



Workshop

We are cyber / WoSEC Montreal

How to create your own lab to practice on your web pentesting skills

Who am I



- Pentester at Okiok
- Blogger, Podcaster, trying to democratize the security of information for all, especially for women.
- Organizer of WoSEC Paris chapter
- Newly organizer of workshops for WeAreCyber aka WoSEC Montreal
- Contact Info:
 - **Gabrielle Botbol**
- Twitter:
 - @Gabrielle_BGB
- LinkedIn
- Blog
 - <https://gabrielleb.fr/blog>

Does everyone here know what is a pentester?



What is pentest?

- Trying to find vulnerabilities in systems by doing what a criminal hacker (black hat) would do.
- Web pentesting: Doing this but specifically for web applications.

In order to get started you should already have:

- Downloaded and installed Virtualbox
- Downloaded Metasploitable
- Downloaded Kali linux virtualbox image





What will we do?

- Install our machines in virtualbox
- Connect them together
- Explore Mutilidae and DVWA
- Start to practice a little

Install Metasploitable



- How to install metasploitable
 - Unzip the downloaded file in the emplacement of your choice
 - Go to virtualbox click on new machine

A screenshot of the 'Create Virtual Machine' dialog box in Oracle VM VirtualBox. The window title is 'Create Virtual Machine'. The section 'Name and operating system' is active. It contains a text box for 'Name' (empty), a dropdown for 'Machine Folder' (set to 'C:\Users\gabri\VirtualBox VMs'), a dropdown for 'Type' (set to 'Linux'), and a dropdown for 'Version' (set to 'Ubuntu (32-bit)'). There is a small Ubuntu logo icon to the right of the version dropdown. At the bottom, there are three buttons: 'Expert Mode', 'Next', and 'Cancel'.


← Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Machine Folder:

Type: 

Version:

- Give a name to your new machine I will call it Metasploitable
- Choose the type Linux and Version Ubuntu (does not matter if it is 32 or 64 bits)

- Choose how much ram you need 1go should be enough:



← Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

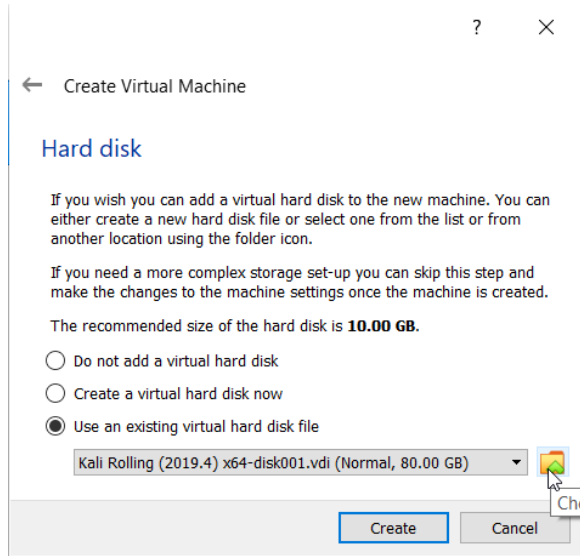
The recommended memory size is **1024 MB**.

4 MB 8192 MB

1024 MB

Next Cancel

- On the next window click on "use an existing virtualdisk file



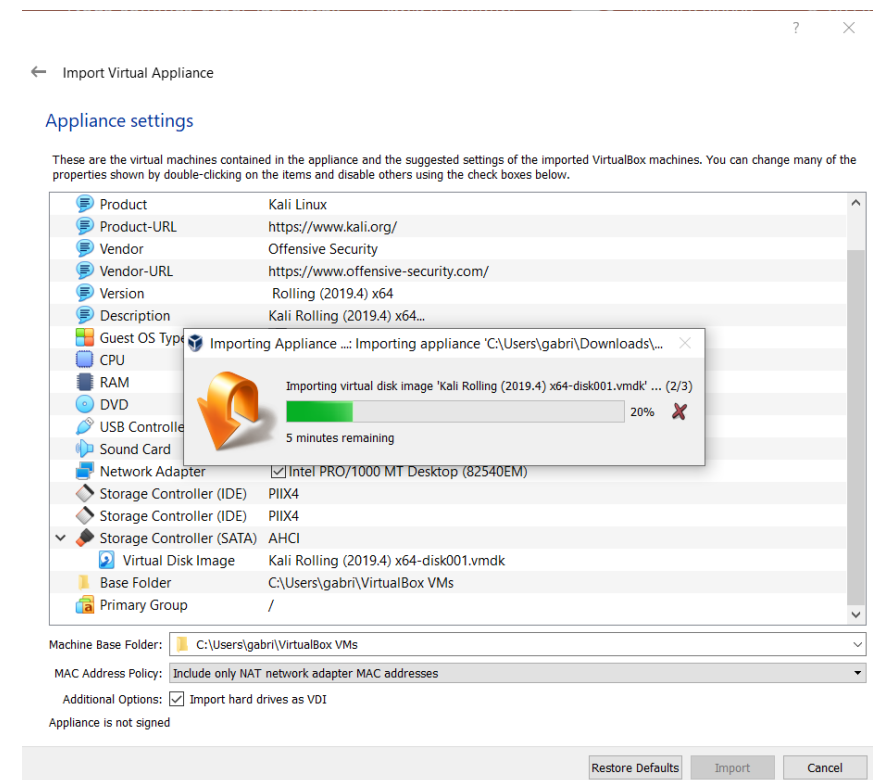
- Click on the yellow folder
- Click on add
- Navigate to the metasploitable folder you have just downloaded and select the .vdmk file
- Select it and then click on choose
- Finally click on create

- You can now start the machine for the first time (it should take a few minutes to start
login is msfadmin and password is msfadmin
- Shut down the machine

Install kali linux



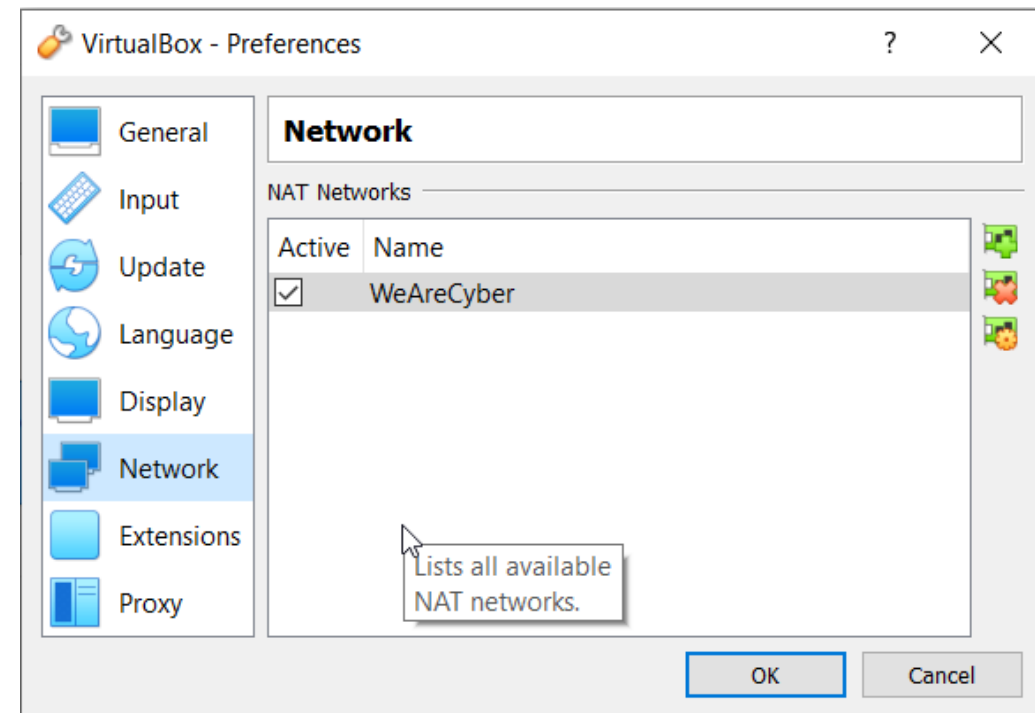
- Go to virtualbox and click on "File" > "Import Appliance..."
- Click on the yellow folder and navigate to the image of kali you downloaded, select it and click on open
- Click on next and then click on import
- It will take a little while...
- And then launch it for the first time
- Username: root
- Password: toor
- Shut down the machine



Connect our machines together

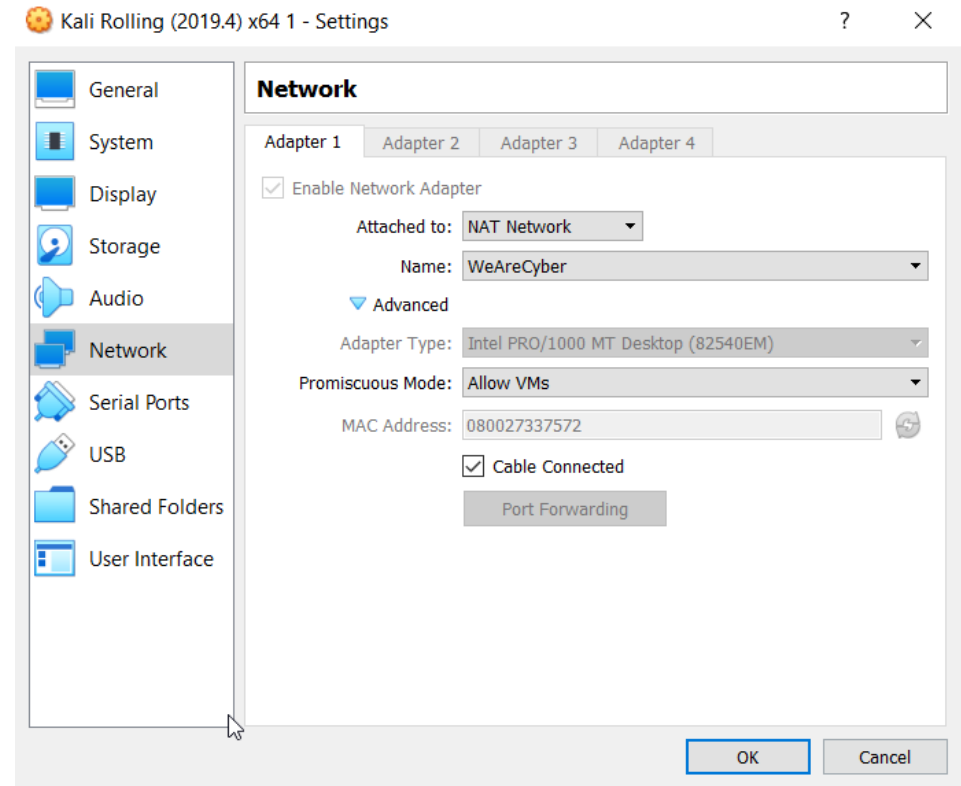


- Go to virtualbox
- Click on file > preferences > network
- Click on the plus
- Rename the network as you like or leave it like this
- And click on ok



- Click on Metasploitable
- Settings
- Network
- And select Nat Network from the dropdown menu
- And then ok
- Ensure that Allows VM is selected in promiscuous mode
- Do the Same for the kali machine
- Launch both the machine

For more information on connection of VM together you can refer to this link: <https://www.virtualbox.org/manual/ch06.html>





See if our machines can connect

- In your Metasploitable type "ip a" and check your ip address
- In you kali open the terminal and type ping <IP-OF-METASPLOITABLE>
 - In my case: ping 10.0.2.4
 - My kali can access metasploitable

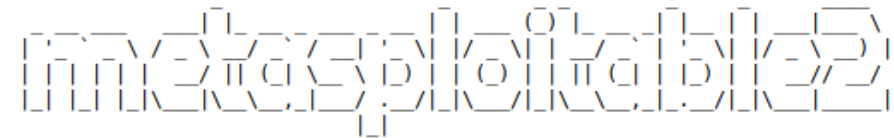
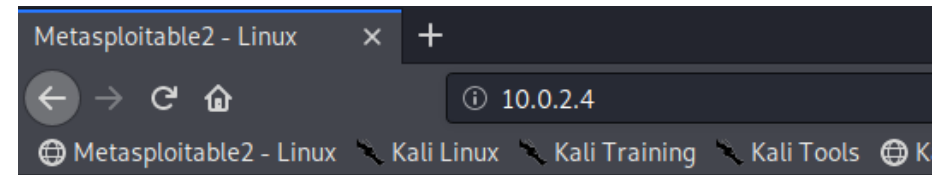
```
root@kali:~# ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=1.15 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=1.11 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=1.04 ms
^C
--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4336ms
rtt min/avg/max/mdev = 1.037/1.097/1.146/0.035 ms
```

- Now type ip a in your kali and ping it from your Metasploitable.
- They can connect to each other both ways.



Start to work on our skills

- Open the navigator from your kali and type:
 - `http://<your-metasploitable-ip>`
 - In my case: <http://10.0.2.4/>
 - You should land on this page:
 - We will explore Mutillidae and DVWA



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



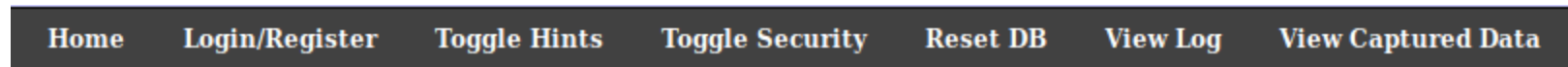
Setup the proper config for Mutillidae

- In order for mutillidae to work properly we need to change the config file.
- In Metasploitable VM navigate to `/var/www/mutillidae`
- Type, “`sudo nano config.inc`”
- Change the database name from ‘metasploit’ to ‘owasp10’
- Close and save the changes

Mutillidae exploration



Click on the link to mutillidae



Most useful menu item

Toggle hints: will activate or deactivate the hints. If you are a beginner you should activate them

Toggle security: Change the level of security of the application. Start at level 0

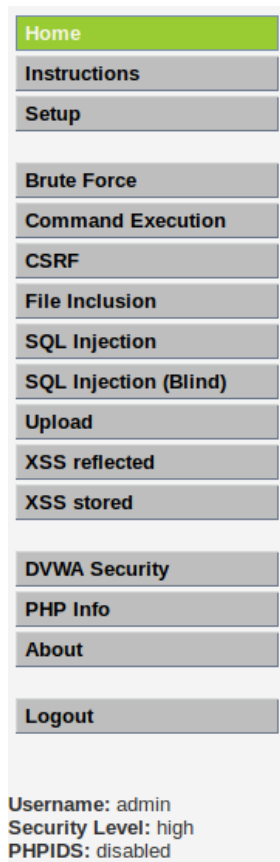
Reset DB: Will reset the database in case you feel like the app is not working properly or in case you break it :D

Now you can start learning but before, let's have a quick look at DVWA

DVWA exploration



- Connect to the app with the help of the hint under the form
 - Hint: default username is 'admin' with password 'password'



Most useful menu item:

Setup: you will be able to reset the database

DVWA Security: you will be able to change the security for it to make it harder to hack. I recommend starting with low.

The items in the middle are different attacks you can try out.

ENJOY!



Similar projects

- A very complete list of similar projects:
 - <https://owasp.org/www-project-vulnerable-web-applications-directory/>
- List of resources I made for self education:
 - <https://gabrielleb.fr/blog/2018/09/16/ressources-resources/>

And now...



Practice your skills on your brand new lab.



I hope you enjoyed this presentation, if you have any question ask away
:D