Name: Patrick niederhauser

Date: 12/3/2021

Course: Information and Security

Semester: Fall 2021

Using Owasp Brick to increase our knowledge on SQL injections

Overview

In this lab we are going to set up two virtual machines (1) a windows 10 vm and (2) a linux kali vm. We are going to use Windows 10 as a server host, which will be hosting our Bricks database. We then are going to connect to our host from our kali machine which we will be using as our attacker. The main outcome of this lab is to successfully achieve an sql injection attack on our Bricks database.

Expected Outcomes

- To get a basic understanding of how to use uWamp to host web servers
- To understand the importance of proper security protocols
- How the bricks database functions
- How an attacker might use an sql injection attack

Resources

- Application name: oWasp bricks
- Hardware Used: Windows 10 virtual machine, and Kali linux VM
- Web resources used: https://www.uwamp.com/en/?page=download ,

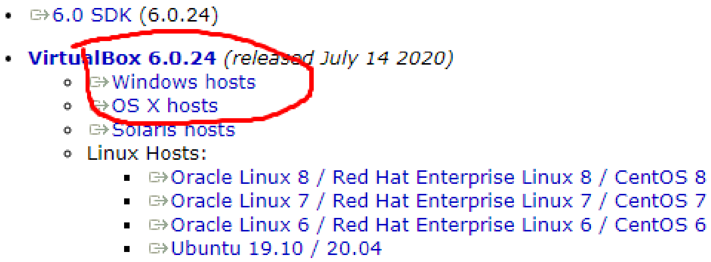
  https://sechow.com/bricks/download.html

  https://www.kali.org/get-kali/

  https://www.microsoft.com/en-us/software-download/windows10

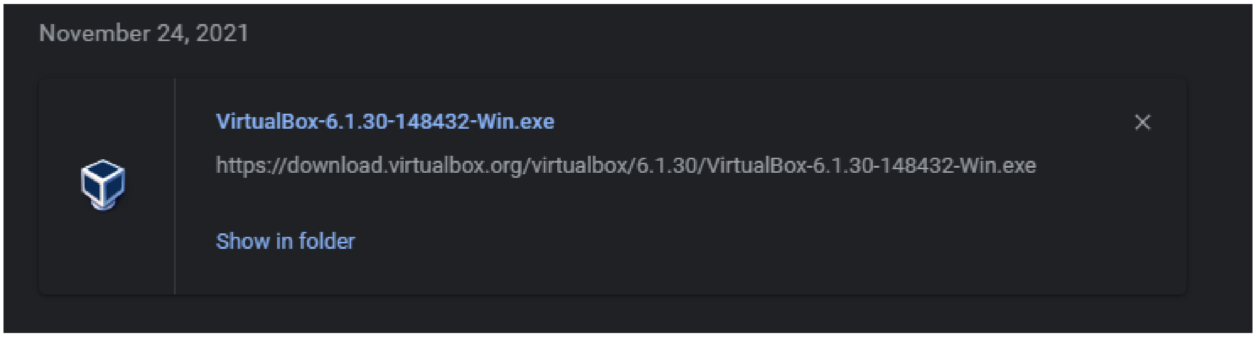
VirtualBox set-up and steps/installation

1. I went to https://www.virtualbox.org/ and downloaded the recentes version of VirtualBox .I'm using a windows machine, so I downloaded the windows version



- ⇨6.0 SDK (6.0.24)
- VirtualBox 6.0.24 *(released July 14 2020)*
  - ⇨Windows hosts
  - ⇨OS X hosts
  - ⇨Solaris hosts
  - Linux Hosts:
    - ⇨Oracle Linux 8 / Red Hat Enterprise Linux 8 / CentOS 8
    - ⇨Oracle Linux 7 / Red Hat Enterprise Linux 7 / CentOS 7
    - ⇨Oracle Linux 6 / Red Hat Enterprise Linux 6 / CentOS 6
    - ⇨Ubuntu 19.10 / 20.04

2. Next step is to click the download.exe file once your download is finished.

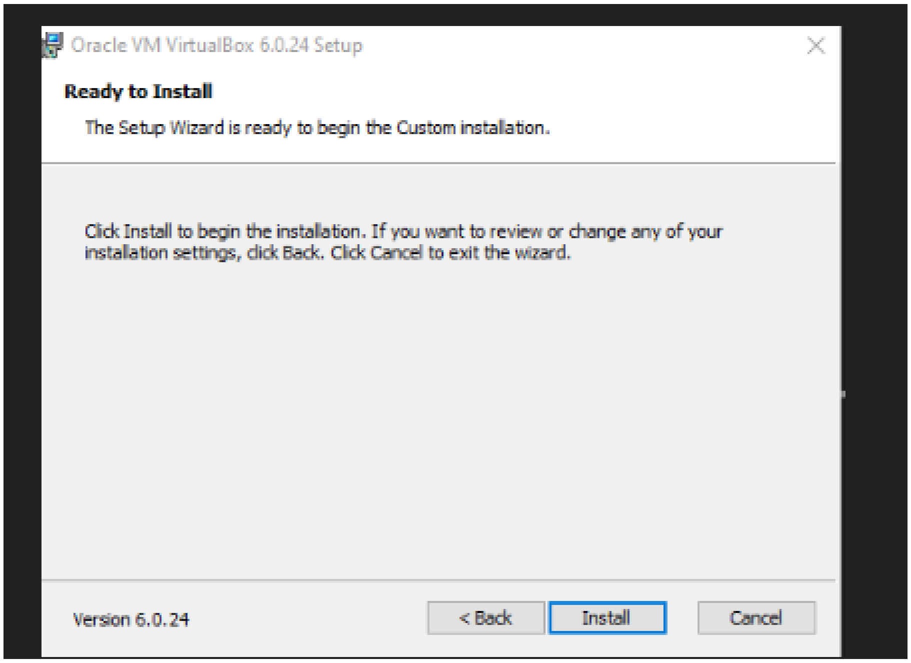


November 24, 2021

VirtualBox-6.1.30-148432-Win.exe

https://download.virtualbox.org/virtualbox/6.1.30/VirtualBox-6.1.30-148432-Win.exe

3. Now we have to follow the instructions we are prompted with, click “next” to continue the installation and then click install.



Oracle VM VirtualBox 6.0.24 Setup

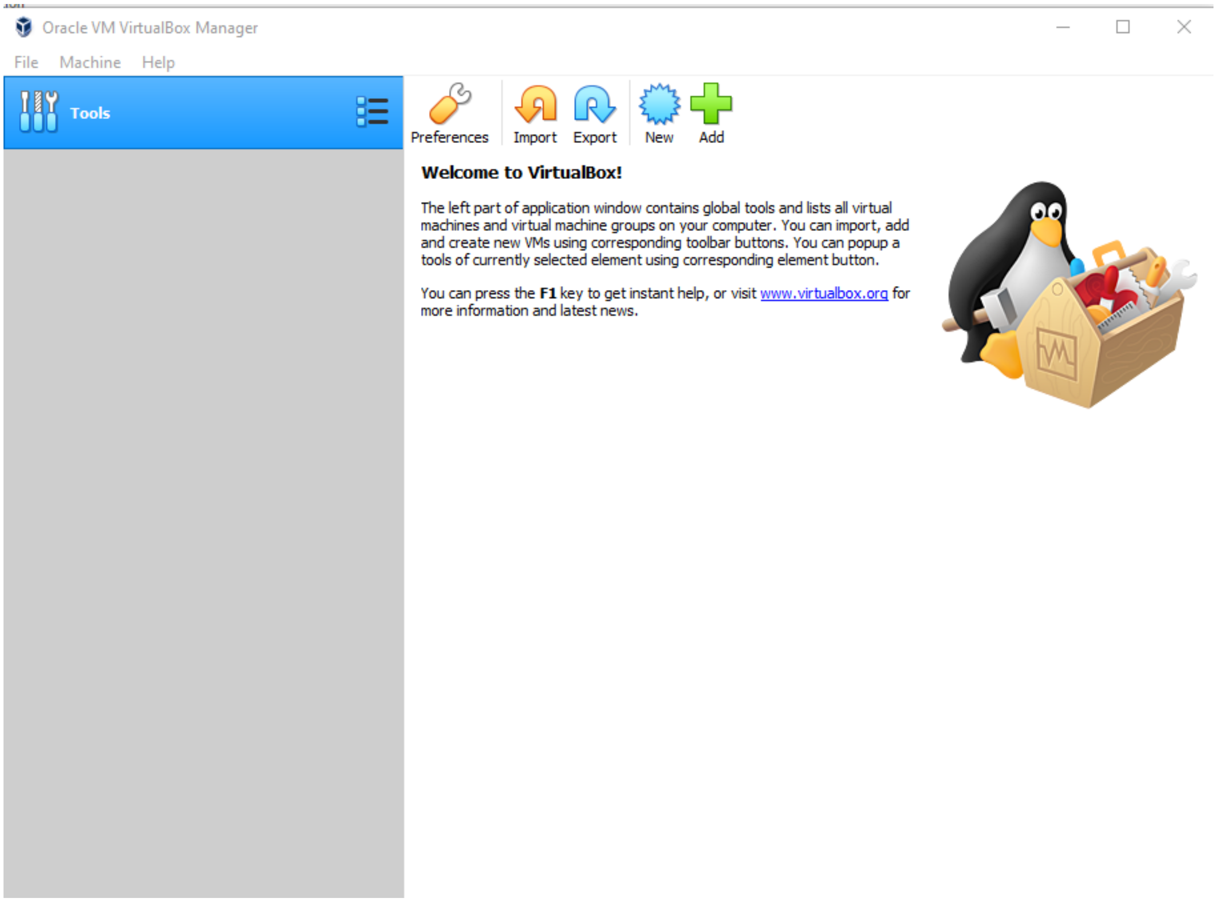
Ready to Install

The Setup Wizard is ready to begin the Custom installation.

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Version 6.0.24

4. After clicking finish install we have now installed VmBox and our ready to install our windows and linux macience



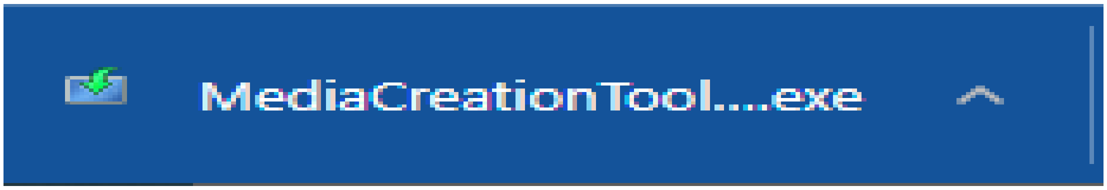
Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

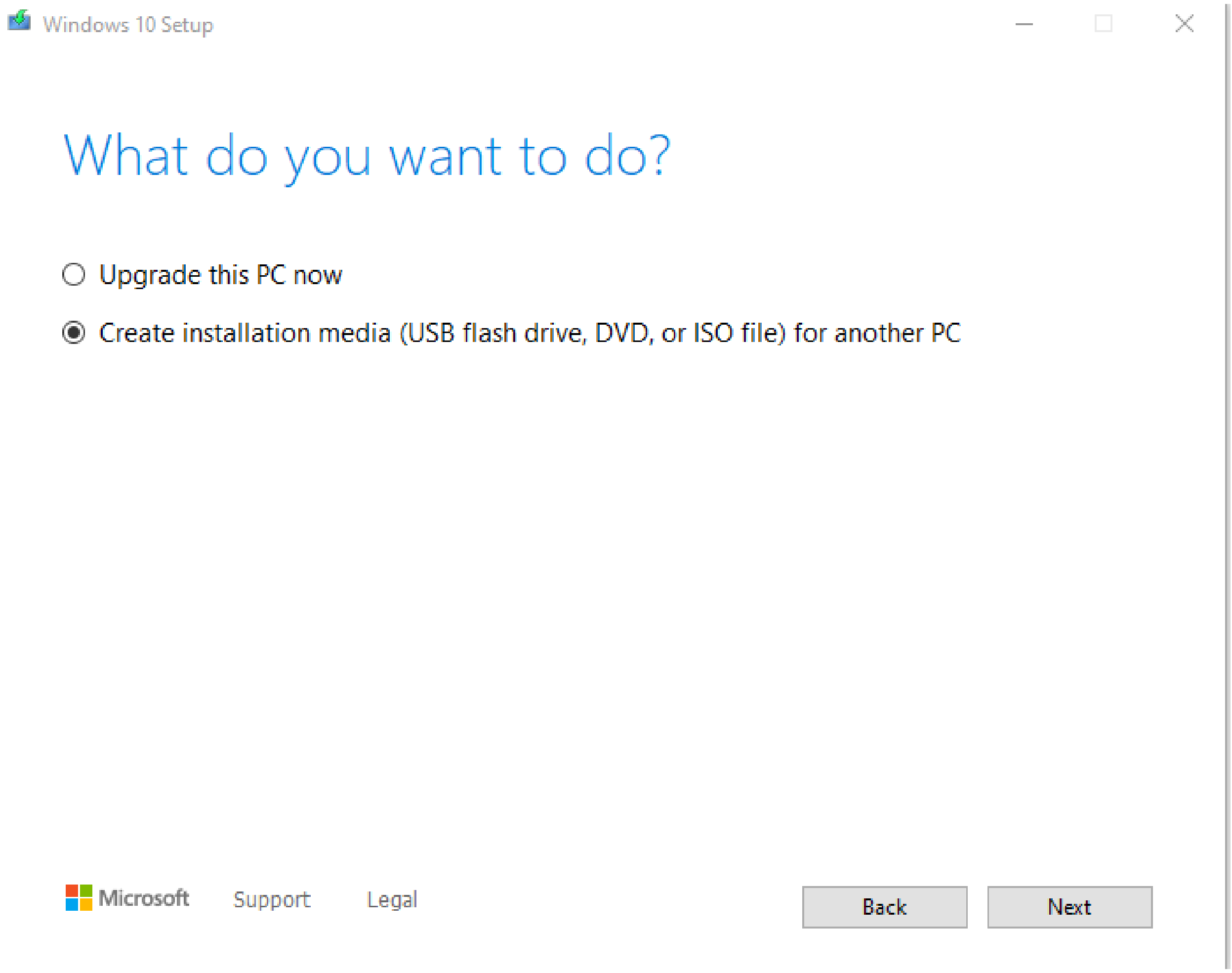
5. Our next step in this installation process is to download the windows, and kali iso. We need these iso in order to install the operating system on the virtual machines. Downloading our windows iso

6. For the windows machine I went to **https://www.microsoft.com/en-us/software-download/windows10**, and clicked the **download tool button**. I then waited for it to download and click the exe file



MediaCreationTool....exe

7. I then clicked **accept** and then clicked **“Create installation media (usb flash drive, DVD or iso file) for another pc.** We want the iso file because this is what we are going to use for our windows 10 machine



Windows 10 Setup

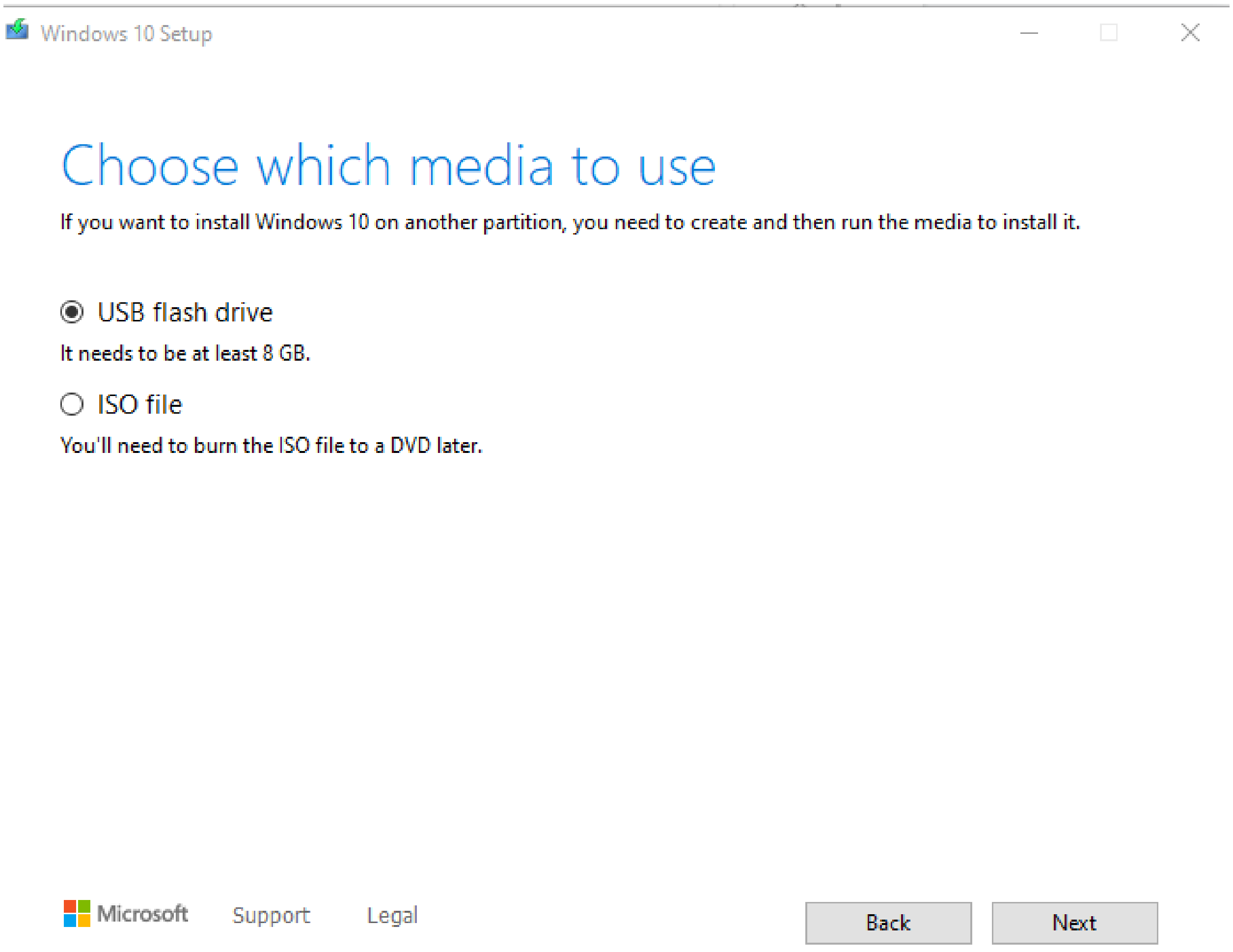
What do you want to do?

○ Upgrade this PC now

● Create installation media (USB flash drive, DVD, or ISO file) for another PC

8. After hitting next, we are then prompted with a download screen. Once again we want to choose the iso selection as we want to have an iso file for

our virtual machine to boot off of.



Windows 10 Setup

Choose which media to use

If you want to install Windows 10 on another partition, you need to create and then run the media to install it.

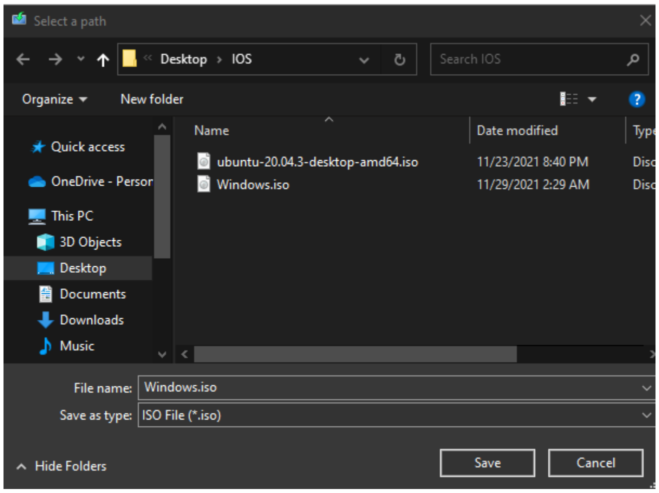
● USB flash drive

It needs to be at least 8 GB.

○ ISO file

You'll need to burn the ISO file to a DVD later.

9. We then need to select a folder to save the iso File into, i created a folder on my desktop called iso and just selected that

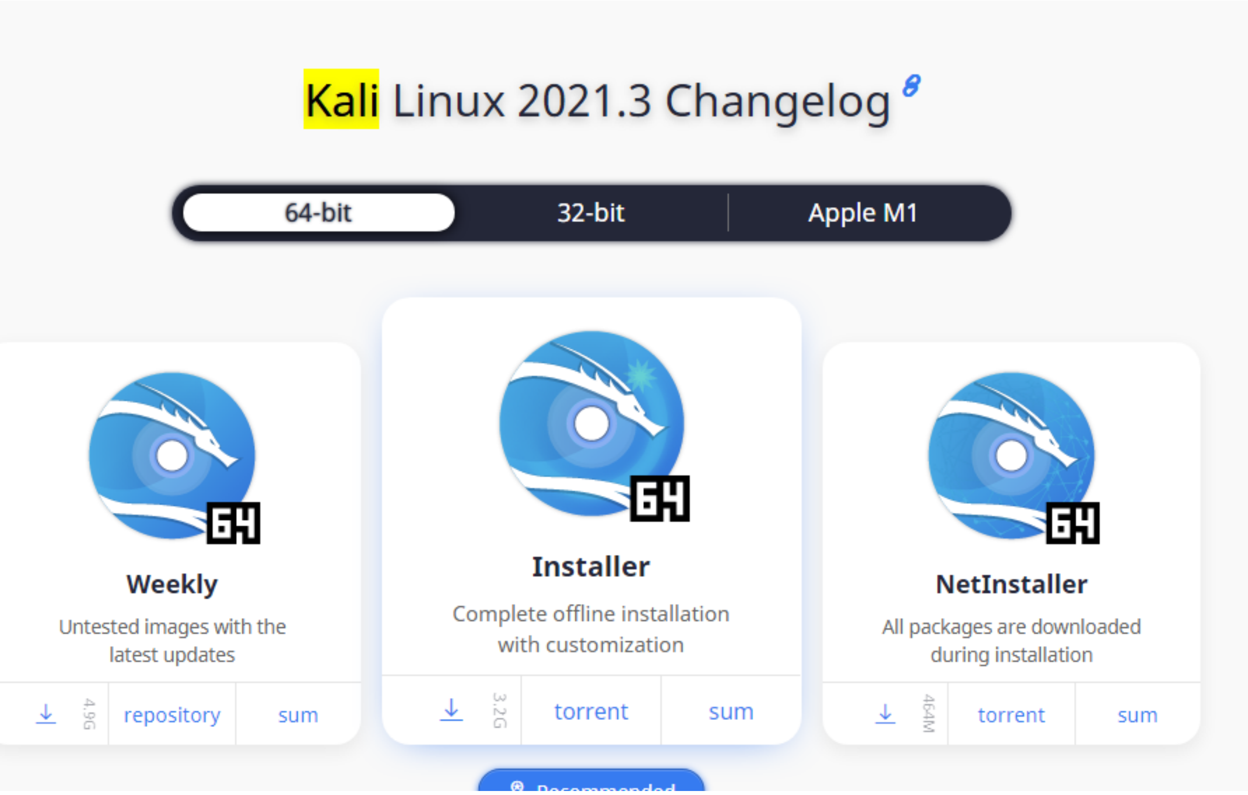


Name	Date modified	Type
ubuntu-20.04.3-desktop-amd64.iso	11/23/2021 8:40 PM	Disc
Windows.iso	11/29/2021 2:29 AM	Disc

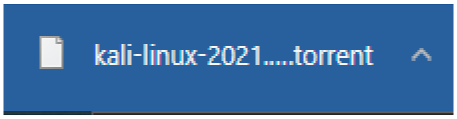
File name: Windows.iso

Save as type: ISO File (*.iso)

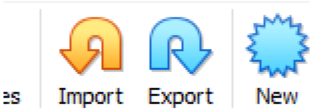
10. After hitting save we now have to wait for windows to install, but we have our windows iso. So now the focus is turned to kali, by going to **https://www.kali.org/get-kali/#kali-platforms** i was able to download a screenshot of kali which made this installation process a lot easier. However it is different from our windows machine setup. By clicking on the link and then click on the download **kali-linus-2021-torrent** we are able to start our kali installation.


Kali Linux 2021.3 Changelog
64-bit
32-bit
Apple M1
Weekly
Untested images with the latest updates
4.9G
repository
sum
Installer
Complete offline installation with customization
3.2G
torrent
sum
NetInstaller
All packages are downloaded during installation
464M
torrent
sum

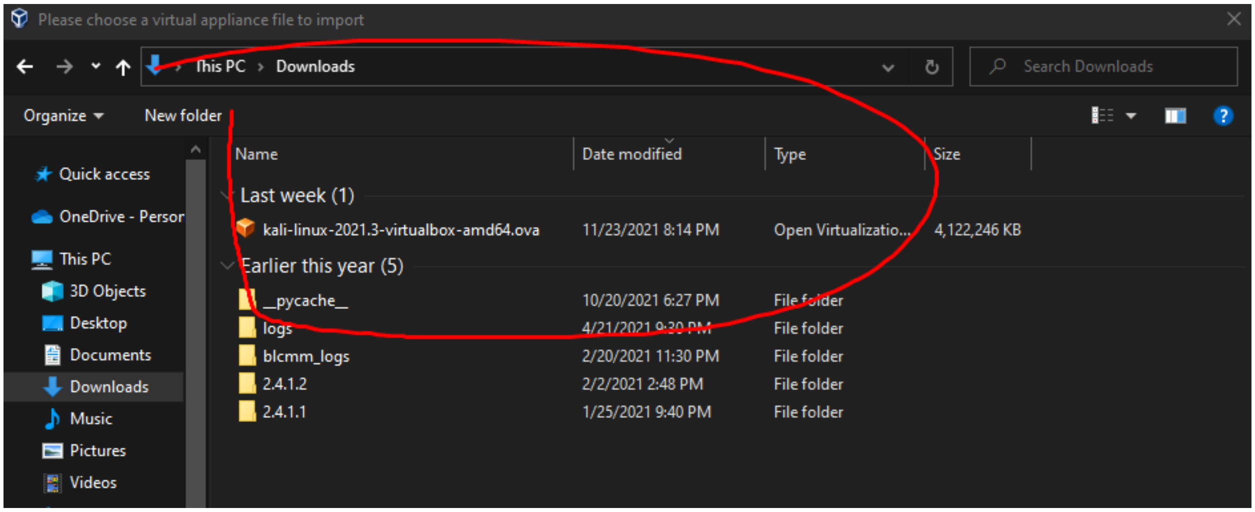
11. Once kali is downloaded we are all set to move foward



12. The next step is to start configuring our virtual machines. Starting with the kali machine we first need to go to the Virtual box and select the **import** button.



13. After selecting import we are then going to select **kali-linus-2021-torrent** that we just downloaded. This file is going to be in our **downloads folder.** So once you find it all you have to do is select and hit next. Virtual box will do the rest for you.

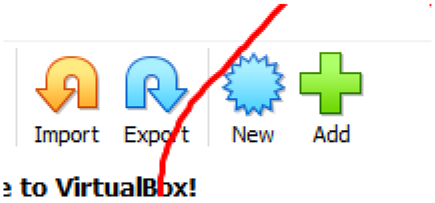


Please choose a virtual appliance file to import

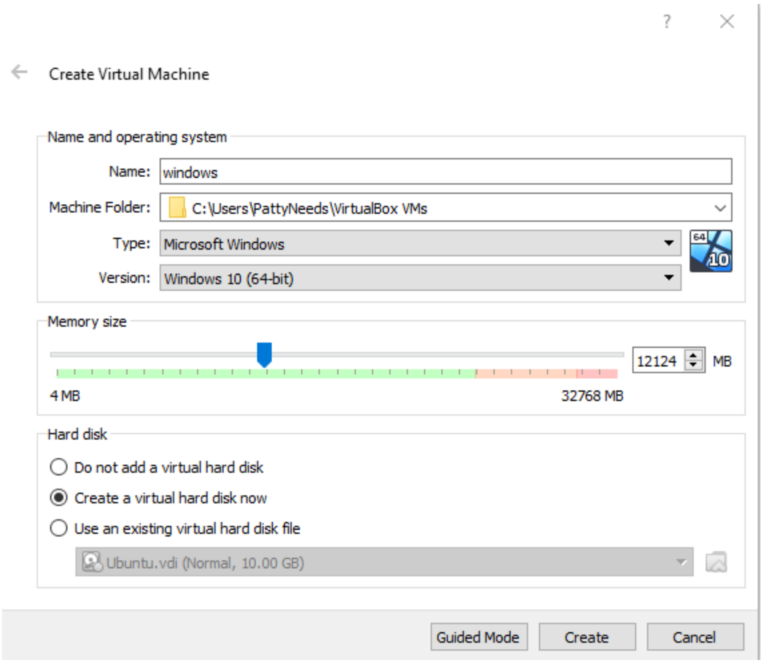
This PC › Downloads

Name	Date modified	Type	Size
Last week (1)			
kali-linux-2021.3-virtualbox-amd64.ova	11/23/2021 8:14 PM	Open Virtualizatio...	4,122,246 KB
Earlier this year (5)			
__pycache__	10/20/2021 6:27 PM	File folder	
logs	4/21/2021 9:30 PM	File folder	
blcmm_logs	2/20/2021 11:30 PM	File folder	
2.4.1.2	2/2/2021 2:48 PM	File folder	
2.4.1.1	1/25/2021 9:40 PM	File folder	

14. We can now start configuring our windows machine. We first need to go to tools on the virtual box, and select the new button. **Since windows is an ISO and not a snapshot we have to configure the machine from scratch.**



15. We now need to create our windows machine, we first change the name to **Windows**, we then **Make the type windows, and the version windows 10.** I also increased the ram size to increase performance. Once you have your settings right you can **hit Create**.



Create Virtual Machine

Name and operating system

Name: windows

Machine Folder: C:\Users\PattyNeeds\VirtualBox VMs

Type: Microsoft Windows

Version: Windows 10 (64-bit)

Memory size

12124 MB

Hard disk

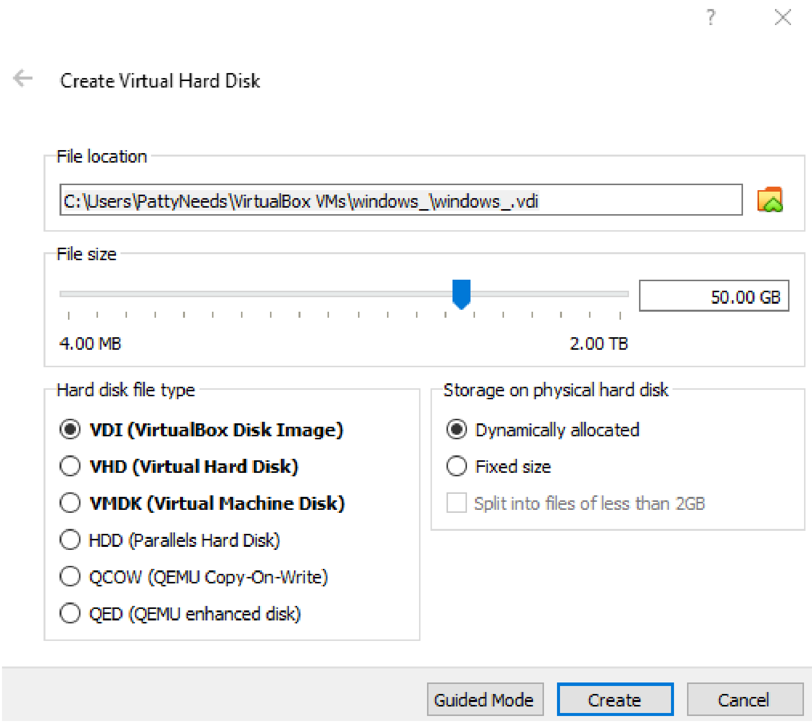
○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Ubuntu.vdi (Normal, 10.00 GB)

16. We don't need to change anything here, so we can also just hit create again.



Create Virtual Hard Disk

File location

C:\Users\PattyNeeds\VirtualBox VMs\windows_\windows_.vdi

File size

50.00 GB

Hard disk file type

● **VDI (VirtualBox Disk Image)**

○ **VHD (Virtual Hard Disk)**

○ **VMDK (Virtual Machine Disk)**

○ HDD (Parallels Hard Disk)

○ QCOW (QEMU Copy-On-Write)

○ QED (QEMU enhanced disk)

Storage on physical hard disk

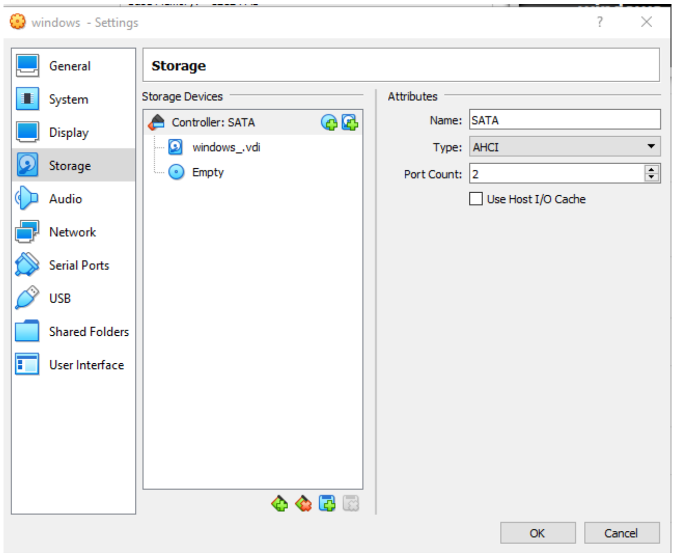
● Dynamically allocated

○ Fixed size

□ Split into files of less than 2GB

17. The next step is to install the ISO into our windows 10 machine. By clicking on the new windows system you have and then clicking on the settings you are able to edit the machine. We want to edit the **storage function** of this machine, so we are going to select

storage on the right hand side.



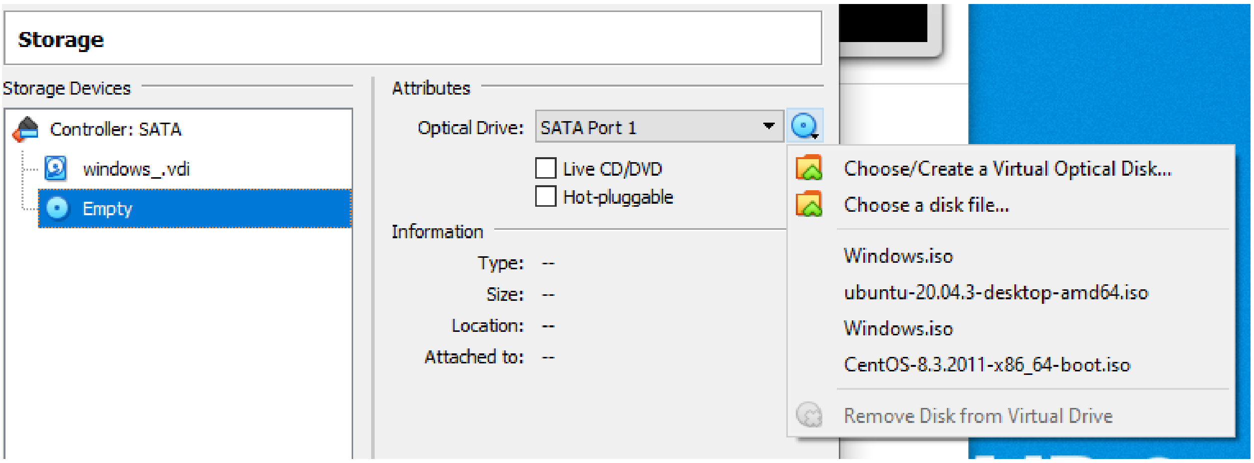
Name: SATA

Type: AHCI

Port Count: 2

□ Use Host I/O Cache

18. By selecting the empty drive and then selecting the little disk on the right hand side we are able to insert our ISO



Optical Drive: SATA Port 1

□ Live CD/DVD

□ Hot-pluggable

Type: --

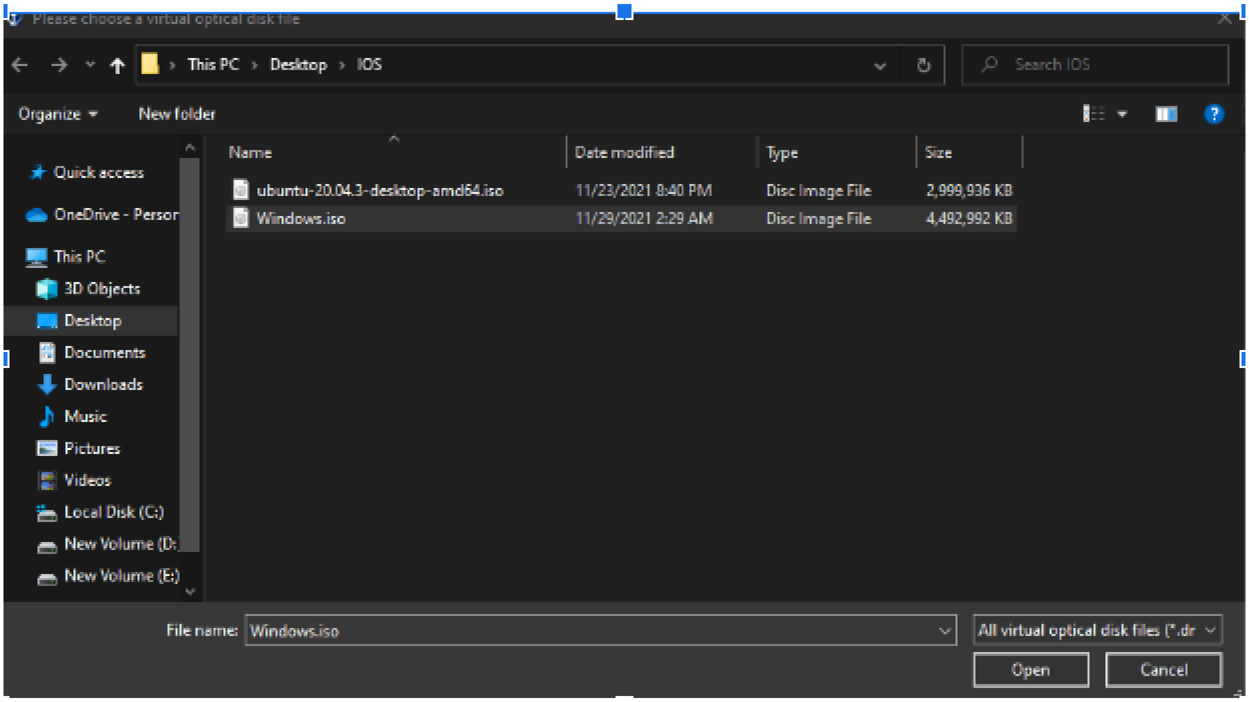
Size: --

Location: --

Attached to: --

Storage
Storage Devices
Controller: SATA
windows_.vdi
Empty
Attributes
Information
Choose/Create a Virtual Optical Disk...
Choose a disk file...
Windows.iso
ubuntu-20.04.3-desktop-amd64.iso
Windows.iso
CentOS-8.3.2011-x86_64-boot.iso
Remove Disk from Virtual Drive

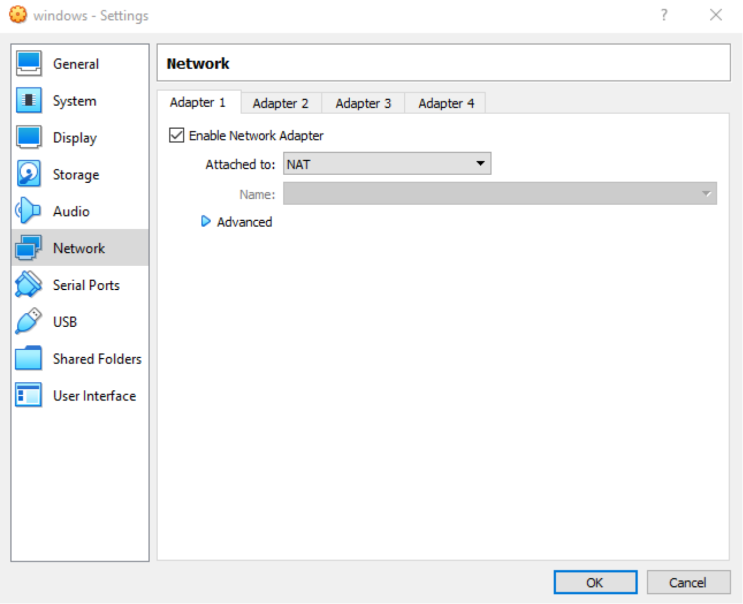
19. Once you select the disk you want to click Choose a disk File this will open up to our fille system. We then want to go into our file system and find the folder we made early for our windows ISO. Once you find it you can select hit and hit open. This links our iso to our boot drive for our windows machine.



Name	Date modified	Type	Size
ubuntu-20.04.3-desktop-amd64.iso	11/23/2021 8:40 PM	Disc Image File	2,999,936 KB
Windows.iso	11/29/2021 2:29 AM	Disc Image File	4,492,992 KB

File name: Windows.iso

20. We now have our windows and our linux machine already to boot for the first time. However we first must change their network in order to get internet on the VMs. To do this we want to select the windows machine and click settings again. We then want to go into the Network settings and change the Adapter 1 settings to NAT,

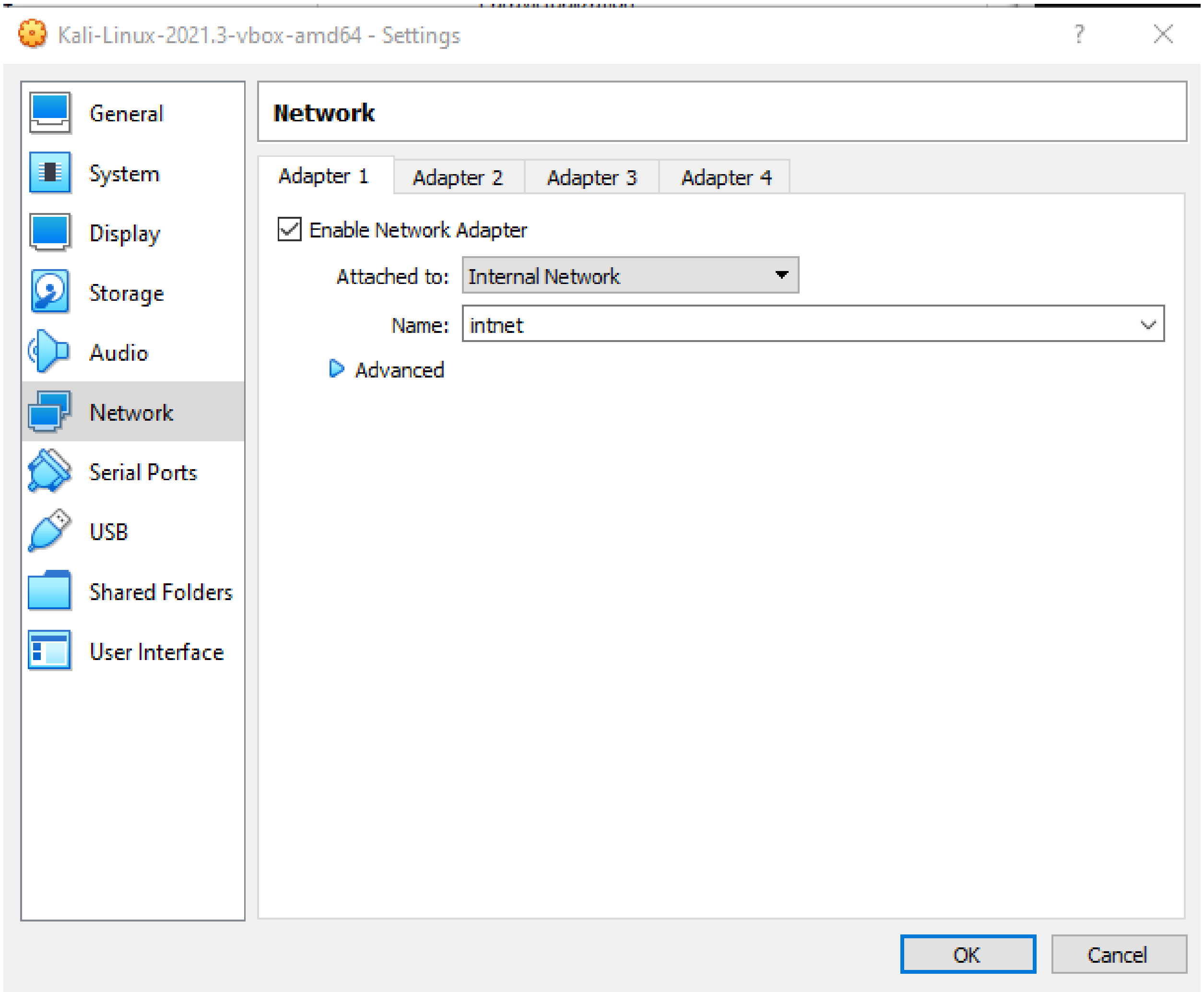


☑ Enable Network Adapter

Attached to: NAT

Name:

21. The last step is to change the network settings for our linus machine. We click on linux and then click the settings tab we then go into the network settings and change the **adapter 1 settings to Internal network, and internet as the name.** Our linux machine is now done and we are ready to start.



Kali-Linux-2021.3-vbox-amd64 - Settings

Network

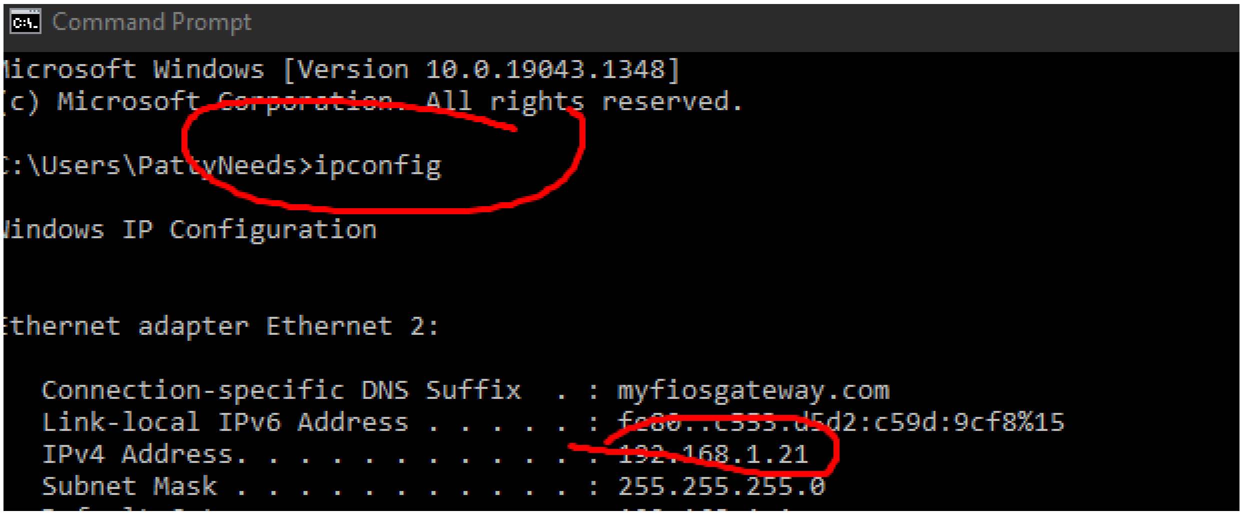
☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

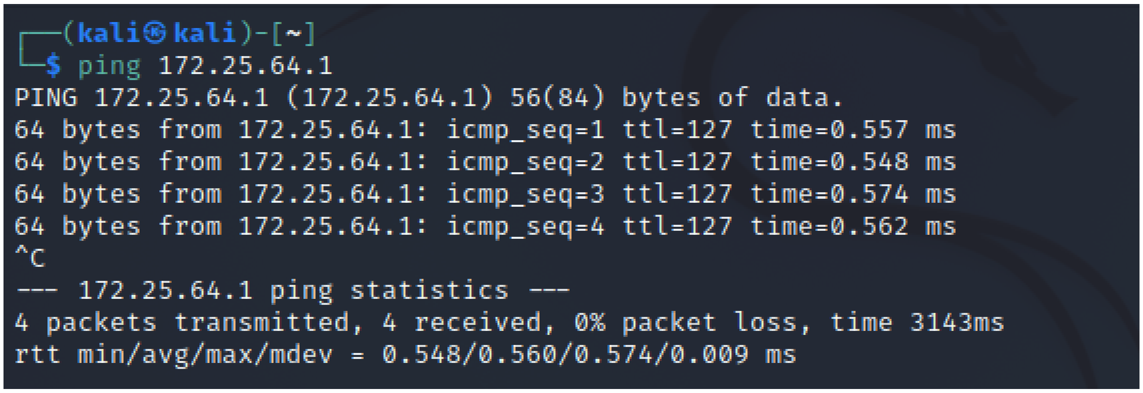
Hands-on activity step/instructions

1. Now that our virtual machines are all up and running we are going to start on the hands-on activities. The first thing we want to do is ensure that our windows machine and our linux machine can ping each other. To do this we are going to need to run IPconfig in cmd on the windows machine to get its ip address.



```
icrosoft Windows [Version 10.0.19043.1348]
c) Microsoft Corporation. All rights reserved.

:\Users\PattyNeeds>ipconfig

indows IP Configuration


thernet adapter Ethernet 2:

  Connection-specific DNS Suffix  . : myfiosgateway.com
  Link-local IPv6 Address . . . . . : fe80::c555:d5d2:c59d:9cf8%15
  IPv4 Address. . . . . . . . . . . : 192.168.1.21
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

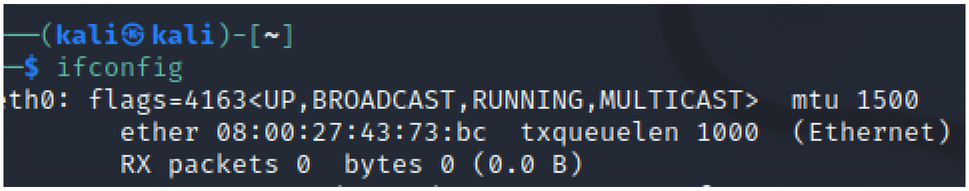
2. After that we are going to open the terminal on kali and ping this ip and see if we get any packet loss. We do this by running the command **Ping 172.25.64.1**



```
┌──(kali㉿kali)-[~]
└─$ ping 172.25.64.1
PING 172.25.64.1 (172.25.64.1) 56(84) bytes of data.
64 bytes from 172.25.64.1: icmp_seq=1 ttl=127 time=0.557 ms
64 bytes from 172.25.64.1: icmp_seq=2 ttl=127 time=0.548 ms
64 bytes from 172.25.64.1: icmp_seq=3 ttl=127 time=0.574 ms
64 bytes from 172.25.64.1: icmp_seq=4 ttl=127 time=0.562 ms
^C
--- 172.25.64.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3143ms
rtt min/avg/max/mdev = 0.548/0.560/0.574/0.009 ms
```

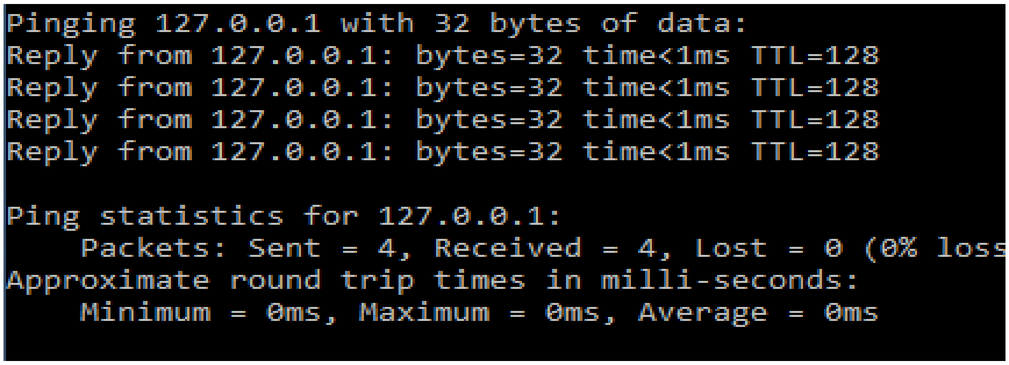
3. Since we have 0 packet loss we can confirm that our windows machine is being pinged by our kali. After that we are going to run ifconfig on kali in the terminal to get the kalis

ip address.



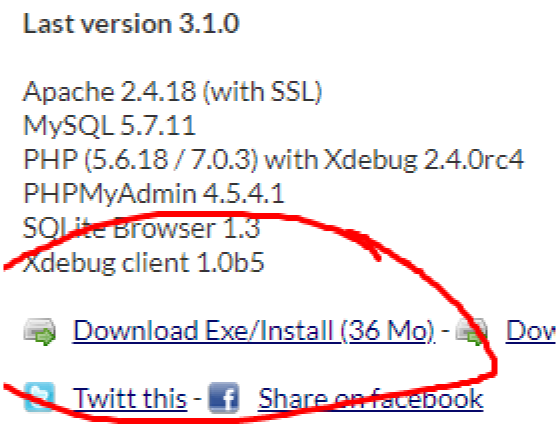
```
—(kali㉿kali)-[~]
—$ ifconfig
th0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:43:73:bc  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
```

4. We then want to ping kali from the windows machine by running the command ping 127.0.0.1



```
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

5. Now that we can confirm that our machines can ping themselves we can start installing our server. The first thing we are going to install is the uWamp Server. By going to https://www.uwamp.com/en/?page=download and downloading the most recent version we are able to start our installation process.

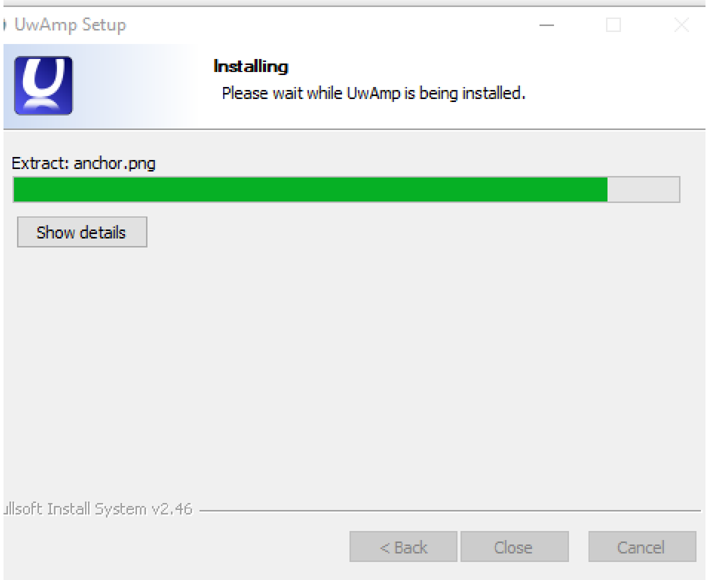


Last version 3.1.0

Apache 2.4.18 (with SSL)
MySQL 5.7.11
PHP (5.6.18 / 7.0.3) with Xdebug 2.4.0rc4
PHPMyAdmin 4.5.4.1
SQLite Browser 1.3
Xdebug client 1.0b5

Download Exe/Install (36 Mo) - Dov
Twitt this - Share on facebook

6. Once it is installed we have to run it, by **clicking next and then install** we are almost done with the installation process



UwAmp Setup

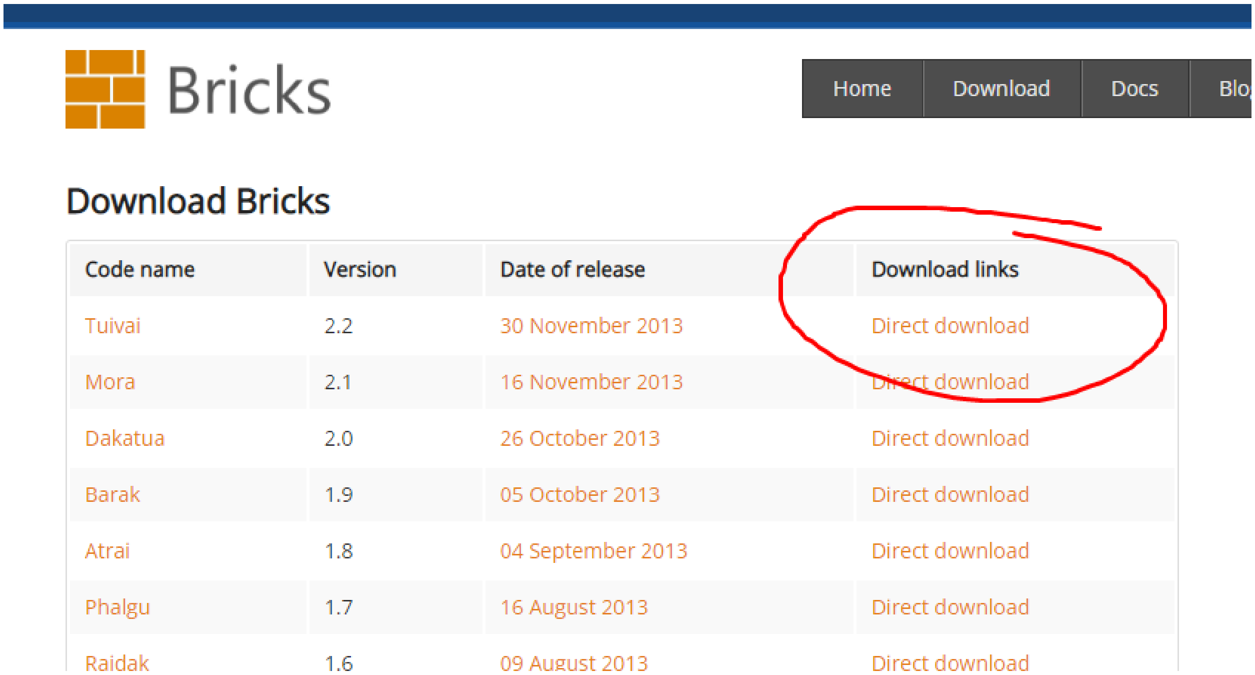
Installing

Please wait while UwAmp is being installed.

Extract: anchor.png

ullsoft Install System v2.46

7. We now need to install oWasp bricks, this is our main project for this pen test. By going to https://sechow.com/bricks/download.html and click the most recent download link the download will begin.

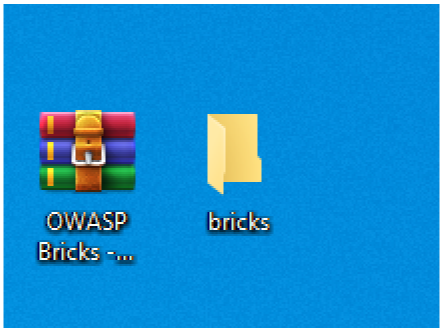


Download Bricks

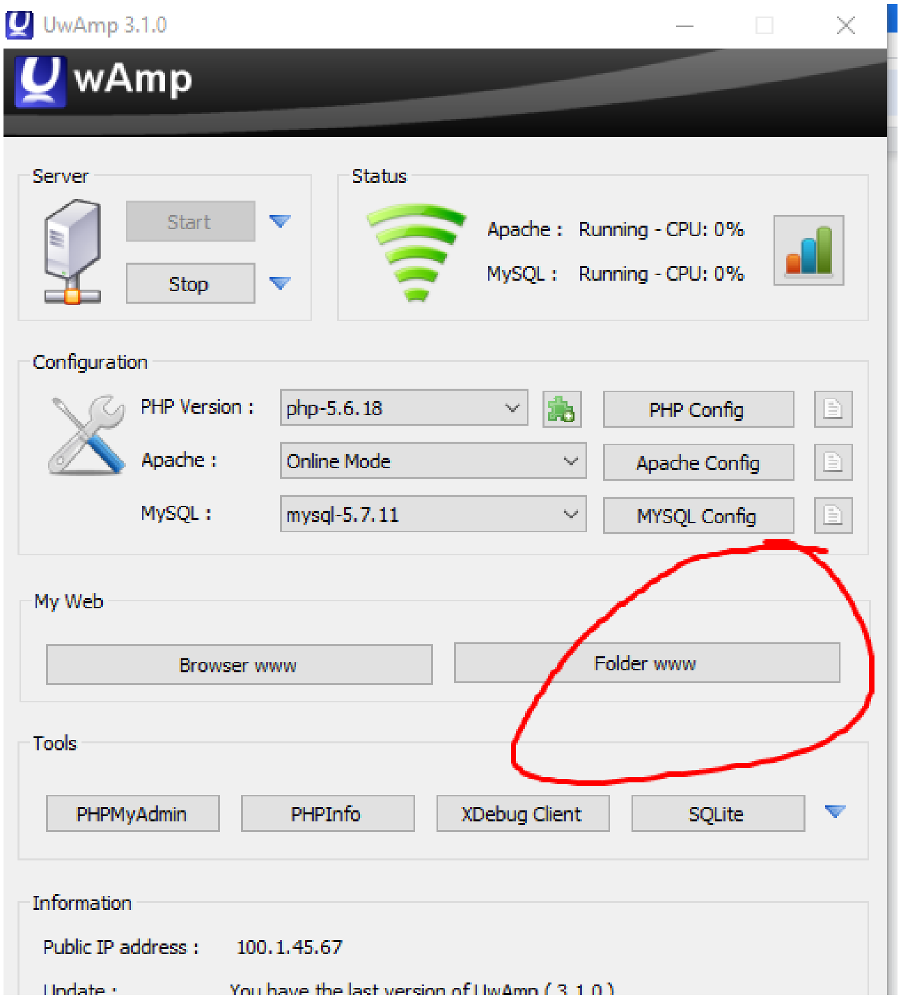
Code name	Version	Date of release	Download links
Tuivai	2.2	30 November 2013	Direct download
Mora	2.1	16 November 2013	Direct download
Dakatua	2.0	26 October 2013	Direct download
Barak	1.9	05 October 2013	Direct download
Atrai	1.8	04 September 2013	Direct download
Phalgu	1.7	16 August 2013	Direct download
Raidak	1.6	09 August 2013	Direct download

8. Bricks downloads as a zip file, so if you don't have a unzipper such as winrar or 7zip you

need the before proceeding forward. Once you get bricks download you are just going to unzip the folder to your desktop



9. We now need to set up the database part of this project. We start this by starting our server. So start your uWamp server and select the WWW folder button.



Apache : Running - CPU: 0%

MySQL : Running - CPU: 0%

PHP Version : php-5.6.18

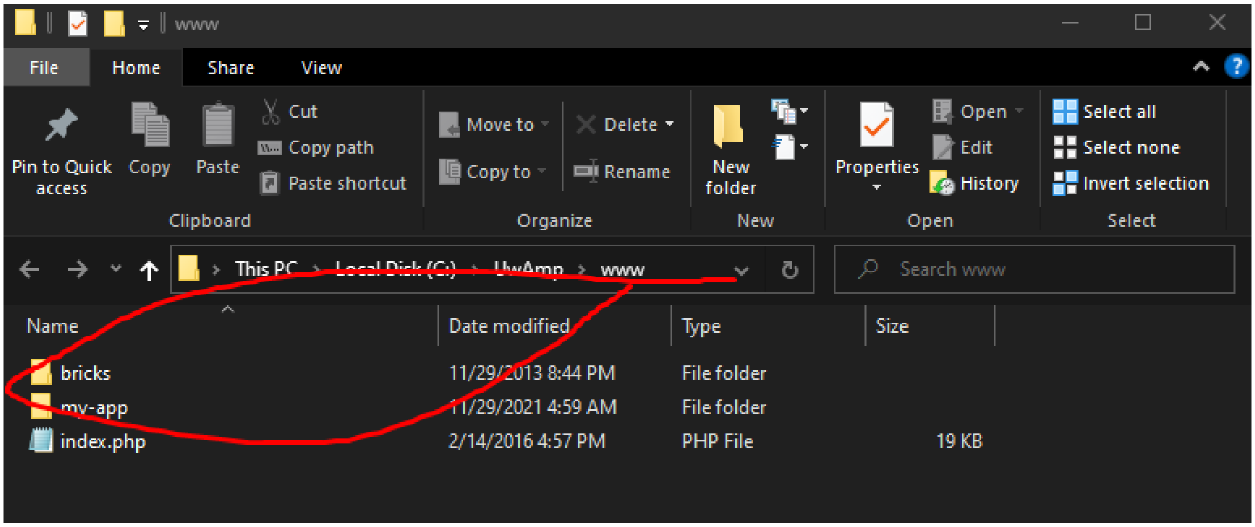
Apache : Online Mode

MySQL : mysql-5.7.11

Public IP address : 100.1.45.67

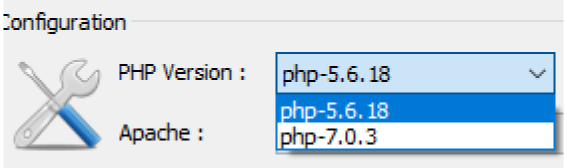
Update : You have the last version of UwAmp (3.1.0)

10. We now want to drop our un zipped bricks database that we just installed into this folder. You can do this by simply just dragging and dropping.



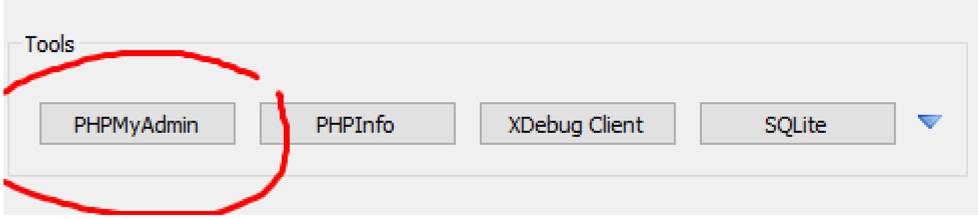
Name	Date modified	Type	Size
bricks	11/29/2013 8:44 PM	File folder	
my-app	11/29/2021 4:59 AM	File folder	
index.php	2/14/2016 4:57 PM	PHP File	19 KB

11. We now have our bricks database in our server and just need to make a few more changes. We need to change the version of PHP that the database is using. Bricks is an older program and needs an older version of PHP to function. However uWamp makes this super easy. You are able to just select an older version of php on the uWamp server screen right where it says **PHP version.** We want the5.6.18 version instead of the 7.0.3 version



PHP Version : php-5.6.18

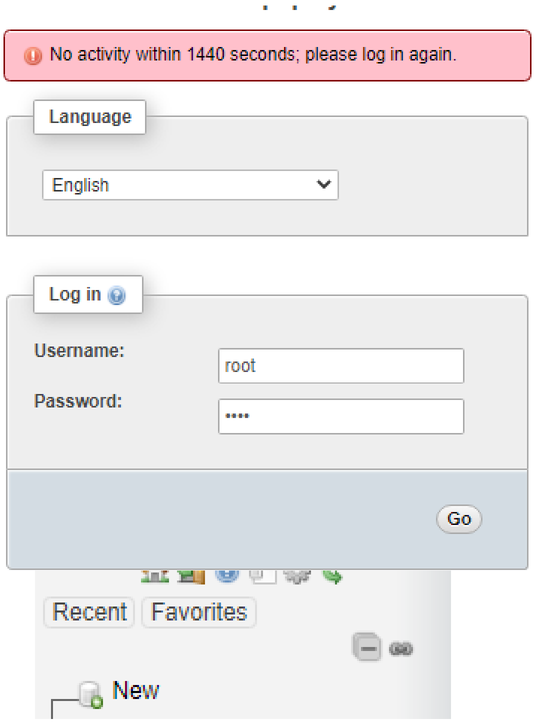
12. Now we have to login into php my admin and configure the database a little more. By selecting phpmyadmin under the tools categories we are able to begin editing our database.



13. Before we can begin editing we first need to longin. The user name and password by default are root.

14. Once we are logged on all we need to do is select the +new button on the left side of the screen. And add a database called bricks.

15. Once you select new all you have to do is put the database name as bricks and hit create.



No activity within 1440 seconds; please log in again.

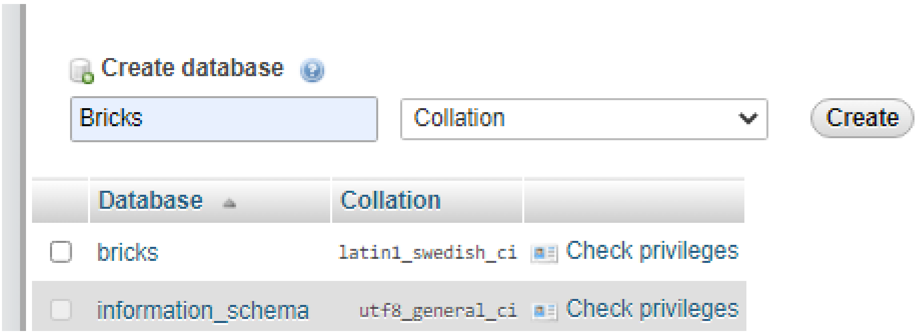
Language

English

Log in

Username: root

Password: ••••



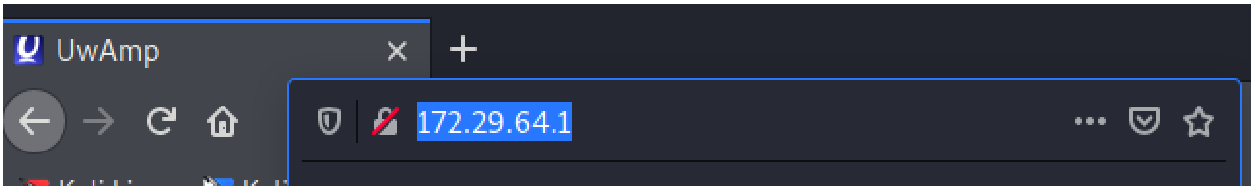
Create database

Bricks

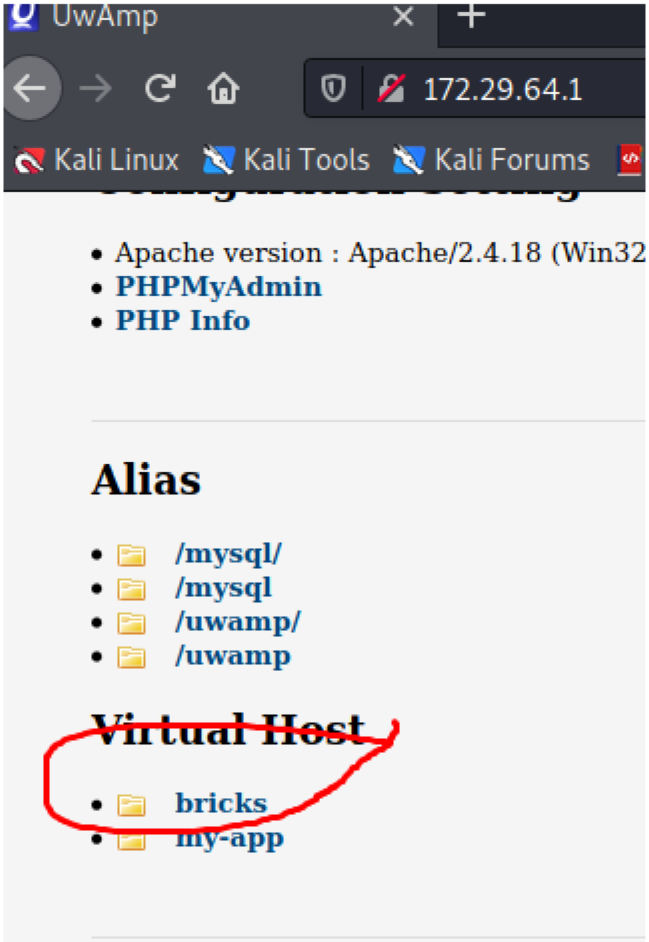
Collation

	Database	Collation	
□	bricks	latin1_swedish_ci	Check privileges
□	information_schema	utf8_general_ci	Check privileges

16. Our database is now all set up and we are ready to begin attacking it using kali. We can simply connect to our server from kali by going to firefox and typing in our windows ip in the search bar.



17. We are then greeted by our new web servers host screen. We now need to select the bricks virtual host because that is what we are going to be working on.



- Apache version : Apache/2.4.18 (Win32
- PHPMyAdmin
- PHP Info

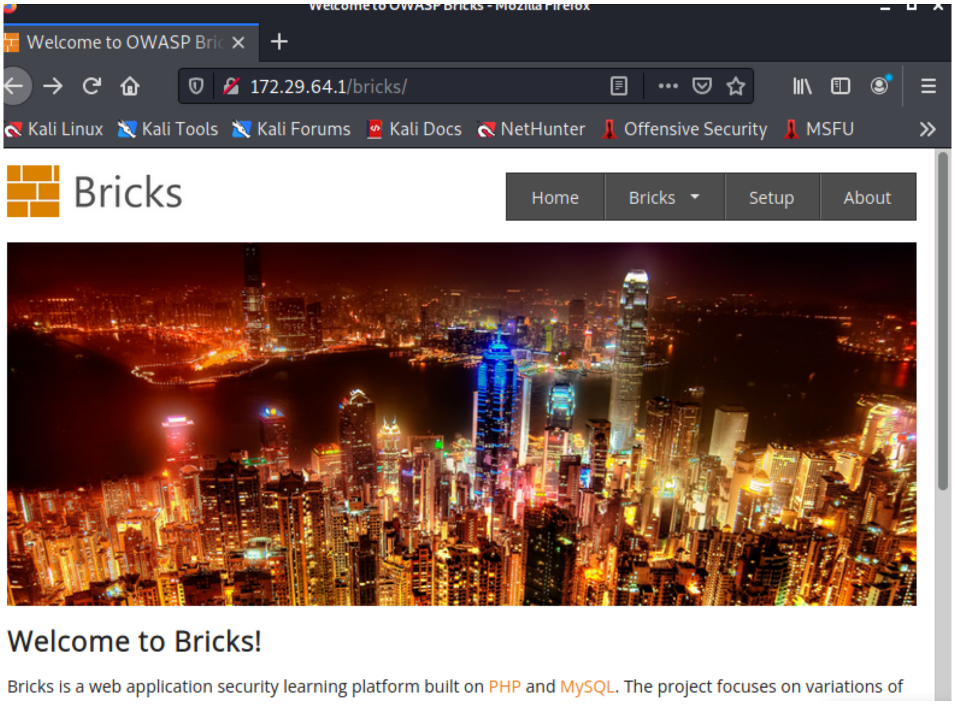
Alias

- /mysql/
- /mysql
- /uwamp/
- /uwamp

Virtual Host

- bricks
- my-app

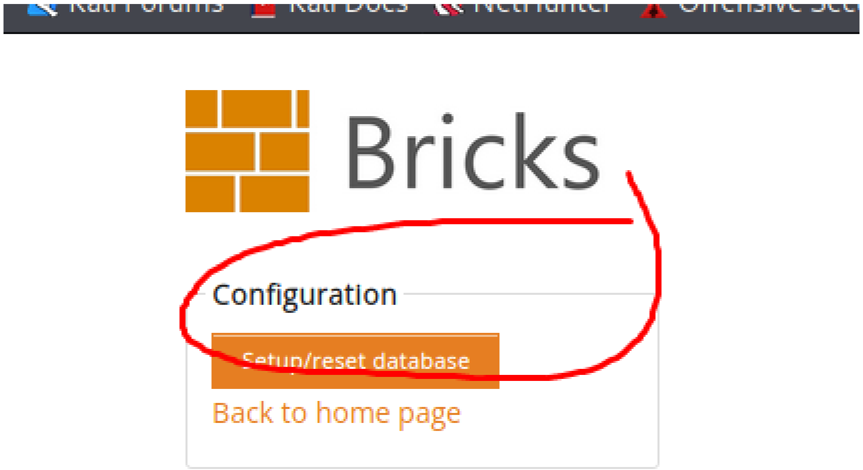
18. We are now on the bricks website and just need to do one final step of installation. We need to click on the setup tab and finish our database setup.



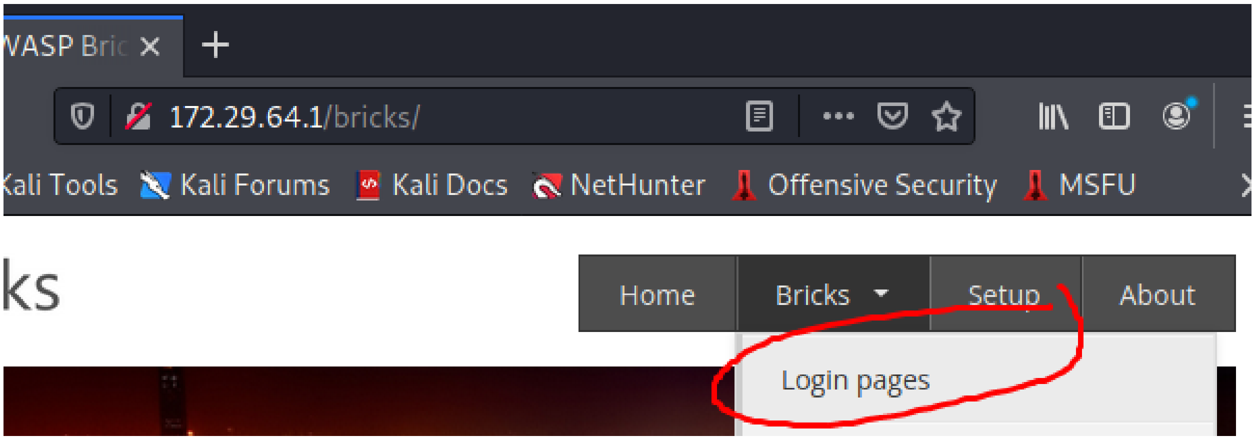
Welcome to Bricks!

Bricks is a web application security learning platform built on PHP and MySQL. The project focuses on variations of

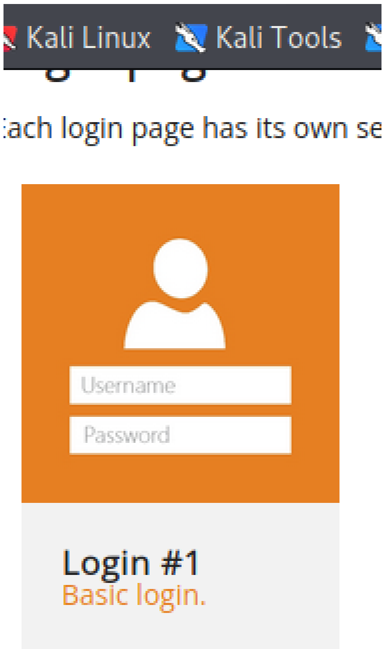
19. All we now need to do is click the setup/reset database button. This will just ensure that everything is going to work properly.



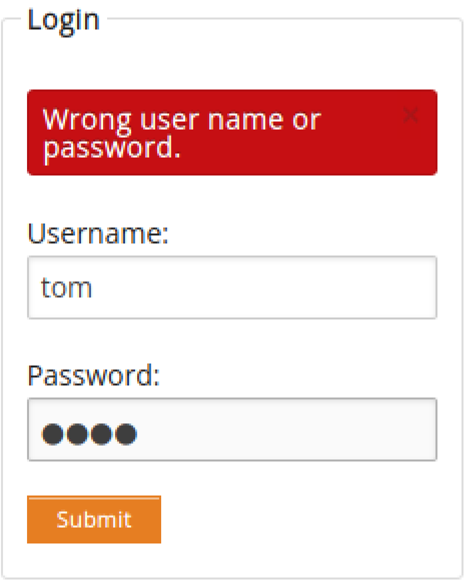
20. We can now go back to the bricks homepage and select the login pages. This is where we are going to be making all of our sql injection attacks.



21. We are going to do one attack. We are going to attack login#1, because these can take a while and login 1 gives a very basic understanding of a sql injection attack.



22. We are now at a login screen and can begin our attack. Our first step is going to guess the password so we can obtain an sql statement here. I guessed tom and root, and was given an error, but I was also given an SQL statement.



Login

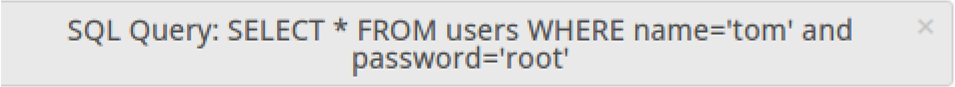
Wrong user name or password.

Username:

tom

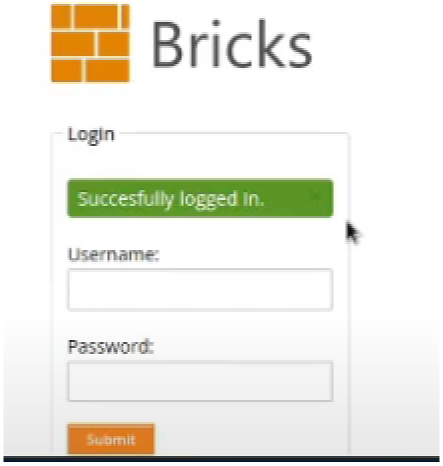
Password:

●●●●



SQL Query: SELECT * FROM users WHERE name='tom' and password='root'

23. n now begin our sql injection. An sql injection manipulates parts of databases to obtain information. Here we are given the statement SQL Query: * from users WHERE name =`tom` and password =`root`. This statement could be broken down very heavily, however all we really need to be concerned with is the last part. This database can be manipulated by adding an or statement onto the end of the query. If we say SQL Query: * from users WHERE name =`tom` and password =(` `) or 1=('1`) it technically wouldn't be wrong because a or statement only requires one part of the statement to be correct. We can also do this for the user name giving us this statement  WHERE name =(` `) or 1=('1`) and password =(` `) or 1=('1). We can then copy and paste the ends of this into the login page and gain access to the account. **Username =' or '1'='1 , password = ' or '1'='1**



24. As you can see by the above login picture our sql injection attack worked and we gained access to the loing account. This concludes my pen testing project since we were able to successfully create a sql injection attack.

Discussion:

- During this project a lot of things went well. I felt most of the project was just setup, but the one thing that I never had an issue with was the virtual box. This program is truly so easy to use, if I had any problems with it I could just google it and there were dozens for form pages.
- However one thing that didn't go well was the setting up of the database. Since my project needed me to set up a server that hosted a database it got a little complicated. Bricks is a great program that I enjoyed using, but they haven't updated their software since 2013, which made the installation process so much more difficult. I had to use an old php version that is compatible with bricks, Since bricks hasn't been updated in 8 years its php version was severely outdated.
- Although bricks gave me a headache I was able to find guides online that helped me set it up and change my php settings. This project was very difficult at times, but guides online really helped me out. Although there was never one clear guide, watching other peoples videos and piecing together my database as they did theirs helped a lot.
- I learned a lot of lessons, but I think the main lesson I learned was to always choose a program with up to date software, because old software makes everything a headache.