AIRT: Application for Incident Response Teams

By Russ McRee – ISSA member, Puget Sound (Seattle), USA Chapter

Prerequisites

Linux OS, documentation exists for Centos and Ubuntu

Apache

Postgresql

Similar Projects

RTIR[1]

As you are likely aware, dear reader, I make my living in security incident management. It butters the bread, you might say. Such is the basic premise of many of the tools discussed from my perch here on the *toolsmith* soapbox. My intent is to further your noble cause, be it through advanced analysis techniques (security data visualization), simple but beneficial point and click applications (NetworkMiner), or the occasional offering to help keep your efforts organized (WebJob).

I was pleased to recently learn of AIRT, the Application for Incident Response Teams, from Kees Leune, the project developer and manager. AIRT is simply an incident tracking Web application with an excellent feature set and a database backend for data retention, querying, and reporting.

According to Kees, "AIRT is a highly specialized web-based tool that was designed to assist computer security incident response teams to automate tasks that do not have to be performed manually. AIRT is able to interact with any IODEF (Incident Object Description Exchange Format[2]) -enabled applications, which includes AIRT itself. AIRT's user base consists of medium- and large-sized (often national) incident response teams who have reported significant increases in productivity, easier cooperation among team members, and improved incident tracking during increased workloads. Work on AIRT is a constant process. New import filters are added regularly which enable automatic processing of computer-generated reports, and bugs are fixed promptly when discovered or reported."

I can tell you from personal experience that Kees is constantly striving to grow and improve AIRT. As always, with tools discussed here, your feedback and participation in the project are welcome.

1 http://bestpractical.com/rtir.

2 http://www.ecsirt.net/service/products.html.

Installing AIRT

There are some specific nuances to installing AIRT; I'll walk you through it with some detail to help you save time. I installed AIRT on Ubuntu 9.04 (Jaunty Jackalope) using the Ubuntu 7.10 installation doc[3] found on the AIRT wiki. I installed version 20090424.1; as you read this there will be a new stable release with some installation and management enhancements, so check the website.[4] You can also install bleeding edge releases from AIRT SVN.

Your system should be *OpenSSH*- and *Apache2* capable; also be sure to include *make functionality*. You'll need *php5-cli, libapache2-mod-php5, php5-pgsql, php-pear, php-mail, php-mail-mime,* and *php-soap*. AIRT also requires *Postgresql*. Easily acquire any and all via `sudo apt-get install <whatever you need>`.

Following the install doc standard, we'll create the database and two users. The `airt_dba` user is the owner of the schema and the `airt` user is used to populate and manipulate the database through the web interface.

1. Create the database: `sudo -u postgres createdb airt`
2. Create the database users.
   - `sudo -u postgres createuser airt` and answer *no* to subsequent questions.

3 http://wiki.leune.com/Home/airt/installation-and-configuration/ubuntu-install.

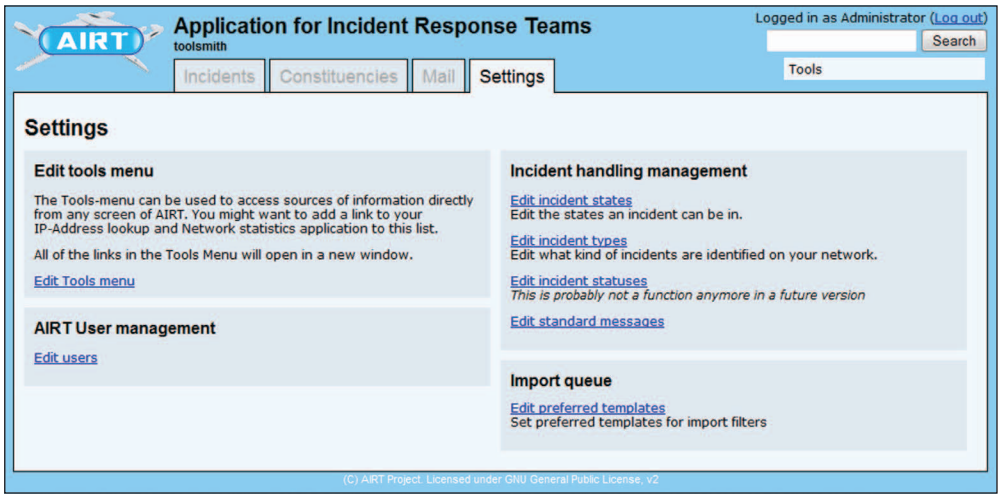
4 http://airt.leune.com/downloads.

Figure 1 – AIRT home page

- sudo -u postgres createuser airt_dba and answer *no* to subsequent questions.

3. Create the system user: sudo adduser airt-admin and answer subsequent questions appropriately.
4. Create an identification map. After # MAPNAME IDENT-USERNAME PG-USERNAME in /etc/postgresql/8.3/main/pg_ident.conf add the following lines.
   - airt-map www-data airt
   - airt-map airt-admin airt
   - airt-map airt-admin airt_dba
5. Create access for the identification map. After # "local" is for Unix domain socket connections only in /etc/postgresql/8.3/main/pg_hba.conf add the following lines.
   - local airt airt ident airt-map
   - local airt airt_dba ident airt-map
   - local a
   - ll all ident sameuser
6. Reload the Postgresql configuration: sudo invoke-rc.d postgresql-8.3 reload
7. Make sure you can connect with the new users.
   - sudo -u airt-admin psql airt airt
   - sudo -u airt-admin psql airt airt_dba
8. Prepare for AIRT code. Create a src directory in airt-admin's home directory: sudo -u airt-admin mkdir ~airt-admin/src then cd /home/airt-admin/src/
9. Unpack and configure.
   - sudo -u airt-admin tar xfz airt-20090424.1.tar.gz
   - cd airt-20090424.1/
   - sudo -u airt-admin ./configure
   - sudo make install
10. Configure AIRT.
    - cd /usr/local/etc/airt/
    - for i in *; do sudo cp $i $(echo $i|sed 's/.dist$//g'); done
    - sudo cp /usr/local/share/airt/php/airt-style.css.dist /usr/local/share/airt/php/airt-style.css
    - sudo -u airt-admin psql airt airt_dba < /home/airt-admin/src/airt-20080402.1/doc/database/airtschema.sql
    - sudo -u airt-admin psql airt airt_dba < /home/airt-admin/src/airt-20090424.1/doc/database/airtperms.sql

Figure 2 – AIRT settings page



- sudo -u airt-admin psql airt airt < /home/airt-admin/src/airt-20090424.1/doc/database/airtbootstrap.sql

11. Prepare Apache.
    - cd /etc/apache2/sites-available/
    - sudo cp /home/airt-admin/src/airt-20090424.1/etc/airt-apache.conf.dist airt-apache.conf
    - cd../sites-enabled/
    - sudo ln -s ../sites-available/airt-apache.conf
    - sudo /etc/init.d/apache2 restart
12. You might have to modify a config file before accessing your new install from a browser on a machine other than the AIRT host.
    - cd /usr/local/etc/airt
    - Open airt.cfg in your editor. Around line 43 note GLOBAL SETTINGS and on line 44 update the localhost reference to your server name or IP. You may find that changing the localhost reference in importqueue.cfg and webservice.cfg to be helpful as well.

Again, as you read this, there should be a newer version that simplifies some of the post-install modifications necessary to get under way. Treat step 12 above as an option only if needed.

Login to your new AIRT installation with username and password admin, then immediately change the passwords for *admin* and *webservice*. Feel free to email me if you have installation questions.

Using AIRT

With the more difficult process out of the way, on to the good stuff!

We'll need to set up an arbitrary AIRT instance with example constituencies, as well as incident states and types.

First, click the *Constituencies* tab and create two, *Corporate* for worker PCs, and *Production* for enterprise servers. If you're part of a consultancy that provides incident response services for a number of clients, each client can be a Constituency. The Constituencies page also offers you the opportunity to provide network details and contacts for each constituency.

Be sure to do so for proper reporting output later.

Next, click the Settings tab and review the *Incident handling management* menu (Figure 2).

Click *Edit incident states* to establish the states an incident can be in. We'll keep it simple for this exercise but keep in mind that you can be as granular as you wish. I chose *InvestigationRequest*, *InvestigationInProgress*, and *InvestigationClosed* as labels and similar terminology for each description. You can also decide which of your chosen incident states should be default and establish it as such accordingly.

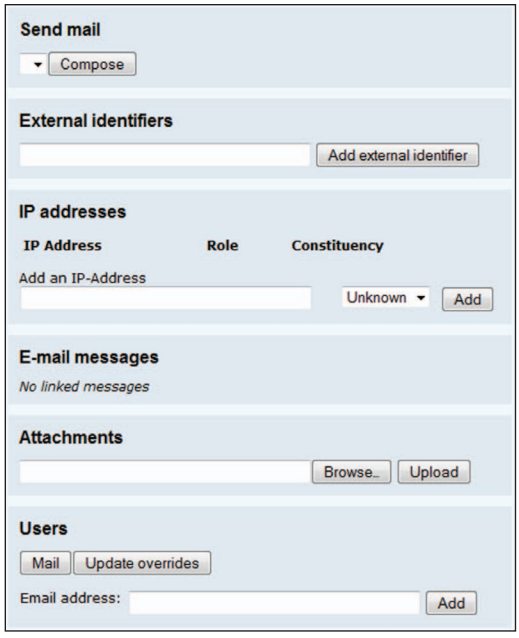


Figure 3 – AIRT incident types

Click the Settings menu again, and Edit incident types to establish what incident types are identified on your network. Again, I kept labels and descriptions very generic and simple for our example effort; you can and should be as specific and granular as is appropriate for your environment (Figure 3).

You may note in the screen shots for this article that there's a category for Edit incident statuses that is tagged as *not a function in a future version*. Depending on the version you install as you read this you may find that is no longer included as it is redundant given the incident states option.

You can also establish preferred mail templates under Settings to establish specific incident communications, manage AIRT users, and modify the AIRT tools menu.

The *Mail* tab on the primary AIRT menu allows you to create new messages from the preferred templates you created.

Under the *Search* form in the upper right-hand area of UI, note a *Tools* drop down menu. Some of the entries are the same as the primary menu bar, but make note of the import and export queues. These will allow you to exchange properly formatted data (IODEF) with other incident management units. Also important on the tools menu is the *Reports* option which we'll close our discussion with.

Now that we've established the basics, let's populate three unique incidents on three different days.

Click the *Incidents* tab on the menu bar. You have the option to *Add multiple incidents* which is useful when you need to create multiple entries for the same incident type (multiple infections). We'll use *Add incident* to create three unique entries.

We'll create three incidents as follows:

Incident One

Type of incident – Malware compromised host

State of incident – InvestigationInProgress

Date of incident – 01 Jul 2009 10:08:41

Short description – Host infected with MyDoom

Notes – Host participating in DDoS attack against South Korean target.

Incident Two

Type of incident – Application layer attack

State of incident – InvestigationInProgress

Date of incident – 02 Jul 2009 12:10:19

Short description – SQL injection attack against CRM

Notes – External attacker compromised primary customer resource management database via SQL injection attack.

Incident Three

Type of incident – System misuse

State of incident – InvestigationInProgress

Date of incident – 03 Jul 2009 22:17:34

Short description – Workstation used to view inappropriate material

Notes – Corporate policy violation.

For purposes of brevity, my notes are extremely limited. They should not be when you conduct a real investigation. ;-)

Once an incident is added you will be presented with the option to provide additional data such as external identifiers, IP addresses, and file attachments. You can also compose mail messages and view history (Figure 4).

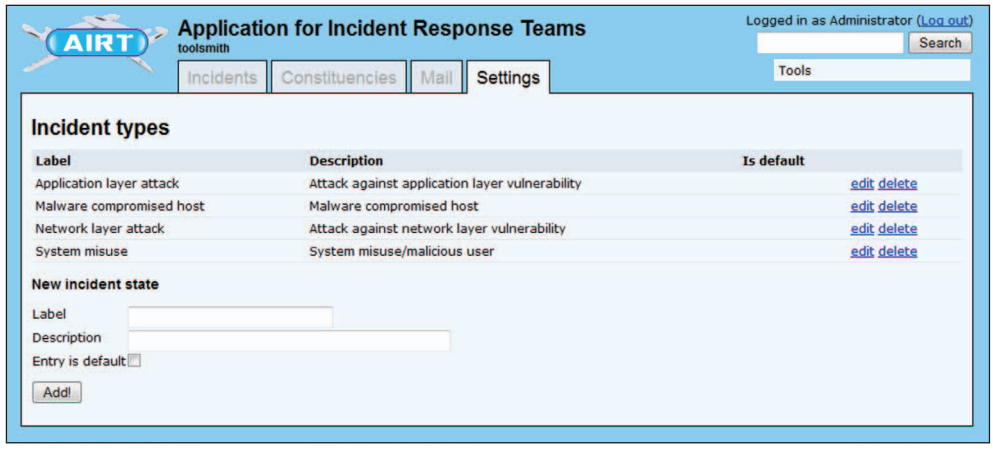
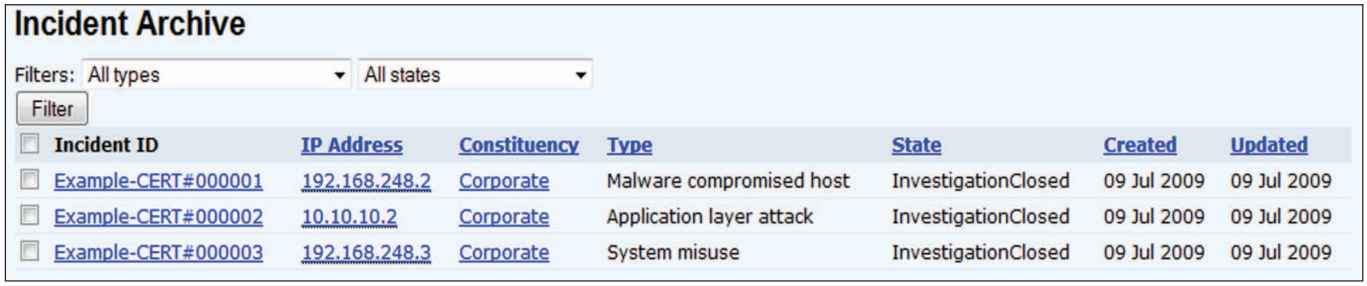


Figure 4 – AIRT incident added

Figure 5 – AIRT archive



Incident Archive

Filters: All types All states Filter

Incident ID	IP Address	Constituency	Type	State	Created	Updated
Example-CERT#000001	192.168.248.2	Corporate	Malware compromised host	InvestigationClosed	09 Jul 2009	09 Jul 2009
Example-CERT#000002	10.10.10.2	Corporate	Application layer attack	InvestigationClosed	09 Jul 2009	09 Jul 2009
Example-CERT#000003	192.168.248.3	Corporate	System misuse	InvestigationClosed	09 Jul 2009	09 Jul 2009

Incidents are dynamic, their states and details change rapidly. AIRT allows you to quickly navigate each incident and populate additional data and findings at will.

One of the most important features of any tool such as AIRT is its reporting functionality. Create a report by clicking the *Tools* menu and choose *Reports*. This functionality is the same as *Statistics* under the *Incidents* menu.

From the Incidents menu you can close cases; they'll be archived for later review (Figure 5).

In conclusion

Proper documentation, tracking, and messaging during security incidents are critical to success. Failure to do so can have catastrophic implications for your enterprise or clients as mistakes are often synonymous with a lack of organization. AIRT is an ideal platform with which to optimize your incident tracking case load and ensure efficiency and clarity.

Cheers…until next month.

Acknowledgments

Kees Leune

About the Author

Russ McRee, GCIH, GPEN, GCFA, CISSP, is a security analyst on the Security Incident Management team for Microsoft's Online Services. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.