`media/cdburner` instead.

4. Type `su` to become root if you are not already.
5. Type `ls.` The following directory listing should display:

```
COPYING devtools immunix-eula setup README rpm
shass-release TRANS.TBL
```

6. To install the AppArmor software, type the following (you should still be logged in as root).

```
./setup --install
```

Note: If you want to update to a new version of AppArmor, repeat steps 1-5 and type `./setup --update`

7. When the installation script then runs, it:
   - Displays the Immunix Commercial License. Use the down-arrow to scroll to the bottom of the license, enter "Q" to exit the license, then enter "Y" to accept the license agreeement if you agree with the terms.
   - Inspects your running kernel, and compiles a kernel module to match your kernel.
   - Installs the rest of the SubDomain infrastructure.
8. Once the installation completes, you should reboot your machine.

Note: If you want to update to a new version of AppArmor, repeat steps 1-5 and type `./setup --update`

If you want to remove AppArmor from your system, repeat steps 1-5 and type `./setup --uninstall`

Getting Started With Profiling Applications

After you have installed AppArmor, you are ready to decide which applications require profiles. You can start by finding out which applications are listening on the network, then begin profiling those applications.

Note: There are some special profiling cases that are not dealt with in this Quickstart Guide. Programs that either start execution before

the system is fully booted, or those whose behavior is only executed when running for long durations, or across reboots, should utilize Systemic profiling method, which is detailed in the AppArmor *Advanced* User's Guide: How to Build SubDomain Profiles.

To get started, perform the following

1. Find out which programs require confinement. To do this, run `unconfined` in a terminal window as the root user.
2. Create approximate profiles for sensitive programs that say **not confined** in the unconfined output.
   - **In YaST:** Execute the Add Profile Wizard for those programs.
   - **In a Terminal Window:** Run `genprof` for those programs.
3. Exercise the full functionality of the programs you are profiling.

Note: This step is important for producing accurate profiles. Make sure that all the program functionality is exercised so AppArmor can protect applications. If you are not familiar with the program and how to use it, obtain an expert user to exercise its functionality.

4. Scan the system events that are generated in Step 3. To do this:
   - **In YaST:** Click the Scan button.
   - **In the Terminal Window in which you ran genprof:** Click "S" to scan the logfiles for events.
5. AppArmor will parse log files. This will generate a series of questions which you must answer to guide `genprof` or the Add Profile Wizard in generating the security profile.
   - **In YaST:** Refer to the AppArmor User's Guide: How to Build SubDomain Profiles for detailed documentation on using the AppArmor Add Profile Wizard.
   - **In the Terminal Window in which you ran genprof:** Refer to the AppArmor *Advanced* User's Guide: How to Build SubDomain Profiles for detailed documentaiton about using `genprof`.
6. Repeat Steps 2-5 as necessary to capture all possible program functionality.

7. **Set up event notification** in AppArmor so you can review security events. Event Notification is an AppArmor feature that informs a specified email recipient when systemic AppArmor activity occurs under the chosen severity level. This feature is currently available via the YaST interface.

   For information on doing this, refer to the Event Notification section in the AppArmor User's Guide: Managing Profiled Applications.
8. **Configure AppArmor reports.** Using reports, you can read important AppArmor security events reported in the log files without manually sifting through the cumbersome messages only useful to the logprof tool. You can narrow-down the size of the report by filtering by date range or program name.

   For information on doing this, refer to the Event Notification section in the AppArmor User's Guide: Managing Profiled Applications.
9. Refer to the AppArmor User's Guide or the AppArmor *Advanced* User's Guide to take advantage of all the benefits of having AppArmor installed on your system.

Running unconfined

Applications that listen to the network have a good chance of being vulnerable to attack. AppArmor comes with the unconfined tool which reports the names of all applications listening on the network.

- To run unconfined, type `unconfined` when you're logged into a terminal window as root.

Note: For detailed help for using `unconfined`, please refer to the AppArmor User's Guide.

Other Resources

Man pages provide useful information about the AppArmor tools. They can be accessed in a terminal window by typing **man *manpagename*** The available AppArmor man pages are listed below:

- autodep
- change hat
- complain
- enforce
- genprof
- logrof
- logprof.conf
- subdomain
- subdomain.d
- subdomain.conf
- subdomain_parser
- subdomain.vim
- unconfined

The **User's Guide** is available after installation of AppArmor. You can find it in: /usr/share/doc/packages/subdo-main/docs/immunizing_applications.pdf

or the **Advanced User's Guide** /usr/share/doc/packages/subdo-main/docs/adv_usersguide.pdf