PentestBox Documentation

Release latest

ManifestSecurity

Feb 23, 2018

Contents

Contents:

CHAPTER 1

Installation

The PentestBox installation is very simple, first you need to download pentestbox. There are two versions of PentestBox:

- PentestBox without Metasploit
- PentestBox with Metasploit

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

After downloading the file, you will be provided with a 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.

1.1 Installation on a USB drive

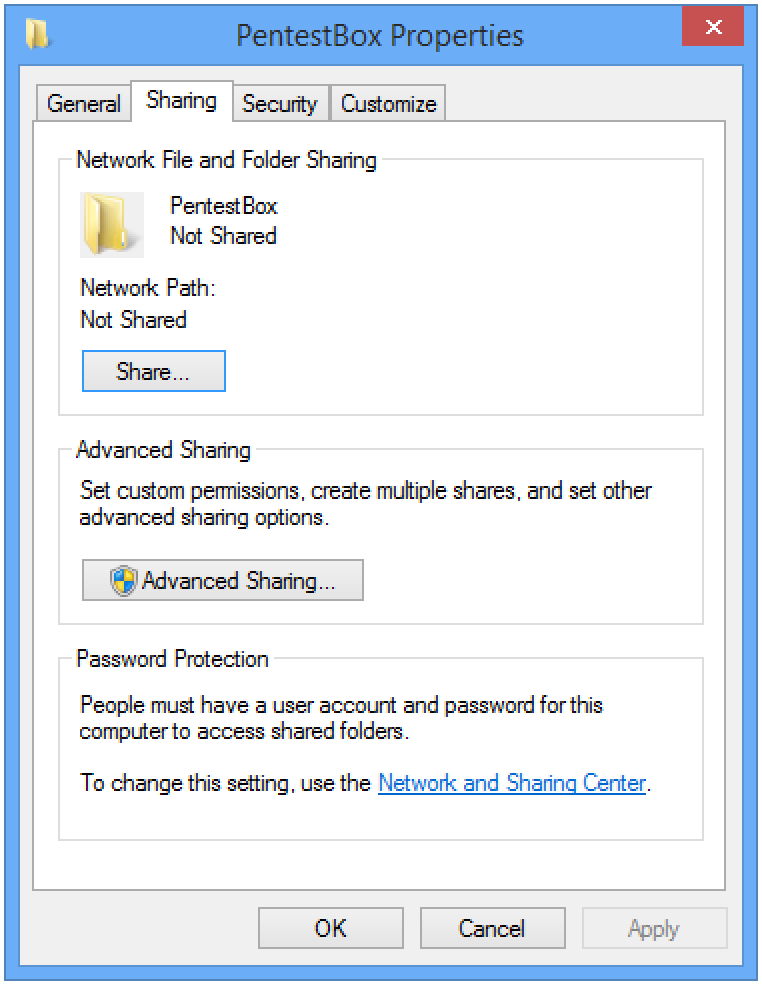
PentestBox is completely portable, that means you can carry it on a USB drive without losing any configuration. You can install PentestBox on a USB drive using the same installer file I mentioned above.

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:/`.

1.2 Sharing PentestBox over a Network

Consider a 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.



PentestBox
Not Shared

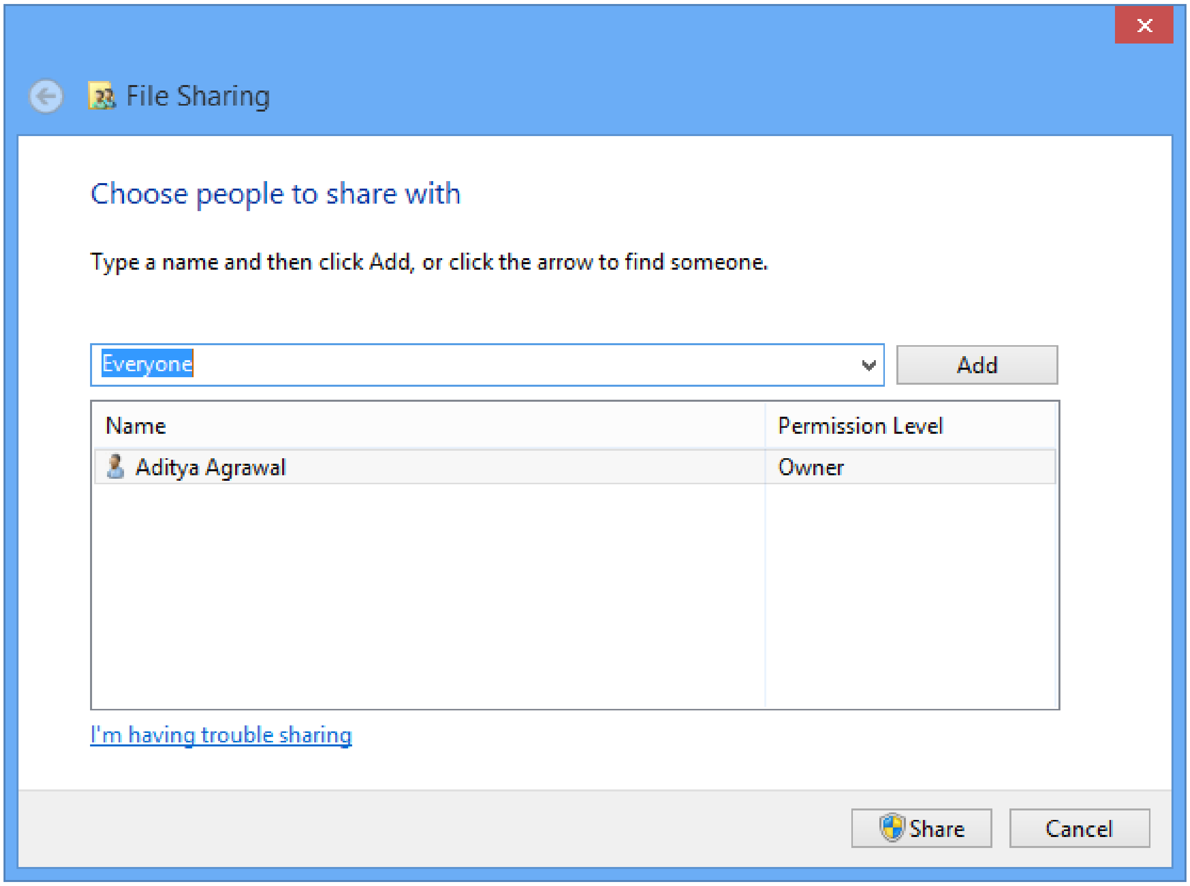
Network Path:
Not Shared

Set custom permissions, create multiple shares, and set other advanced sharing options.

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.

- Select the **Sharing** tab and then click on **Share**.



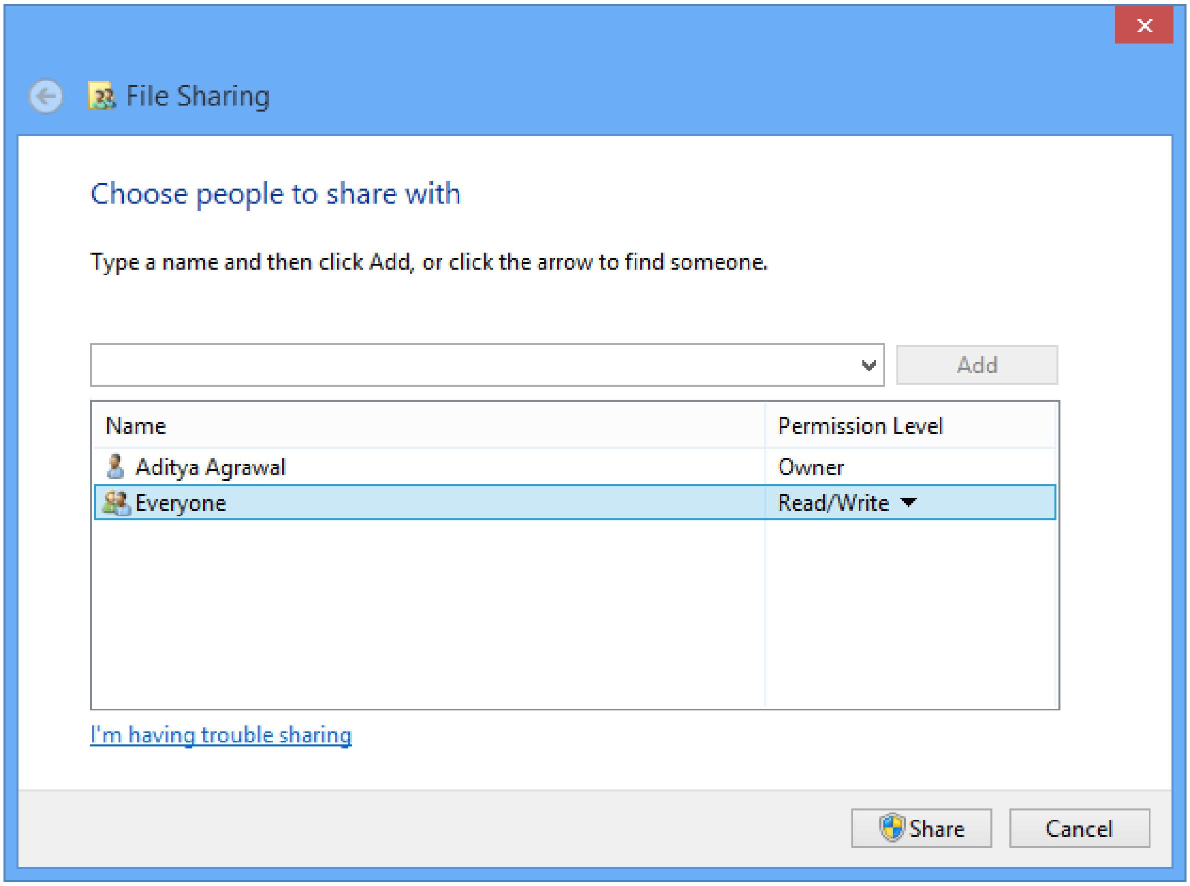
Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Everyone

Name	Permission Level
Aditya Agrawal	Owner

- Change read permission to **read/write** and click Share.

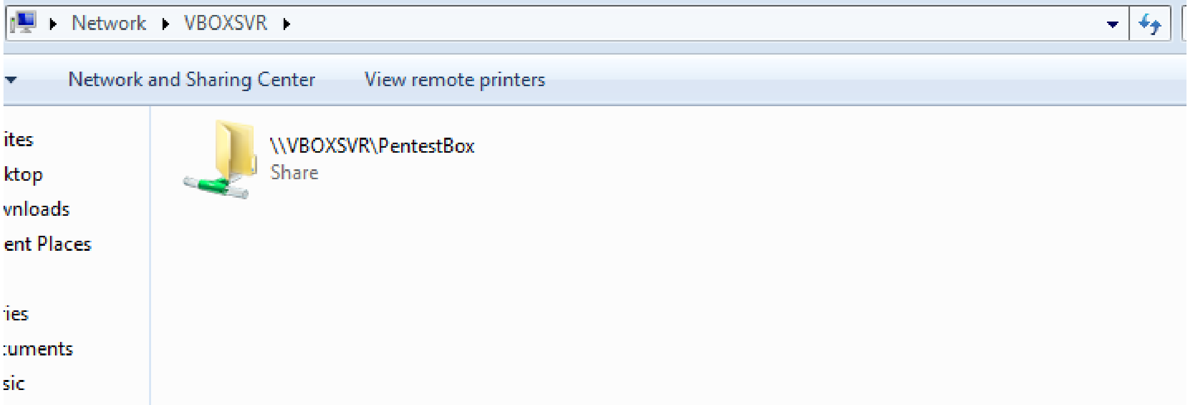


Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

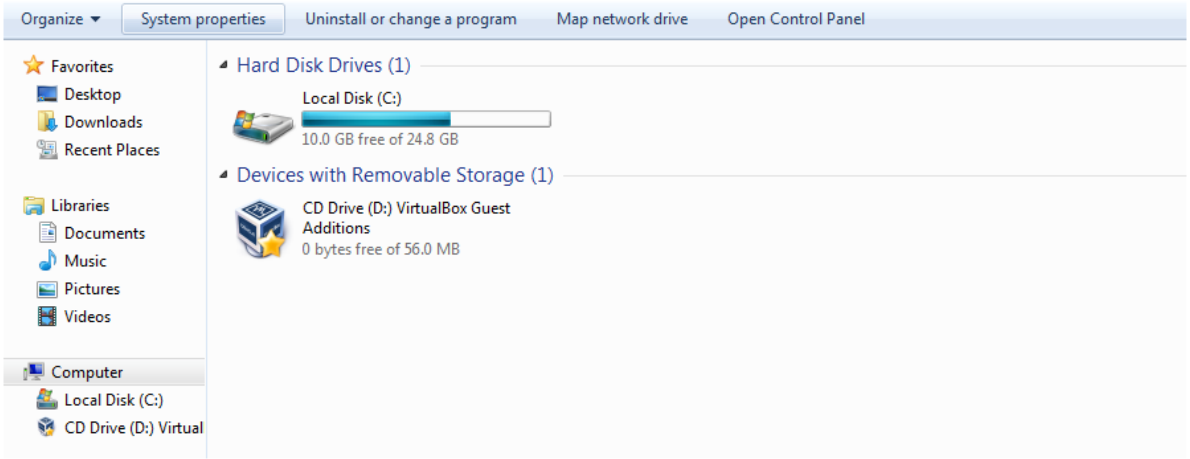
Name	Permission Level
Aditya Agrawal	Owner
Everyone	Read/Write

- Now go the computer where you want to operate PentestBox and then click on Network and locate the PentestBox folder.

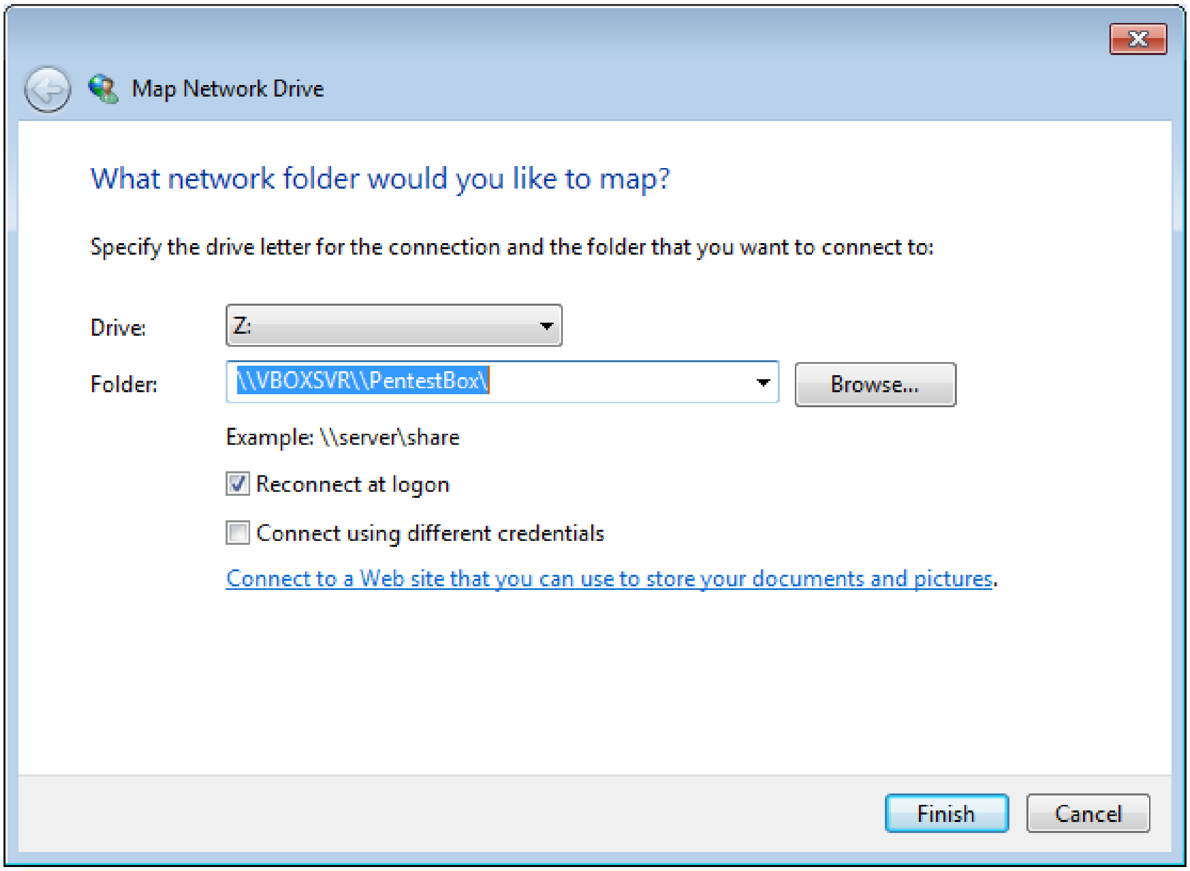


\\VBOXSVR\PentestBox
Share

- Now go to my computer and then click on Map Network Drive.



- Enter the PentestBox path and click on Finish.



What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\VBOXSVR\\PentestBox\

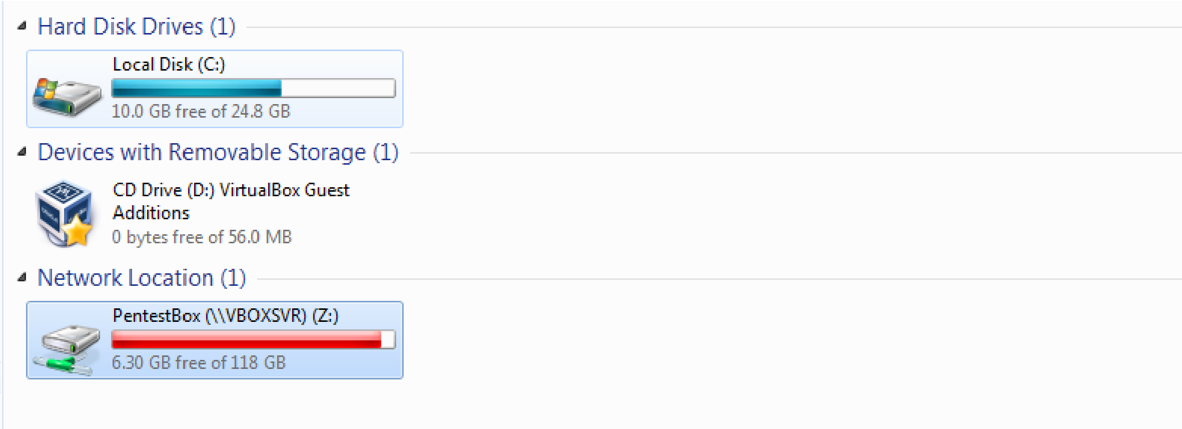
Example: \\server\share

☑ Reconnect at logon

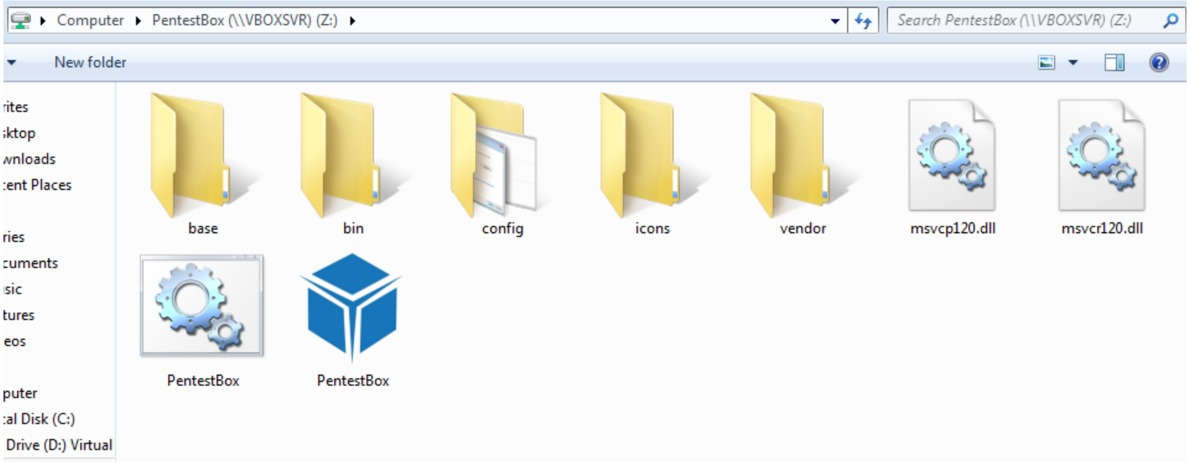
□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

- 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

CHAPTER 2

Contributing

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.

2.1 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`

2.2 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

2.3 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.

2.4 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.

CHAPTER 3

Frequently Asked Questions

3.1 When will it be available for Linux/Mac?

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

3.2 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.

3.3 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.

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

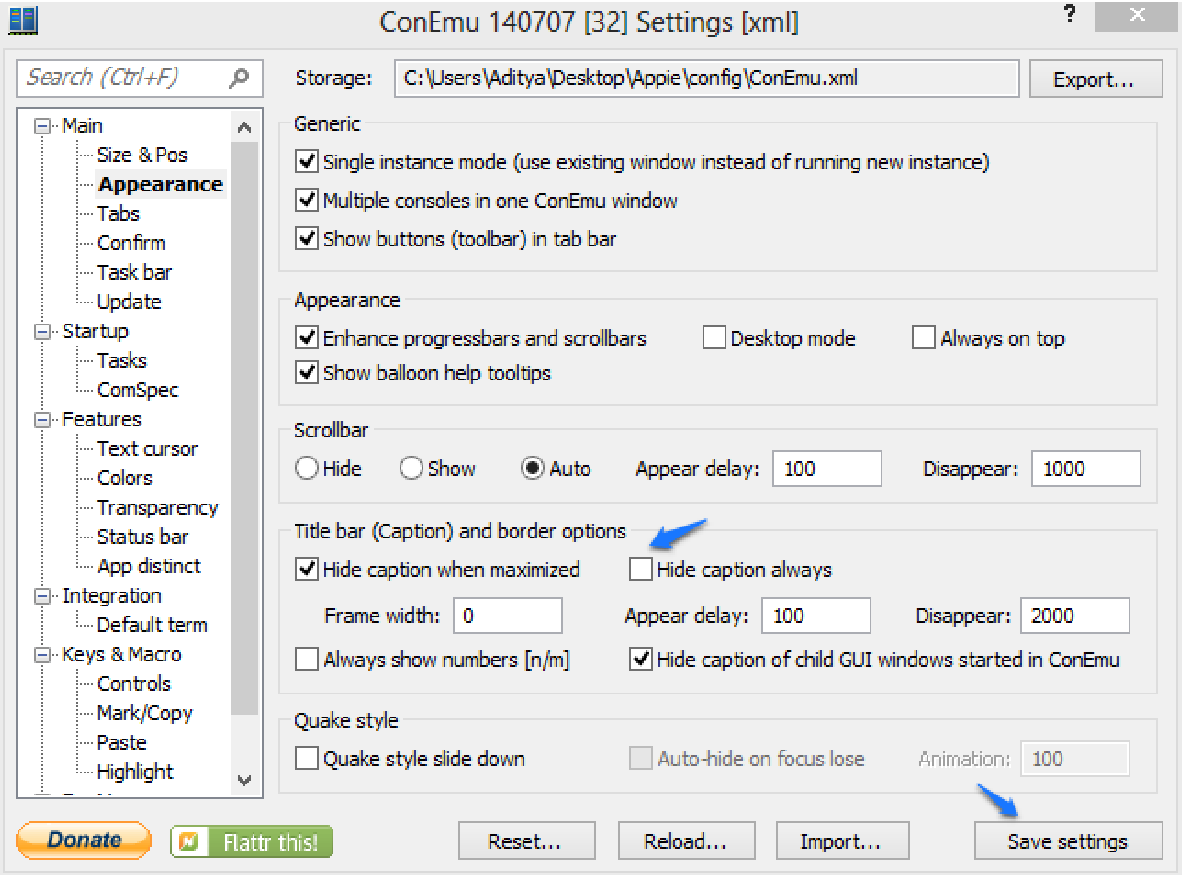
By default PentestBox runs like a normal user, no administrative permission is required to launch it. But you might want to use some tool which requires administrative permission. In that case you need to right click on the tab and choose restart as admin, after that the tab will be given administrative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

3.5 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.



ConEmu 140707 [32] Settings [xml]

Storage: C:\Users\Aditya\Desktop\Appie\config\ConEmu.xml

Generic
☑ Single instance mode (use existing window instead of running new instance)
☑ Multiple consoles in one ConEmu window
☑ Show buttons (toolbar) in tab bar

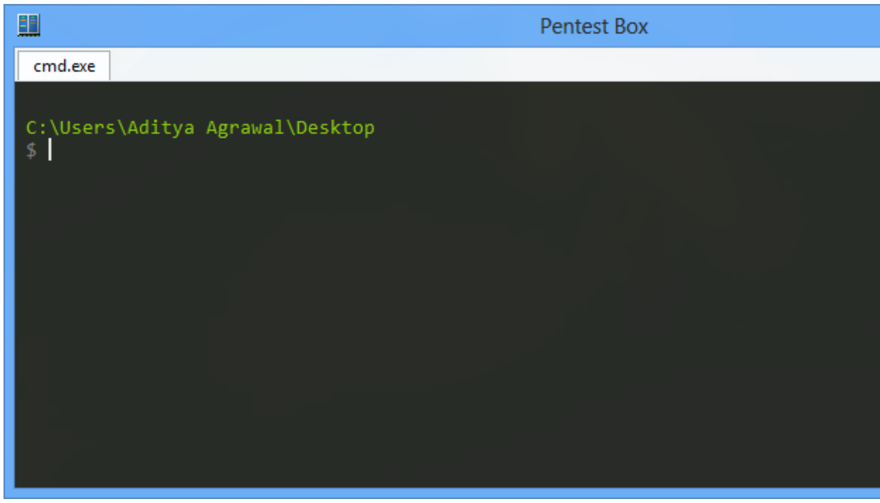
Appearance
☑ Enhance progressbars and scrollbars □ Desktop mode □ Always on top
☑ Show balloon help tooltips

Scrollbar
○ Hide ○ Show ● Auto Appear delay: 100 Disappear: 1000

Title bar (Caption) and border options
☑ Hide caption when maximized □ Hide caption always
Frame width: 0 Appear delay: 100 Disappear: 2000
□ Always show numbers [n/m] ☑ Hide caption of child GUI windows started in ConEmu

Quake style
□ Quake style slide down □ Auto-hide on focus lose Animation: 100

- Then PentestBox will look something like this.



Pentest Box

```
C:\Users\Aditya Agrawal\Desktop
$ |
```

- 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.

3.6 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 Metsaploit on Windows, you can download the "PentestBox with Metasploit" version from the Download option.

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

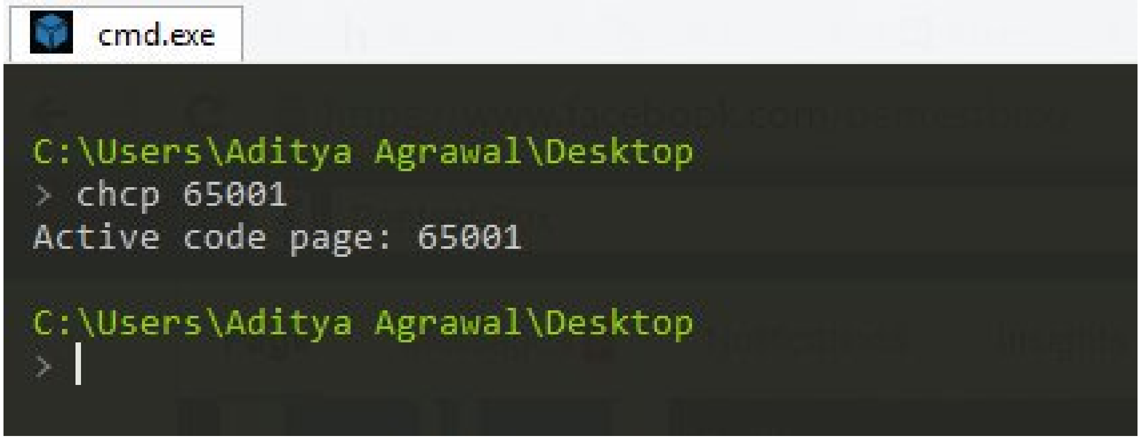
- There are two Variants of PentestBox, one with Metasploit and one without Metasploit. Metasploit contains many exploits/payloads, so if you are using the version with Metasploit then your antivirus will definetly make warnings. But you don't need to worry about this, it won't infect your system, you 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.

3.8 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.



```
C:\Users\Aditya Agrawal\Desktop
> chcp 65001
Active code page: 65001

C:\Users\Aditya Agrawal\Desktop
> 
```

3.9 Why Ruby cannot be updated in PentestBox ?

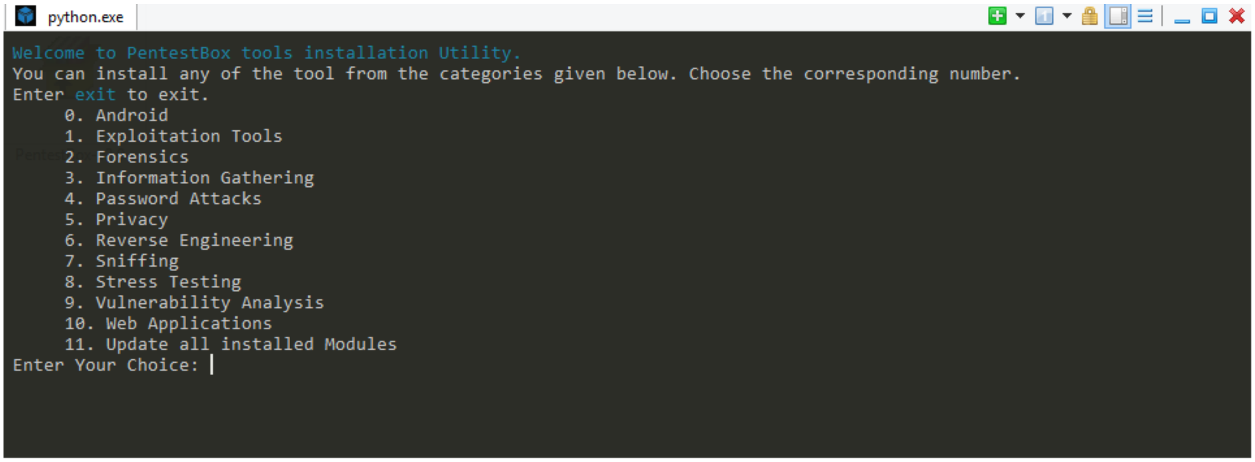
Most of the ruby based tools are not compatible with every version of Ruby, also ruby on windows has many issues. An update on ruby can make most of the tools non-functional. This is the main reason for not providing update functionality for Ruby.

CHAPTER 4

Tools Manager

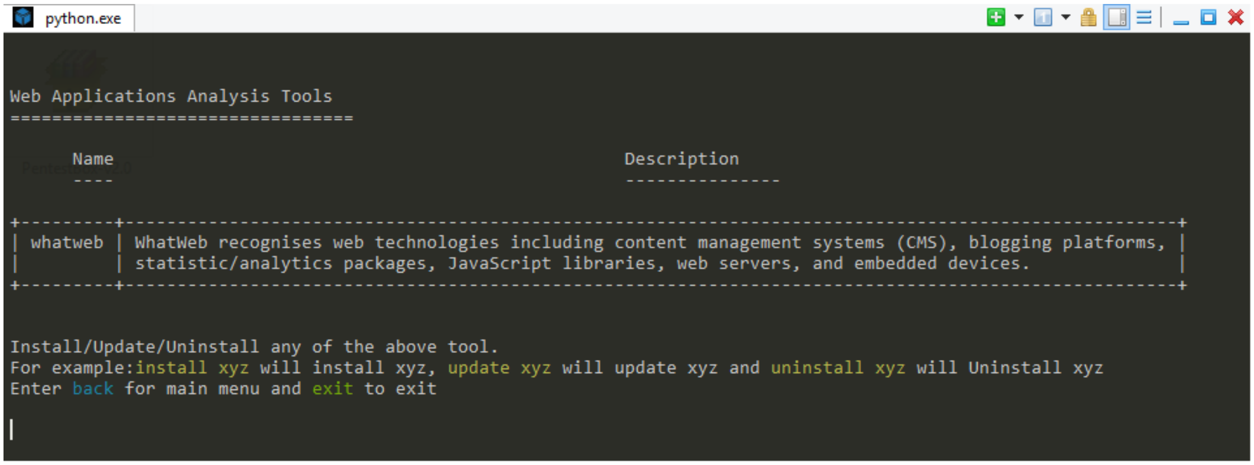
Tools Manager was introduced in PentestBox v2.0. Using this utility you can install/update/uninstall tools which are not there in PentestBox. This makes PentestBox more modular. The list of tools which can installed using toolsmanager can be found at modules.pentestbox.com.

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.



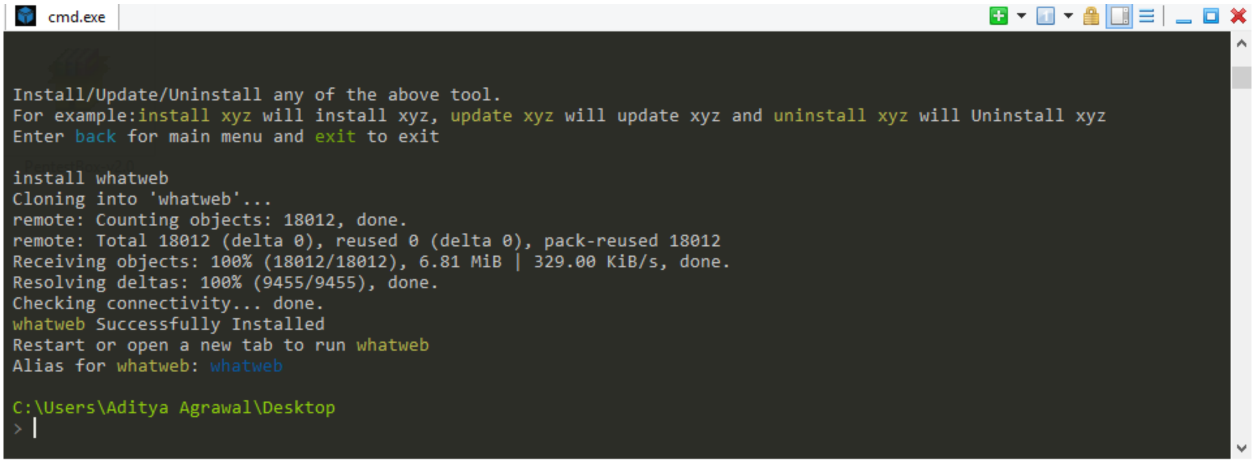
```
Welcome to PentestBox tools installation Utility.
You can install any of the tool from the categories given below. Choose the corresponding number.
Enter exit to exit.
     0. Android
     1. Exploitation Tools
     2. Forensics
     3. Information Gathering
     4. Password Attacks
     5. Privacy
     6. Reverse Engineering
     7. Sniffing
     8. Stress Testing
     9. Vulnerability Analysis
     10. Web Applications
     11. Update all installed Modules
Enter Your Choice:
```

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**.



```
Web Applications Analysis Tools
=================================

      Name                                                   Description
      ----                                                   ---------------

+---------+---------------------------------------------------------------------------------------------+
| whatweb | WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, |
|         | statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.       |
+---------+---------------------------------------------------------------------------------------------+


Install/Update/Uninstall any of the above tool.
For example:install xyz will install xyz, update xyz will update xyz and uninstall xyz will Uninstall xyz
Enter back for main menu and exit to exit

|
```

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**.



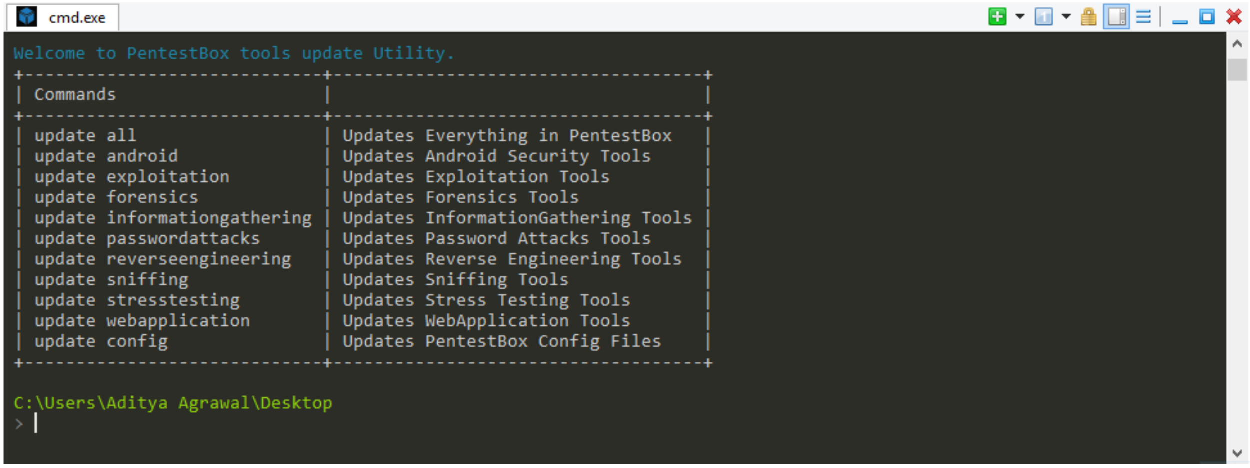
```
Install/Update/Uninstall any of the above tool.
For example:install xyz will install xyz, update xyz will update xyz and uninstall xyz will Uninstall xyz
Enter back for main menu and exit to exit

install whatweb
Cloning into 'whatweb'...
remote: Counting objects: 18012, done.
remote: Total 18012 (delta 0), reused 0 (delta 0), pack-reused 18012
Receiving objects: 100% (18012/18012), 6.81 MiB | 329.00 KiB/s, done.
Resolving deltas: 100% (9455/9455), done.
Checking connectivity... done.
whatweb Successfully Installed
Restart or open a new tab to run whatweb
Alias for whatweb: whatweb

C:\Users\Aditya Agrawal\Desktop
> |
```

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.

CHAPTER 5

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.



```
Welcome to PentestBox tools update Utility.
+-----------------------------+------------------------------------+
| Commands                    |                                    |
+-----------------------------+------------------------------------+
| update all                  | Updates Everything in PentestBox   |
| update android              | Updates Android Security Tools     |
| update exploitation         | Updates Exploitation Tools         |
| update forensics            | Updates Forensics Tools            |
| update informationgathering | Updates InformationGathering Tools |
| update passwordattacks      | Updates Password Attacks Tools     |
| update reverseengineering   | Updates Reverse Engineering Tools  |
| update sniffing             | Updates Sniffing Tools             |
| update stresstesting        | Updates Stress Testing Tools       |
| update webapplication       | Updates WebApplication Tools       |
| update config               | Updates PentestBox Config Files    |
+-----------------------------+------------------------------------+

C:\Users\Aditya Agrawal\Desktop
> 
```

It will first update itself from it's 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 Aplications Tools** then just type **update webapplication**, you can update all the tools with one command by typing **update all**.

5.1 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 it's Github Repositories .

You can find it's 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.

CHAPTER 7

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.

CHAPTER 8

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.

8.1 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.

8.2 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.

8.3 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.

8.4 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.