## G TrueCrypt

You can install TrueCrypt on your Ubuntu instance with:

sudo add-apt-repository ppa:stefansundin/truecrypt

sudo apt-get update  
sudo apt-get install truecrypt

|  |  |  |
| --- | --- | --- |
| **No** | **Description** | **Result** |
| **1** | Go to your **Ubuntu** instance (User: root, Password: toor). Now **Create a new volume** and use an **encrypted file container** (use **truecrypt**) with a Standard TrueCrypt volume.  When you get to the Encryption Options, run the benchmark tests and outline the results:  Graphical user interface, text, application  Description automatically generated | **CPU (Mean)**  AES:  AES-Twofish:  AES-Two-Seperent  Serpent -AES  Serpent:  Serpent-Twofish-AES  Twofish:  Twofish-Serpent:  Which is the fastest:  Which is the slowest: |
| **2** | Select AES and RIPMD-160 and create a 100MB file. Finally select your password and use FAT for the file system. | What does the random pool generation do, and what does it use to generate the random key? |
| **3** | Now mount the file as a drive. | Can you view the drive on the file viewer and from the console? [Yes][No] |
| **4** | Create some files your TrueCrypt drive and save them. | Without giving them the password, can they read the file?  With the password, can they read the files? |

The following files have the passwords of “Ankle123”, “foxtrot”, “napier123”, “password” or “napier”. Determine the properties of the files defined in the table:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **File** | **Size** | **Encryption type** | **Key size** | **Files/folders on disk** | **Hidden partition (y/n)** | **Hash method** |
| <http://asecuritysite.com/tctest01.zip>  (use: **wget** [**http://asecuritysite.com/tctest01.zip**](http://asecuritysite.com/tctest01.zip)  and then: **unzip tctest01.zip**) |  |  |  |  |  |  |
| <http://asecuritysite.com/tctest02.zip> |  |  |  |  |  |  |
| http://asecuritysite.com/tctest03.zip |  |  |  |  |  |  |