engine that uses Aanval's Sensor Management Tools (SMTs) to directly import its event logs. Aanval's SMTs can further be utilized for IDS sensor and signature management.

1. Inside the Aanval console, go to the **Configuration** menu by hovering over the user login at the top-right of the screen. Under **Event Import Options**, go to **Unified2 Module** > **Sensor Configuration**.

2. To add a new sensor, click the **+** button at the upper-right of the menu.

3. Select the new sensor, check the **Enabled** box at the top, continue to enter sensor information (**SMT ID**, name, description, location, etc.) and click **Update** to commit the changes.

4. Ensure the **Sensor Permissions** at the bottom of the menu are enabled for each user that will be viewing and managing the events for the given sensor; otherwise, events will not display or be available on any menu.

5. From the menu directory display in the upper-right of the screen, go back one menu by clicking **Configuration**, and then under **Event Import Options**, select **Unified2 Module** > **Sensor Management**.
6. Select a sensor from those listed on the left of the menu and click its **Configuration** (gear icon) button.

7. Provide the paths and values to the following:

   Configuration File (location of the snort.conf or suricata.yaml file)

   Unified2 Path (location of the IDS log file)

   sid-msg.map File

   gen-msg.map File

   Engine Start Command

   Engine Stop Command

   Engine Reload Command

   Engine Status Command

8. Ensure the SMTs are running and that the **SMT ID**s that are on the sensor **conf.php** (located on the sensor itself in the **/smt** directory) and the **Unified2 Module** > **Sensor Configuration** locations match, and click **Update** to commit the changes. Aanval will then initiate first-time and continuous communication; paths for the engine rules (**Rules Path**, **SO Rules Path**, etc.) will be imported and displayed, and IDS event log importing will commence.

ADDING A SYSLOG SENSOR

A Syslog sensor can be a logging file from which Aanval imports log data, or a log data stream sent to the Aanval console (UDP port 514) from an external device. In either mode of transport, if the data is in a syslog format, Aanval will import the data for normalization and processing alongside any other syslog or IDS sensors.

1. Inside the Aanval console, go to the **Configuration** menu by hovering over the user login at the top-right of the screen. Under **Event Import Options**, go to **Syslog Module** > **Settings**.

2. Check the box that enables the Aanval Syslog module and click **Update**.

3. From the menu directory display in the upper-right of the screen, go back one menu by clicking **Configuration**, and then under **Event Import Options**, select **Syslog Module** > **Sensor Configuration**.

4. (**Note:** The following step is only necessary for adding a syslog sensor in which the logging device is directly sending log data to Aanval.) From the command line on the Aanval console, go to Aanval's **/apps** directory. The following command will start a basic syslog server designed to receive UDP syslog messages on port 514:

   ```
   nohup perl idsSyslog.pl > /dev/null &
   ```

5. On the **Sensor Configuration** menu, if external logging devices are streaming data logs to Aanval, and with the syslog server from step 4 running, those devices will appear under the **Sensors** listing on the left of the menu. To create a file-based sensor, in which Aanval will retrieve the data logs from a given location, click the **+** button in the upper-right.

6. Select the new sensor from the **Sensors** listing and check the **Enabled** box at the top. A file-based sensor below the **Enabled** box will ask for the **Log File Path**; on a data stream-based sensor the value displayed will be the device's IP address and cannot be changed. Continue to enter sensor information (name, description, location, etc.) and click **Update** to commit the changes.

7. Ensure the **Sensor Permissions** at the bottom of the menu are enabled for each user that will be viewing and managing the events for the given sensor; otherwise, events will not display or be available on any menu.

8. From the menu directory display in the upper-right of the screen, go back one menu by clicking **Configuration**, and then select **Event Import Options** > **Syslog Module** > **Filter Management**. It's on this menu users will create regex-based filters to parse specific values from the imported syslog events such as **Source Address**, **Destination Address**, **Risk Level**, **Payload**, etc.

9. Click the **+** button to create a new filter. Edit the filter and provide a name and the regular expression, and click **Update** to commit the changes. New to Aanval 8 are tools to test the regex with the desired value to parse. They'll be found on this menu and are further designed to work with Aanval's advanced syslog filtering options. For example, a user can link two separate regex that will be recognized as a single regex by adding a double tilde (~~) between the two expressions. Continue to create all necessary filters. A full listing of available import values (**Source Address**, **Source Port**, etc.) will be shown on the next menu.

10. From the menu directory display in the upper-right of the screen, go back one menu by clicking **Configuration**, and then under **Event Import Options**, select **Syslog Module** > **Filter Assignment**.

11. Select a sensor from the listing on the left of the menu and from the import values listed on the right, click the drop-down box, select the proper filter, and click **Add**. Users may select and add multiple filters for a single value. In the event the imported data may have various formats of a single value, Aanval will cycle through the filters listed until a value in the data matches a filter. Repeat these steps for every necessary sensor and value.

ABOUT TACTICAL FLEX, INC.

Tactical FLEX, Inc. is a privately owned software development firm based in Washington, specializing in information security research, engineering, technology design, and production. With the technological development of Aanval, Tactical FLEX, Inc. has become a global provider of information security vulnerability and risk management software solutions that protect businesses and organizations. The firm also provides IT consulting and professional services.

Corporate Headquarters
2049 Rd 3 SW
Suite 100
East Wenatchee, WA 98802

Contact
T 800-921-2584
F 501-648-0875

https://www.aanval.com/
sales.group@tacticalflex.com
support.group@tacticalflex.com