
PentestBox Documentation

Release latest

ManifestSecurity

Jun 22, 2017

Contents

1	Installation	3
1.1	Installation on a USB drive	3
1.2	Sharing PentestBox over a Network	3
2	Contributing	5
2.1	Submitting Bug Reports	5
2.2	Improving PentestBox Documentation	6
2.3	Improve PentestBox Website UI	6
2.4	Our Awesome Contributors	6
3	Frequently Asked Questions	7
3.1	When will it be available for Linux/Mac?	7
3.2	How can I work in FullScreen in PentestBox?	7
3.3	Why is [ToolName] not working in PentestBox?	7
3.4	Is there any way I can give administrative rights to a particular tab?	7
3.5	How can I resize PentestBox?	7
3.6	Why is Metasploit not included in PentestBox?	8
3.7	Why is PentestBox throwing up red flags with it being malware?	8
3.8	Metasploit is not running. It's showing some kind of error.	8
3.9	Why Ruby cannot be updated in PentestBox ?	9
4	Tools Manager	11
5	Update Feature	13
5.1	How does the update feature work in the backend ?	13
6	Keyboard Shortcuts	15
7	Tools Include Policy	17
8	Include Your own Tool	19
8.1	Including a Python Based Tool	19
8.2	Including a Ruby Based Tool	19
8.3	Including an Executable Based Tool	20
8.4	Including a Java Based Tool	20

Contents:

Installation

The PentestBox installation is very simple, first you need to [download](#) pentestbox. There are two versions of Pentest-Box:

- PentestBox without Metasploit
- PentestBox with Metasploit

Note: In order to use the PentestBox with Metasploit version, you will need to switch off your antivirus and firewall before installation.

After downloading the file, you will be provided with an installer. Make sure the extraction path is `C:/PentestBox/` and then click next to extract files.

After the extraction is finished, you can find PentestBox files in `C:/PentestBox/`, you can start PentestBox using the **PentestBox.exe** or **PentestBox.bat** file.

Installation on a USB drive

PentestBox is completely portable, that means you can carry it on a USB drive without losing any configuration. You can install PentestBox on a USB drive using the same installer file I mentioned above.

If your pendrive location is `F:` on your computer then you can change the installation path of the PentestBox installer from `C:/PentestBox` to `F:/`.

Sharing PentestBox over a Network

Consider an environment where you want to use PentestBox on many computers like in your office, lab, etc. Instead of installing PentestBox on each and every computer, you can just install that on one computer and share that folder as a drive to other computers on the same network.

- First, right click on the PentestBox folder which is located in the C drive and select properties.
- Select the **Sharing** tab and then click on **Share**.
- Change read permission to **read/write** and click Share.
- Now go the computer where you want to operate PentestBox and then click on Network and locate the Pentest-Box folder.
- Now go to my computer and then click on Map Network Drive.
- Enter the PentestBox path and click on Finish.
- Now that folder will be created as a Network Drive.
- Finally, you can use PentestBox like you are using on the installed computer.

I have personally tested most of the tools on a shared PentestBox and they seem to be working absolutely fine. But if you face any issue with any tool inside the shared PentestBox, then please report it on the [forums](#) or send an e-mail to aditya@manifestsecurity.com

Coding knowledge is not required to contribute to this project. Below are some ways you can contribute if you would like to help:

- Help me complete my `todo` list.
- Improve the PentestBox documentation.
- Translate the website or documentation to your native language.
- Submitting bug reports.
- Suggest features and functionalities.
- Improve the PentestBox website UI.
- Spread the word in at a conference, local meetup or in your circle.
- Write reviews about PentestBox on websites/blogs.

If you find this project interesting, consider donating :)

Submitting Bug Reports

If you face any issue or error with any tool or functionality then you can submit a bug report on forum.pentestbox.com, create a issue on [tracker](#) or you can email me at aditya@manifestsecurity.com

Please make sure to include following things when sending a Bug report.

- Tool which is causing the issue
- System Architecture: 32 bit or 64-bit
- Command Used with the tool which caused that error
- Screenshot of the error

Improving PentestBox Documentation

If you would like to improve PentestBox then you can make changes to [docs github repo](#), it uses readthedocs to generate documentation. But if you are not aware of working of readthedocs framework, then you can send changes/suggestions to aditya@manifestsecurity.com

Improve PentestBox Website UI

If you can make main website more awesome, that would be really helpful. All files of the PentestBox website are located at it's [github repo](#).

Our Awesome Contributors

Below are the some of the awesome folks who have contributed their time in making PentestBox more awesome.

- [Naveed Sheik](#)
- [Sumit Srivastava](#)
- [Gustavo Speranza](#)
- [Kirit Sankar Gupta](#)
- [Sreemoyee Mukherjee](#)
- [Manh Tuan](#)
- [Michele Cisternino](#)
- [João Vitor BF](#)
- [wu litao](#)
- [Benhabi Mahdi](#)

Note: This list was created on 1 July, 2016 after i started using [readthedocs](#) on docs.pentestbox.org.

Frequently Asked Questions

When will it be available for Linux/Mac?

PentestBox was developed to provide the best penetration testing environment for Windows users. So it will never be developed for Linux/Mac. For Linux/Mac you can use any Linux Pentesting Distro.

How can I work in FullScreen in PentestBox?

Just press Alt + Enter while using PentestBox to go into FullScreen Mode and do the same to come back in normal mode.

Why is [ToolName] not working in PentestBox?

In case if you are facing any issue or error with any of the tools inside PentestBox or the ones which are provided through [Toolsmanager](#), please submit yours [Bug Reports](#).

Is there any way I can give administrative rights to a particular tab?

By default PentestBox runs like a normal user, no administrative permission is required to launch it. But you might want to use some tool which requires administrative permission. In that case you need to right click on the tab and choose restart as admin, after that the tab will be given administrative rights.

How can I resize PentestBox?

If you move your cursor along it edges, the cursor will change and you will be able to resize it by clicking and dragging, but this procedure is something not everyone is able to follow.

There is an alternative way to do this:

- Right click on the top bar and then click on settings.
- Then a new window will appear, uncheck “Hide caption Always” and save the settings as given below.
- Then PentestBox will look something like this.
- You can now resize the window as you like. After that you can go to settings, check that option again and save settings. PentestBox will save your current windows size and will open as it is when you open it up next time.

Why is Metasploit not included in PentestBox?

Metasploit contains exploits/payloads inside it, so when installed on Windows machines nearly all antiviruses and firewalls will put up warnings. Also, Metasploit officially instructs to disable antiviruses and firewalls while using it.

So in order to make PentestBox work without switching off any antiviruses programs, I have not included that. But if you are willing to switch off your antivirus program and want to use Metasploit on Windows, you can download the “PentestBox with Metasploit” version from the [Download](#) option.

Why is PentestBox throwing up red flags with it being malware?

- There are two Variants of PentestBox, one with Metasploit and one without Metasploit. Metasploit contains many exploits/payloads, so if you are using the version with Metasploit then your antivirus will definitely make warnings. But you don’t need to worry about this, it won’t infect your system, you can put the PentestBox folder in the exception list instead of switching off antivirus.
- But if you are using the PentestBox version without Metasploit, only some files can be detected as malicious depending on your antivirus. In case of Avira, below are some of the files detected malicious and the reason why it’s detected:
 - C:/PentestBox/PentestBox.exe: If this is detected then you can use the PentestBox.bat file, even though the exe is just a compiled version of the PentestBox.bat file.
 - C:\PentestBox\bin\beef\modules\exploits\local_host\ie_ms12_004_midi\ie_ms12_004_midi.html: It’s a part of the Beefproject, if deleted then some particular modules will not work.

Let me know if you have any concern regarding this issue.

Metasploit is not running. It’s showing some kind of error.

First of all make sure that you have installed the PentestBox with Metasploit version in C:\PentestBox\ and that any antivirus/firewall have been switched off right before installation (including Microsoft Windows Defender). Below are possible cases for Metasploit failure:

- If there is any ruby installation on your system, please remove it from the PATH. In order to remove that, go to Control Panel > System > Advanced System Settings > Environment Variables. Then look for Ruby path in the PATH variable.
- In case if you are using the arabic language on your system, then you first need to type `chcp 65001` on the console in order to user Metasploit.

Why Ruby cannot be updated in PentestBox ?

Most of the ruby based tools are not compatible with every version of Ruby, also ruby on windows has many issues. An update on ruby can make most of the tools non-functional. This is the main reason for not providing update functionality for Ruby.

CHAPTER 4

Tools Manager

Tools Manager was introduced in PentestBox v2.0. Using this utility you can install/update/uninstall tools which are not there in PentestBox. This makes PentestBox more modular. The list of tools which can be installed using toolsmanager can be found at modules.pentestbox.com.

It is an interactive Installation utility, type **toolsmanager** on terminal to open it. First it will update itself from the Github Repository and then will display the menu. In case there is no internet connection, the script will wait for some time and then display the menu.

You can see the list of tools by selecting a particular category. For example, if I choose the **Web Applications** category and press **10**, it will display something like this. At the time of writing, it only contains **whatweb**.

Now if you want to install **whatweb**, then type **install whatweb** and it will install it. After installing, it will display the alias for the tool, in the case of whatweb it is **whatweb**.

Note: Since toolsmanager is just an installation utility, when any tool without re-distributable license is installed, the user automatically accepts the agreement provided by developer of that tool.

Update Feature

Maintaining a product is always much more important than actually making one. That is why to keep all the tools updated inside PentestBox we have included an update utility. Also I have added `update config` which will be used as a medium to fix the bugs if any comes up. You would see something similar if you typed `update` on console.

It will first update itself from its Github Repository if there are any changes and then display the menu. In case there is no internet connection, the script will wait for some time and then display the menu.

For example if you need to update your **Web Applications Tools** then just type **update webapplication**, you can update all the tools with one command by typing **update all**.

How does the update feature work in the backend ?

PentestBox is an open source project, so all files that are used in PentestBox are there on its [Github Repositories](#) .

You can find its update script [here](#) . Nearly 80% of the tools which are shipped in PentestBox are fetched from their respective Github repositories, other are provided in zip format or in other way which are then manually configured in PentestBox.

Whenever you type **update** on console, you will see it trying to update something, at the moment it is updating itself. Then whenever you provide a command to update a set of tools, for example `update webapplication`, it will try to update the tools which are located in `C:/PentestBox/bin/webapplications/`, as most of the tools are based on git VCS, it requires less data to acquire the changes of the respective tool.

CHAPTER 6

Keyboard Shortcuts

- CTRL + T : To open new tab
- CTRL + C : To close the script/program that is running.
- If multiple tabs are open, then you can access them using SHIFT+ ALT + number , number is the value for the tab. For example, the number will be 1 for first tab, 2 for second tab and so on.
- CTRL + w : This will close your current active console.
- ALT +Enter : Pentestbox will go FullScreen.

Tools Include Policy

PentestBox currently contains the most efficient and popular security tools. I am aware that our users require more tools than what is provided by PentestBox, that is why we have [Toolsmanager](#) which can be used to install tools which are currently not there in PentestBox. A list of tools which can be installed using Toolsmanager can be found at modules.pentestbox.com.

If you want to have more tools through toolsmanager then you can let me know at [Facebook](#), [Twitter](#), aditya@manifestsecurity.com or you can create a thread on my [todo](#) list.

But if you would like to suggest some tool that should be included by default in PentestBox, then please make sure it fulfills following points.

- The tool/software license should allow redistribution of their package.
- If software size is large (more than 300 MB) and it's author already provides the Windows version of that tool then i won't be able to include it, because it won't be comfortable for the users to download a large size installer, also the main motive of PentestBox is to provide security tools which are not compatible on Windows by default or if their installation is troublesome.

After clearing the above points, if the tool is compatible with Windows then I will add it to the list for inclusion in the next version. But since in the most cases the tool is not compatible on Windows, I usually check it's code to see if there is possibility of porting that tool to Windows, otherwise I will try to contact the developer to provide Windows support for the tool.

Include Your own Tool

There are many situations someone wants to run a tool which may be not be provided by `toolsmanager` or isn't installed by default in PentestBox. You can follow the guide below to include your own tool.

In order to include a tool in PentestBox, you need to do two things, download/clone tool files and then set alias for it. **alias** is basically a terminal command which need to be passed in PentestBox console, for example **sqlmap** is an alias for accessing SQLMAP.

Including a Python Based Tool

- First download/clone the files of that tool in `C:/PentestBox/bin/customtools`
- Install any needed libraries using pip, for example if you need to install the **BeautifulSoup4** library then you can install it using **python -m pip install BeautifulSoup4**.
- Since python is preconfigured in PentestBox, you can run the tool by prepending **python** to the python file.
- To add an alias, open the **customaliases** file located in `C:/PentestBox/bin/customtools/` folder.
- For example if you needed to add an alias for the sqlmap tool, then the alias for it would be `sqlmap=python "%pentestbox_ROOT%\bin\customtools\sqlmap\sqlmap.py" $*`
- Add the above line to customaliases and save the file
- Likewise you can create an alias for your tool. You can run your tool after restarting PentestBox.

Including a Ruby Based Tool

- First download/clone the files of that tool in `C:/PentestBox/bin/customtools`
- Install any needed gems using gem, for example if you need to install the **nokogiri** library then you can install it using **gem install nokogiri**.
- Since ruby is preconfigured in PentestBox, you can run the tool by prepending **ruby** to the ruby file.

- For example if you needed to add an alias for the wpscan tool, then alias for it would be `wpscan=ruby "%pentestbox_ROOT%\bin\customtools\wpscan\wpscan.rb" $*`
- Add the above line to the customaliases and save the file
- Likewise you can create an alias for your tool. You can run your tool after restarting PentestBox.

Including an Executable Based Tool

- First download/clone the files of that tool in `C:/PentestBox/bin/customtools`
- You can directly access the file by typing it's filename, for example you can access `tool.exe` by typing **tool.exe** on the console.
- For example, an alias for an executable would be like `tool="%pentestbox_ROOT%\bin\customtools\tool.exe" $*`
- Add the above line to customaliases and save the file.
- Likewise you can create an alias for your tool. You can run your tool after restarting PentestBox.

Including a Java Based Tool

- First download/clone the files of that tool in `C:/PentestBox/bin/customtools`
- Since Java is preconfigured in PentestBox, you can run the tool by prepending **java -jar** to the jar file.
- For example if you need to add an alias for “tool”, then the alias for it would be `tool=start javaw -jar "%pentestbox_ROOT%\bin\customtools\tool.jar" $*`
- Add the above line to customaliases and save the file
- Likewise you can create an alias for your tool. You can run your tool after restarting PentestBox.

You can have a look at the [aliases](#) file for more examples of aliases.