Lab 2: Building a Security Lab

QUICK REVIEW

When we talk about security penetration testing, the best and safest method is to practice within a virtual environment. The virtual environment can be created in virtual machines. Virtual machines are simulated machines running inside real machines. In the virtual world, the actual Operating System running on a computer is called "host" and every virtual machine that is run is called "guest." Virtual machines are safe because if a guest VM gets hacked, the host machine will remain safe.
Some of the virtualization systems are VMware Workstation, VMware Workstation Player, Oracle VirtualBox, etc. Even though you have your own choice to select any virtual machine for your lab, in this course, we will be using a VMware workstation Player. The main difference between these two (VMware Workstation and VMware Workstation Player) is that Player can only play the virtual machines while Workstation can both create and play the virtual machines.
You may choose to install Oracle VirtualBox or VMware Workstation Player for this class.
In this Lab, we will take a deeper look at the http requests and responses.

⚠ Important Notice:

Please carefully read the disclaimer declaration on the course webpage, before you start the lab practice, and make sure you fully understand all statements. The disclaimer is available on https://hogeschool.github.io/Software-Quality.

LAB PRACTICES

2.1. Installation of VirtualBox

VirtualBox is a cross-platform virtualization application. It can create and run a "guest" operating system (Virtual Machine) in a window of the host operating system such as Windows, Mac, Linux. We will use VirtualBox to install Kali Linux which comes with a set of security test tools that are useful for the labs.
To install VirtualBox, go to the download page available on https://www.virtualbox.org/wiki/Downloads.

- MacOS installation
  - Download the setup file
  - Run the installer by clicking on `VirtualBox.pkg` and follow the installation instructions
  - Click on the VirtualBox icon inside the application folder of your macOS
- Windows installation
  - Download the setup file
  - Run the installer and follow the installation instructions.

- Linux installation (Ubuntu)
  - To install VirtualBox, update first the list of available repositories. Run the commands below to install VirtualBox repository key.

```
wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- | sudo apt-key add -
wget -q https://www.virtualbox.org/download/oracle_vbox.asc -O- | sudo apt-key add -
```

  - Next run the commands below to add VirtualBox repository to your system.

```
sudo sh -c 'echo "deb http://download.virtualbox.org/virtualbox/debian $(lsb_release -sc)
contrib" >> /etc/apt/sources.list'
```

  - Run the install command.

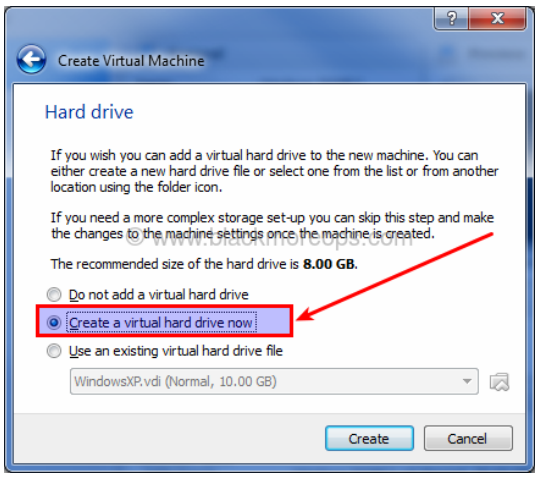
```
sudo apt-get update
sudo apt-get install virtualbox-6.0 //you can specify any available version here
```

2.2. Installation of Kali Linux

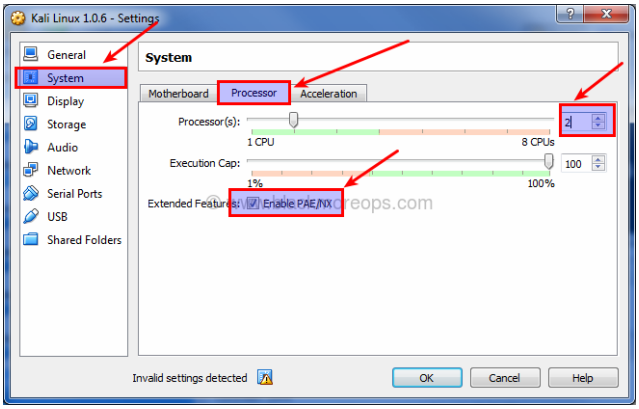
Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It includes some preinstalled tools like SQLMAP that is going to be used to detect and exploits SQL injection flaws.
To install Kali Linux, go to the download page, which is available on https://www.kali.org/downloads. Then download the ISO-file Kali Linux 32/64 Bit. To install it on your VM, follow the instructions below:

- Start the VirtualBox application on your machine
- Create a new Virtual Machine
- Create a new Virtual disk (VDI, dynamic allocation etc.)

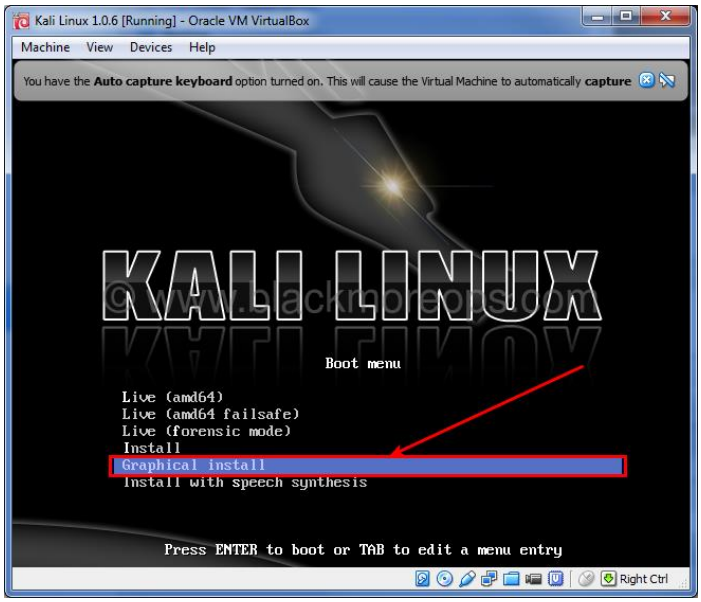
During the installation process, some setup settings are only accessible in expert mode.



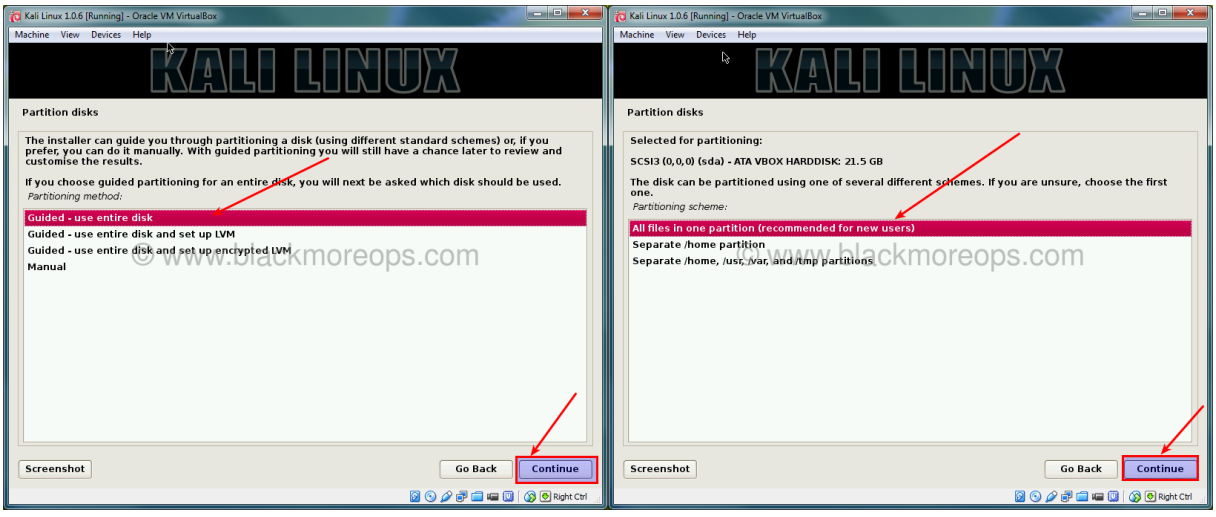
- Modifying some VirtualBox settings (It depends on the specification of your machine):
  - Allocate physical memory
  - Allocate video memory
  - Select OS Type
  - Select CPU acceleration and core numbers
  - etc.



- Loading Kali ISO by mounting the ISO-image to VirtualBox.
- Booting Kali ISO (initial info, location, time zone, etc.). You might see a different user interface for Kali Linux on your screen due to a newer version, but the installation steps remain the same.



- Partition your disk with Kali disk partitioning.



- Finalizing installation and running Kali on VirtualBox.
- Install VirtualBox Guest Additions packages.

2.3. DVWA (Damn Vulnerable Web Application)

Damn Vulnerable Web Application is a PHP/MYSQL web application that is vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

2.3.1. Perquisites of the installation

Note: If you have the full version of Kali Linux installed, then the required packages/tools are preinstalled. In case you have installed another version, you need to check which packages/tools are preinstalled.

- First you need to check the installation of PHP 7.3.x, MYSQL v15.x, Apache2, Git in the Terminal.

```
php --version  //version output 7.3.x
mysql –-version //version output 15.x
git –-version //version output 2.x
apache2 -version //version 2.x
```

- In case you are missing one of those packages/tools, then you need to install them using the `apt-get install` command. For example, if Git is missing:

```
sudo apt-get install git
```

2.3.2. Setup MYSQL server

Since the MYSQL server is empty, we need to create the database for the DWVA application, a user other that the root and its password. In addition, we need to give this user the permissions to create tables.

- To setup the password for the MYSQL server, you need to start the server

```
sudo service mysql restart
```

- Then change the password:

```
sudo mysqladmin -u root password "your password"
```

- After changing the password, you can connect to the MySQL server to create the database:

```
sudo mysql -u root -p
```

  - Type the MySQL root password you have created earlier, and then press Enter.

- To create a database, type the following command:

```
CREATE DATABASE dvwadb;
```

- To create a database user, type the following command. Replace "`dvwausr`" with the user you want to create, and replace "`your password`" with your actual password:

```
CREATE USER 'dvwausr'@'127.0.0.1' IDENTIFIED BY 'your password';
```

- Now you can grant permission to the user you have created:

```
GRANT ALL PRIVILEGES ON dvwadb.* TO 'dvwausr'@'localhost' IDENTIFIED BY 'your password';
```

- Once done, exit the application by typing the following commands:

```
\q
```

2.3.3. Download DVWA

We need to download the archive of DVWA from GitHub.

- Go to the apache2 folder:

```
cd /var/www/html/
```

- Clone DVWA from GitHub, type the following command:

```
sudo git clone https://github.com/ethicalhack3r/DVWA.git
```

2.3.4. Configure DVWA

Now we are ready to edit the source of PHP config files to make sure your web application connects to the database. You will use the text editor to edit the configuration file. The configuration file needs to be renamed, so that the application can use.

- To change the configuration file name, enter the following command:

```
sudo cp /var/www/html/DVWA/config/config.inc.php.dist /var/www/html/DVWA/config/config.inc
.php
```

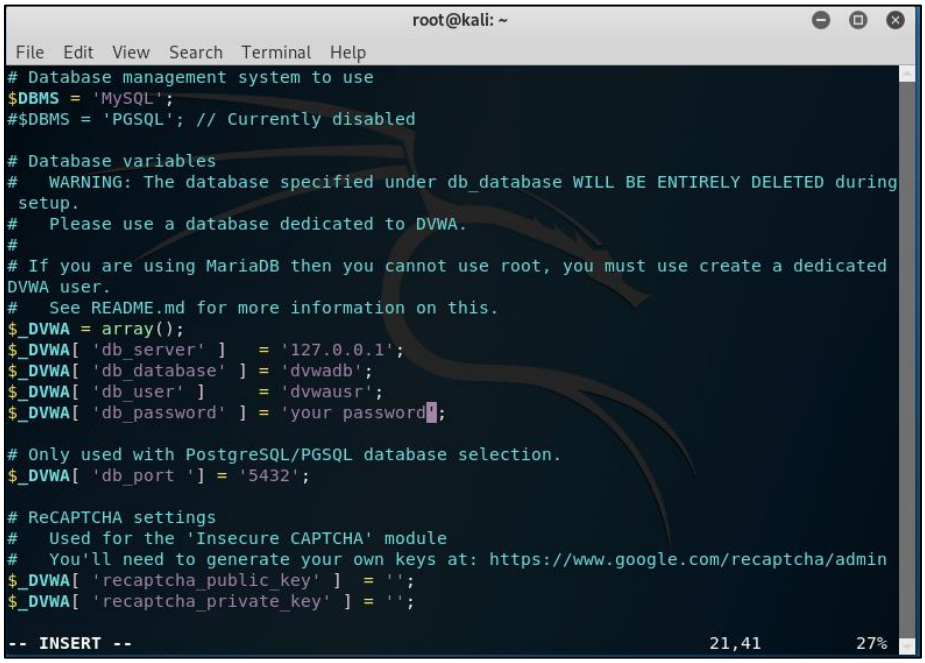
- After that the file can be edited with another command

```
sudo vim /var/www/html/DVWA/config/config.inc.php
```

- You need to change the database name, user, and password of the MySQL database. To do this the *VIM* file editor accepts keyboard shortcuts.
  - The arrow-button allows you to navigate through the file.
  - The button “x” removes a character in a string
  - The button “i” allows you to enter the writing mode
  - The button “Esc” exits you from the writing mode
  - The buttons combination “:q!” exits the file without any changes
  - The button combinations “:wq” exits the file after saving the changes

- Navigate to the string you need to change using the arrow-buttons. After reaching the string type the letter “x” to remove the strings letter by letter. Then type “i” to start editing. The start replacing the values one by one using the button combinations mentioned above.

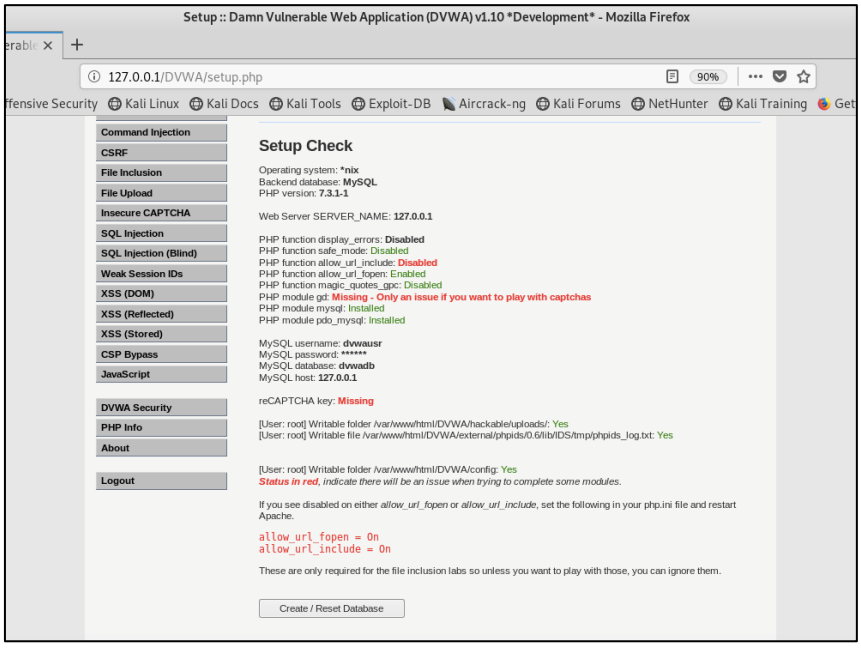
```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = ‘dvwadb’;
$_DVWA[ 'db_user' ]     = 'dvwausr';
$_DVWA[ 'db_password' ] = ‘your password’;
```



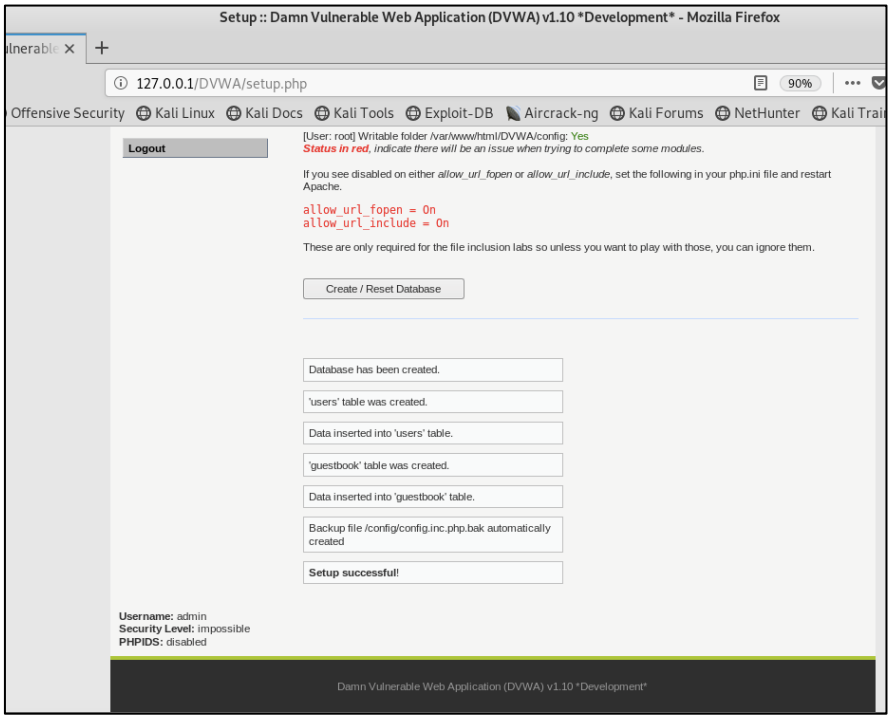
- Now you need to start or restart both servers the Apache2 (webserver) and the MYSQL(database) depending on the current status

```
sudo service mysql restart  //or stop and then start
sudo service apache2 restart //or stop and then start
```

- In the browser insert the following url: *http://127.0.0.1/DVWA/setup.php*



- Then click on the button “create/reset database” in the bottom of the page. After a successful installation you should see a message bellow the button indicating the changes.



- The final step is to go to the login page and enter the credentials to use the application. Enter the path to the login page in the browser *http://127.0.0.1/DVWA/login.php*, then login with the default username and password:

```
Username: admin
Password: password
```

Full description of DVWA is available on: https://github.com/ethicalhack3r/DVWA/blob/master/README.md