Concise Courses

"Learn How to Hack and Defend Your Website in Just 3 Hours"

Presented by

Alejandro Caceres
@DotSlashPunk
@HyperionGray

October 2, 2013

Lesson 0: Getting your hacking lab set up

Goal

Get all the necessary tools and test websites that we'll be using throughout the course. This lesson will go through the step by step process for installing these tools on a Debian-based Linux machine (preferably a virtual machine, but this is not required). This example will use Kali Linux, but should be general enough to work on any Debian-based Linux distribution.

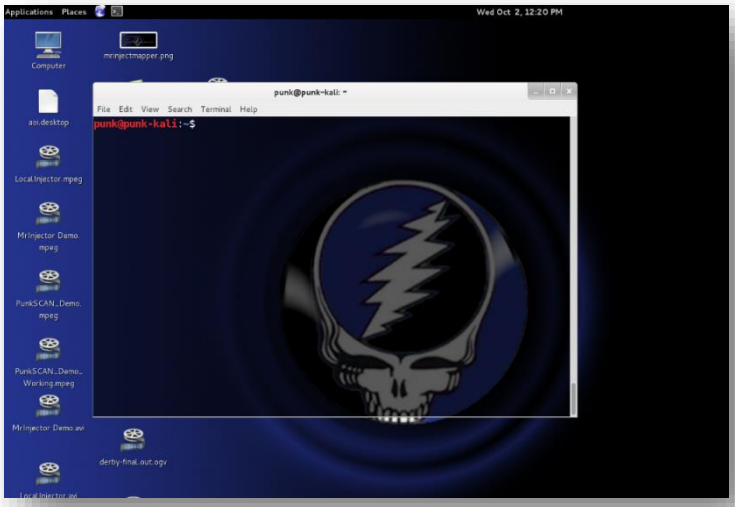
Don't worry if you don't fully understand these steps or the commands you will be using, we'll be talking more about the technologies we're using here during the course!

Prerequisites

- Upon registering for the course, you should have received instructions on installing a Debian-based Linux Virtual Machine. If any of you are having trouble with this, please email me at acaceres@hyperiongray.com
- Alternately, if you are already comfortable with Linux and have chosen to use an existing distribution of your choice, please feel free to do so. Just please make sure that you install the tools listed below for your own distro.

Steps

Step 1: Open up your Linux virtual machine and login, for this example I will be using Kali Linux, but these steps should be quite similar on any other Debian-based distribution. Open up the "terminal" application. This is typically found in the menu at the top under *application -> accessories -> terminal* or a similar path. Alternately, you can do a search for "terminal" in your Application Dashboard if you are using Ubuntu.

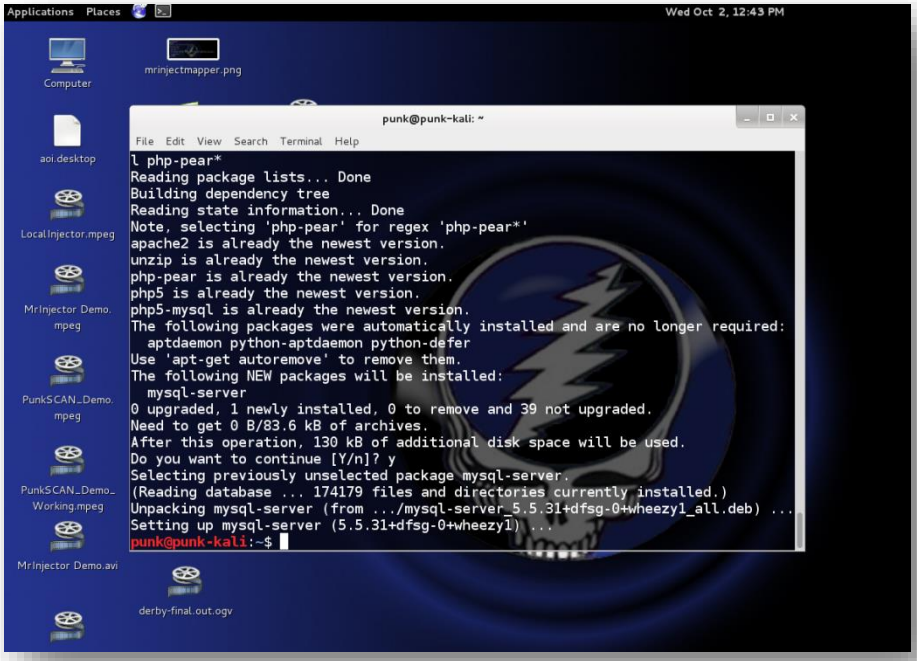


Additional Links:
https://help.ubuntu.com/community/UsingTheTerminal

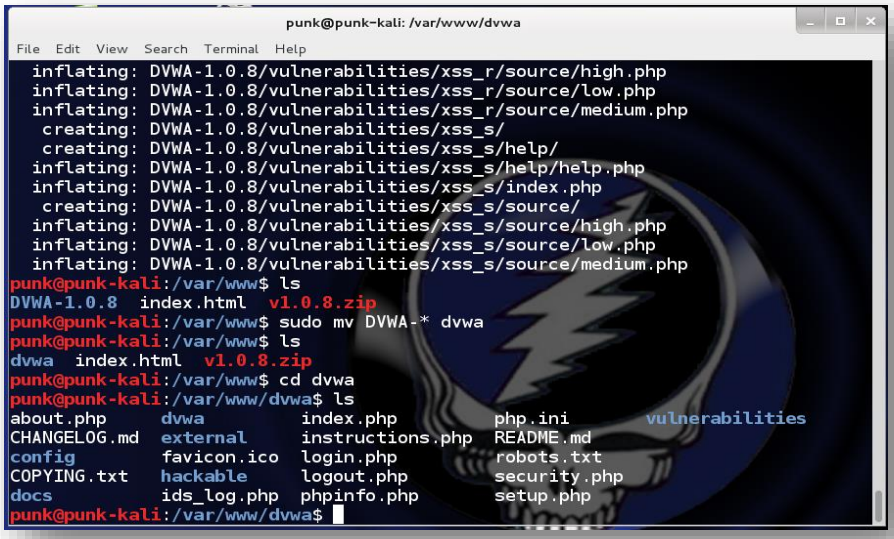
Step 2: Now we will need to install the dependencies. If you have your terminal open, simply copy and paste the following line into your terminal and press enter:

```
sudo apt-get install apache2 mysql-server php5 unzip php5-mysql php-pear*
```

You'll be prompted for your password, type in your user's password and press enter. You'll see the terminal doing a bunch of stuff and then it will prompt you for a MySQL password. It doesn't matter what password you use, but make sure you remember it! We will need it in the next steps. You should see no errors when doing this.



Step 3: In this step we will download and decompress the DVWA into our web server root (the folder that our web server is sharing with the world) and prepare to install it. Run the following



commands in the terminal to do this:

```
$ wget https://github.com/RandomStorm/DVWA/archive/v1.0.8.zip
$ sudo cp v1.0.8.zip /var/www/
$ cd /var/www
$ sudo unzip v1.0.8.zip
$ sudo mv DVWA-* dvwa
$ sudo chmod -R 777 dvwa
$ cd dvwa
```

Step 4: In this step we will configure the DVWA to work with your database. We're going to open the configuration file required in the DVWA and enter the MySQL root password that you set up in **Step 2**. This can be accomplished with the following:

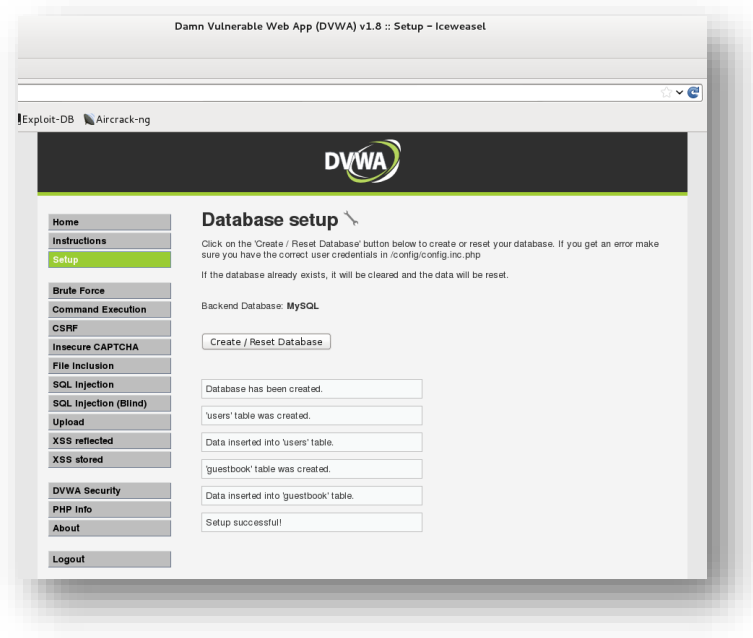
```
nano config/config.inc.php
```

This should open the file for editing with the 'nano' text editor

Go to line # 20 where it says `$_DVWA[ 'db_password' ] = 'p@ssw0rd';` and change `p@ssw0rd` to your password, being careful to not remove the semi-colon or single quotes.

To save and exit your work press <Ctrl + o> followed by <Enter> and then <Ctrl + x> to exit this config file.

Step 5: In this step we're going to make sure that our web server and database are started and we're going to finish setting up the DVWA. When you're back at your command prompt, start Apache with the following command:




```
sudo /etc/init.d/apache2 start
```

```
sudo /etc/init.d/mysql start
```

And we're done with the terminal! Now open up a web browser in your virtual machine. And point it to the following:

http://localhost/dvwa/setup.php

Then click on "Create/Reset Database."

Step 6: In this step we'll be downloading some additional tools that we'll be using in the course. First we will install SQLMap, then Burp Suite, then Nikto and finally DirBuster. We'll install all of them to the `/home/<user>` directory for easy access. Use the following command:

```
$ cd /home/<user>
```

Make sure to replace <user> here with your username.

Now type:

```
$ wget https://github.com/sqlmapproject/sqlmap/zipball/master
$ unzip master
$ mv sqlmapproject-* sqlmap
```

You now have SQLMap on your system! Next we're going to install Burp Suite:

```
$ wget http://portswigger.net/burp/burpsuite_free_v1.5.jar
$ java -jar burpsuite_free_v1.5.jar
```

You should see Burp Suite open up! Now we're going to install Nikto:

```
$ wget http://www.cirt.net/nikto/nikto-2.1.5.tar.gz

$ tar -xzvf nikto-2.1.5.tar.gz

$ mv nikto-2.1.5 nikto
```

Finally, we're going to install DirBuster:

```
$ wget -O dirbuster.zip
http://downloads.sourceforge.net/project/dirbuster/DirBuster%20%28jar%20%2B%20
lists%29/0.12/DirBuster-0.12.zip?r=&ts=1380737926&use_mirror=softlayer-dal

$ unzip dirbuster.zip

$ mv DirBuster-0.12/ dirbuster
```

Alternately, you can download all of these applications through your graphical front-end and a web browser (just Google them, they're easy to find) and use the decompression tools built-in to the GUI – but you should take the opportunity to get familiar with the Linux command line if you are not already!

If you choose to go this route, please make sure you know where these tools are installed on your system – you're going to need them!

So, after following all these steps, you now have the DVWA, SQLMap, Burp Suite, Nikto and DirBuster installed. And now we're ready for the fun stuff!