AIRT Tutorial

1 Introduction

This document provides an overview of the functionality of the AIRT system. By reading at least chapter 4 (all five pages of it!) you should be able to get AIRT started with a minimal effort. In addition, chapter 4 describes the expected behaviour of AIRT, and therefore it doubles are a (fairly primitive) testing guide.

Table of Contents

2 Concepts

AIRT is a customisable web-based application for computer security incident response teams. In building AIRT, we have assumed a minimal working set of assumptions, which are discussed in this section.

- An incident response team manages incidents for one or more constituencies.
- A network is described by a network address, followed by a netmask.
- Each constituency has zero or more constituency contacts.
- All "entities" that interact with AIRT are users.
- Incidents are identified by an incident prefix which uniquely identifies the team and an incident number, which uniquely identifies the incident.
- An incident may be associated with zero or more IP addresses.
- An incident may be associated with zero or more users.
- An incident has a type, representing the nature of the incident.
- At any point in time, an incident has a state, which represents in which phase of the incident handling procedure it is.
- At any point in time, an incident has a status, which represent the extent to which the incident has been resolved.

3 Default installation

AIRT out of the box contains a small set of initial data. The initial dataset consists of

- A single user 'admin', with default password 'admin'. If you have not change this yet, do so now!
- A single network with network address 0.0.0.0 and netmask 0.0.0.0.
- Three statuses: open, closed, stalled

4 Getting started

This section assumes that AIRT has been installed according to the instalation guidelines that are outlined in the README file.

4.1 Adding new users

To add a new user to the AIRT system, select the option Edit users from the Settings menu. Fill out the new user section near the bottom of the screen and push the Add! button to create the new user. Your new user should now show up in the user list at the top of the screen.

It is important to realise that AIRT considers everybody who has anything to do with the system a user. However, not all users have the right to interact with the system directly. Only those users who have been assigned a login and a password will be able to use AIRT's web interface. Any other users are merely kept for reference.

Although none of the fields in the input field is required, it is strongly advised to assign everybody at least an email address and, when possible, a last name.

4.2 Deleting existing users

Users may be deleted by selecting the Edit users option in the Settings menu. Scroll to the user that you want to remove, and push the delete link on the user's line. If your browser supports JavaScript, you will be asked to confirm your choice. If your browser does not support JavaScript, the confirmation step will be skipped and the user will be removed immediately.

Removal of users will fail if they are currently associated with any incident.

4.3 Editing users

To change the details of a user, choose the Edit users option in the Settings menu. Scroll to the user that you want to edit, and push the edit link on the user's line. All information that is currently on file will be placed in the input fields, with the exception of the user's password. After you make the changes that you want to make, push the Update! button to submit your changes.

Note that it is not possible to retrieve a user's password with this field, but it is possible to assign a new one.

To prevent a user from accessing the system, simply remove his login and blank the password.

4.4 Adding, editing or updating constituencies

In the context of computer emergency response team, the term constituency is often used to represent an organizational unit that is responsible for resolving an incident. An AIRT constituency consists of a short label and a more elaborate description of the constituency. To add a new constituency, choose the Edit constituencies option in the Settings menu, fill in the form near the bottom of the screen and push the Add! button. After adding the constituency, it will show up in the constituency list at the top of the screen. The constituencies are sorted in the order that they were created.

To edit the constituency label or the constituency description., simply click the edit link in the correct row and hit the Update! button.

To delete a constituency, click the edit link in the correct row and hit the Delete! button. Note that you will not be able to delete constituencies that are associated with any incident.

Although not strictly required, it is advised to only use lower-case characters for the constituency label. Note that by changing the label or the description of a constituency, all incidents with have IP addresses in that constituency will be updated accordingly.

4.5 Setting or removing constituency contacts

To associate a user with a constituency as its constituency contact, select the Edit constituency contacts option in the Settings menu. You will be shown a list of previously defined constituencies. Select the correct one by clicking on its URL.

A screen will appear which lists the currently selected constituency contacts for the selected constituency near the top of the screen, and a second section with users who are not associated with the constituency near the bottom. Select one or more users from the lower list to add as constituency contacts, and push the Assign button.

The screen will now refresh and the user will have been added.

To remove a constituency contact, hit the Remove button in the corresponding line.

4.6 Adding, removing and/or editing networks

To define networks, and select the constituency which manages them, select the Edit networks option in the Settings menu. Begin by entering a network address and a netmask in the appropriate fields (in dotted decimal notation). AIRT currently only supports IPv4 addresses. Enter a descriptive short description in the label field and select the proper constituency from the drop-down menu. Hit Add! to add the network.

Networks can be edited by hitting the edit link and removed by the delete link on the corresponding row.

Note that the constituency to which a network belongs is only used when the incident is initially classified. If an IP address associated with a particular incident has been manually placed in a different constituency, it will remain in that constituency. Networks cannot be deleted when any incident that has IP addresses in the constituency stille exists.

4.7 Editing incident types

The type of an incident represent a nature of the incident. Examples of states are spam, copyright, infection, etc. As each organization prefers its own classification, AIRT does not ship with any predefined values.

4.8 Editing states

The state of an incident represent a phase in the incident handling process. Examples of states are 'blockrequest', which may indicate that all IP addresses of an incident are going to be blocked on a router, or 'forwarded', to indicate that the incident has been forwarded to another constituency.

AIRT does not include any predefined states, since we believe that the specifics of the incident handling process are different for each site. As an example, we include the list of states that are currently in use at UvT-CERT

- acknowledged: constituency contact acknowledges the problem, but has not solved it yet.
- blockrequest: A network block of the addresses associated with the incident has been requested of network operations.
- blocked: Network operations confirmed the block request.
- unblockrequest: A network block release of the addresses associated with the incident has been requested of network operations
- unblocked: Network operations confirmed the unblock request.
- inspectionrequest: A request for inspection has been sent to a user.
- forwarded: The incident has been forwarded to another team.
- solved: A user has indicated that the problem has been solved.

4.9 Editing statusses

Associated with each incident is also a status. AIRT ships with three predefined statusses and it is strongly recommended not to change or remove these. The three statusses are:

- open: The incident is being processed
- closed: The incident has been resolved.
- stalled: The incident has not been resolved yet, but for some reason no progress is being made.

4.10 Using the built-in search capabilities

AIRT is able to automatically search for details about a given IP address, classify it in a predefined network and provide the corresponding constituency details to the incident handler.

The search functions can be found under the Search menu. Simply enter a DNS host name or an IP address (in dotted decimal notation) and hit the search button to look for details.

The following output screen is divided into three section. The top section shows the IP address, it's hostname according to DNS, the network details and constituency information. The second section of the output contains site-specific output (more detail later) and an overview of previous incidents in which the IP address was involved. It also offers the ability to link the search output directly to an already existing (open) incident, and to create a new incident based on the search results. Finally, the bottom half of the screen facilitiates subsequent searches.

4.11 The incident overview

By choosing the Incident management option in the main screen, or the Incidents option in the left-hand navigation bar, the incident management console is openend. By default, it shows all incidents with status 'open', ordered by incident ID. Each incident line contains a number of columns:

- A details link to view additional incident details, or to change those details.
- The fully normalized incident identifier (team prefix, followed by sequence number)
- The constituency to which the primary IP address of the incident belongs
- The hostname of the primary IP address. If the hostname is followed by a double asterix (**), this means that the DNS name of the host has changed between creating the incident and generating the overview.
- A label representing the incident status
- The state in which the incident currently is.
- The type of incident.
- The date that the incident details were last updated.

The selection box near the top of the screen can be used to directly jump to the details of an incident. Simply enter the incident number and click the Details button. To get an overview of all incidents that are open or stalled, or to get an overview of all incidents that are either open or stalled, select the corresponding label from the pulldown menu and hit the Ok button.

4.12 Creating a new incident

New incidents can be created clicking the New incident button on the search result screen, or by selecting the New incident button at the bottom of the incident overview screen.

The benefit of using the button on the search result page is that those results are carried over and will be automatically entered in the form. After clicking on the New incident button, a screen containing three sections appear. By the top of the screen, the state, status and type of incident can be edited by selected the appropriate option in the pulldown menus and by hitting the Update button.

The second section allows the incident handler to enter an IP address and to select a constituency. Finally, it is also possible to associate a user with the incident. The user is identified by email address and can be added by entering that address and clicking the Add button.

If the user already existed in the AIRT user database, he will be associated with the current incident. If the email address cannot be found, and the option 'create user if email address unknown' has been checked, a new user is automatically created and associated with th incident. If the box had not been checked, and the email address can not be found, the incident handler will be notified.

Note that email addresses in AIRT are always converted to lower case characters. If the box 'Check to prepare mail' is checked, the mail template facility will be started after adding the user to the incident.

4.13 Incident details

The incident details screen provide additional information about a specific incident. By the top of the screen, the state, status and type of incident can be edited by selected the appropriate option in the pulldown menus and by hitting the Update button.

Immediately following that section is a list of IP addresses that is associated with the incident. This list may contain any number of IP addresses (including none). To add an IP address to an incident, simply enter the host name or the IP address in the input field and hit the Add button. To remove an address, hit remove. By clicking the IP address itself, a new search for that address will be performed.

Like a list of IP addresses, it is also possible to associate zero or more users with an incident. The users are identified by email address and can be added by entering that address and clicking the Add button. If the user already existed in the AIRT user database, he will be associated with the current incident. If the email address cannot be found, and the option 'create user if email address unknown' has been checked, a new user is automatically created and associated with th incident. If the box had not been checked, and the email address can not be found, the incident handler will be notified.

Note that email addresses in AIRT are always converted to lower case characters.

The final section of the incident details screen contains a full history of the event. Any manipulation of the incident will automatically result in an entry in this log file, and incident handlers may add custom short messages to it.

4.14 Defining or editing email templates

Mail templates are standard email messages that can be sent via the AIRT system. The email templates may contain variables which are automatically changed, based on the last incident that was created, edited or viewed before selecting this option.

From the main menu, or from the navigation bar, select the Mail templates option. You will be able to create a new message by clicking the corresponding link. The input screen that appears asks for a file name and a message. The file name is the name of a file relative to the STATEDIR which has been defined in the global AIRT configuration file.The file name can only contain alphanumerical characters and a very small selection of special characters (such as undercores or hyphens).

AIRT expects the first line of the message to be delimited by the strings @SUBJECT@ and @ENDSUBJECT@, which represents the subject of the mail message. The subject line, like the rest of the message, may contains the following additional variables:

- @HOSTNAME@Will be replaced with the currently active hostname
- @IPADDRESS@ Will be replaced with the currently active IP address
- @IPADDRESS@ Will be replaced with the currently active IP address
- @USERNAME@ Will be replaced with the subject of the current incident
- @USEREMAIL@ Will be replaced with the email address of the user.
- @USERINFO@ Will be replaced with detailed information about the user, if that information is available.
- @YOURNAME@ Will be replaced with the full name of the logged in incident handler
- @YOURNFIRSTAME@ Will be replaced with the first name of the logged in incident handler
- @INCIDENTID@ Will be replaced with the current incident id

Hit the Save! button when your message template is ready to save it.

4.15 Using email templates to send mail

As mentioned before, mail templates are standard email messages that can be sent via the AIRT system. The email templates may contain variables which are automatically changed, based on the last incident that was created, edited or viewed before selecting this option.

To create a new message, either check the 'prepare' message box when creating a new incident, or select Mail templates from the main screen or from the navigation bar. Then, select the 'prepare' option of the desired email template. A new screen will appear, based on the template:

- The To: header will contain the email address of the current user. Generally this is the constituency contact (or the constiuency contacts), but the value can be altered in local customization.
- The Subject: header is derived from the mail template.
- The From: and the Reply-To: headers are derived from the global AIRT configuration.

After reviewing the message, and making any modifications that may be required, the message can be sent by hitting the Send button. If the 'attach incident data in AIRT format' option is checked, an XML representation of the basic incident information will be attached to the message.

If the option MAIL_CC in the global AIRT configuration has been set, the value of that option will automatically receive a copy of all outgoing messages.