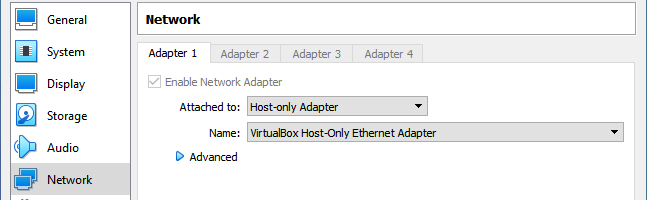
Lab - Brute forcing WordPress

**Overview**

Unlike hacks that focus on vulnerabilities in software, a Brute Force Attack aims to be the most straightforward kind of method to gain access to a site: it repeatedly tries usernames and passwords until it gets in. Often deemed ‘inelegant,’ they can be very successful when people use passwords like ‘123456’ and usernames like ‘admin.’

**Lab Requirements**

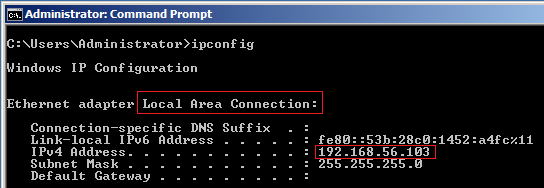
* One virtual install of Kali Linux
* One virtual install of Metasploitable3-win2k8 (password: **vagrant**)
* VirtualBox adapters should be set to Host-only adapter.



**Find your target’s IP address.**

Log on to your Win2k8 target machine as the user **vagrant**, using the password **vagrant**.

Once you have a desktop, open a command prompt, and at the prompt, type **ipconfig**. Next, find the IP address for the local area connection.

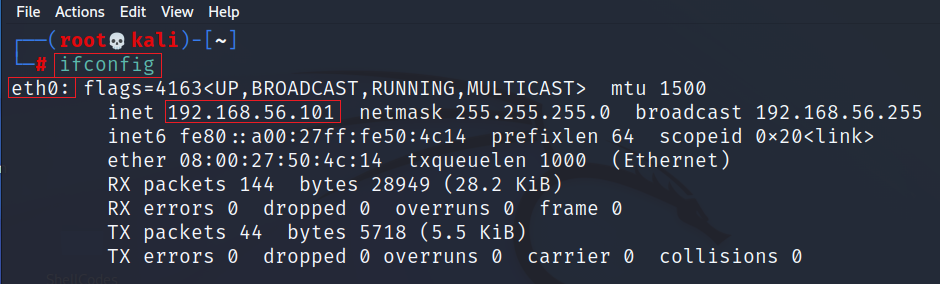
****

This is the IP address for my Metasploitable3 target. Yours may differ.

You’ll also need the IP address of your Kali machine. Open a new terminal on your Kali machine. At the prompt and type, **ifconfig**.

Press enter.

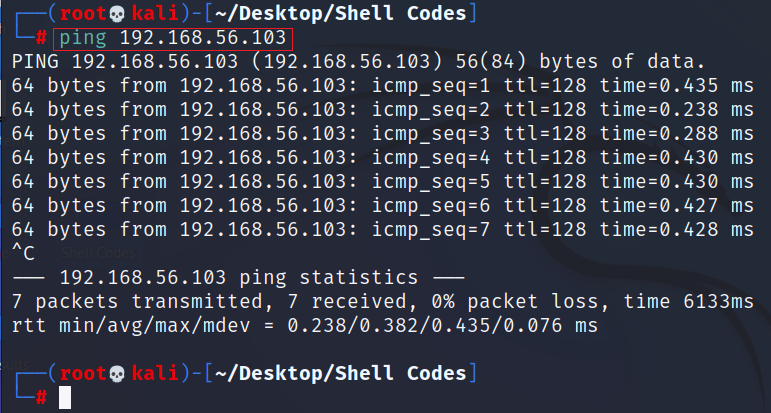
Find the IP address for your eth0 adapter.



This is the IP address for my Kali machine. Yours may differ.

**Check for Connectivity**

From your Kali desktop, open a new terminal. At the prompt type, ping <target IP address>.



You can stop the ping by pressing the Ctrl+C keys on your keyboard. If you do not have a positive response, set your VirtualBox adapters to Host-only adapters and try again.

**Begin the lab**

On your Kali desktop, right-click and create a new folder and name that new folder, ShellCodes.

**Using a Custom Wordlist**

We first need to create or find a custom wordlist. Some tools will crawl a website that can create a custom wordlist, such as [cewl](https://www.geeksforgeeks.org/cewl-tool-creating-custom-wordlists-tool-in-kali-linux/). We could also use one of the many word lists available in Kali or find a custom wordlist searching the Internet.

To see all the wordlists that come preinstalled with Kali, open a terminal, and use the **locate** command followed by the word wordlists.

Text

Description automatically generated

We can use the following usernames and passwords to create a customized wordlist for Metasploitable3.

testpassword

loginpassword

composer

vagrant

credential

hello

world

tryme

2123456789

987654321

qwerty

abcdefghijkl

abcd

hyperledger

network

toolsandhack

admin

sploit

user

manager

Highlight and copy the above wordlist. Then, on your Kali desktop, open your working folder. In the right windowpane, create a new document, and from the next context menu, select **Empty file**.

Graphical user interface, text, application

Description automatically generated

Give your wordlist a user-friendly name. For example, I called my wordlist metasploitable3.

Graphical user interface, text, application

Description automatically generated

Click the Create button.

Inside your working folder, find the empty file you just created. Open using mousepad. Copy and paste the Raw data that you copied for the GitHub site.

Graphical user interface, text

Description automatically generated

Close out the file. When prompted, click Save.

Graphical user interface, text, application

Description automatically generated

Close out your working folder.

Graphical user interface, application

Description automatically generated

Right-click on the new folder, and from the context menu, select Open Terminal Here.

Graphical user interface, application

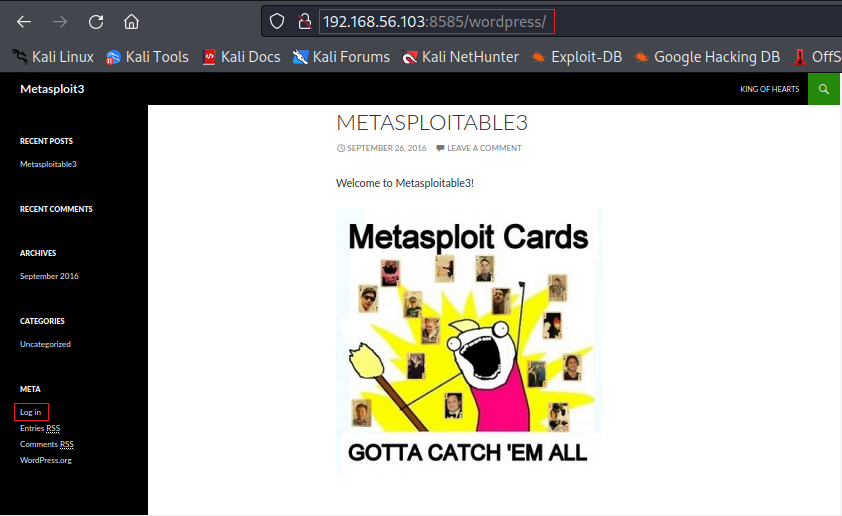
Description automatically generated

**Begin the lab!**

From your Kali machine, open a browser, and in the address bar, type the IP address of your target machine followed by the port number your Apache HTTPd service is running on (:8585) followed by /wordpress.

Example: **192.168.56.140:8585/wordpress**

This brings up the WordPress home page. Under Meta, you will find a link for the login page. The link to the login page will take you to /wordpress/wp-login.php.

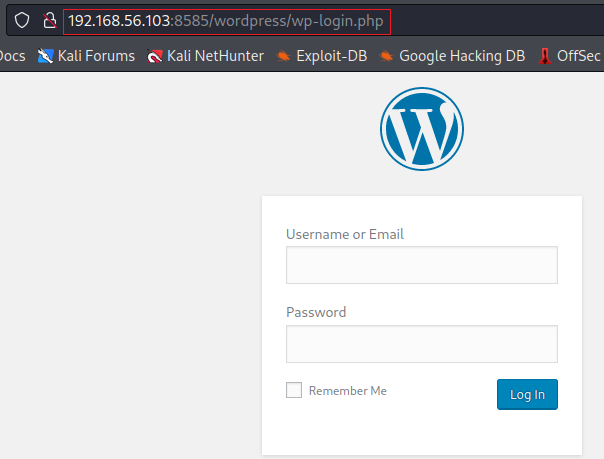


We have the username and password, but what if we didn’t? We could attempt to guess the username and password. We could try the default username and password for WordPress.

Chart

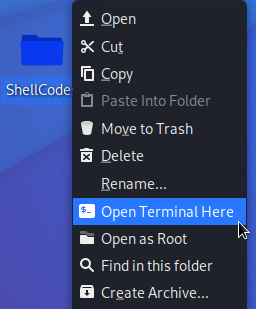
Description automatically generated with low confidence

When guessing and using the default username and password fail, we can try several methods to brute force the username and password using our custom word list.

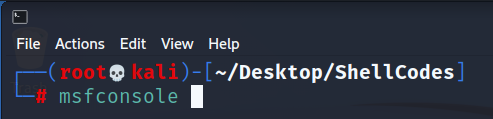


**Brute forcing WordPress using Nmap**

From your Kali desktop, right-click on your working folder, and from the context menu, select Open terminal here.



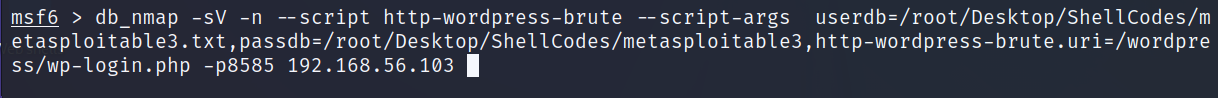
At the prompt, type **msfconsole**. Press enter.



At your Metasploit prompt, type or copy and paste the following Nmap command at the prompt.

db\_nmap -sV -n --script http-wordpress-brute --script-args userdb=/root/Desktop/ShellCodes/metasploitable3.txt,passdb=/root/Desktop/ShellCodes/metasploitable3.txt,http-wordpress-brute.uri=/wordpress/wp-login.php -p8585 192.168.56.140

This is my IP address for my target; your IP address will differ!



Press enter.

You receive the following error message.

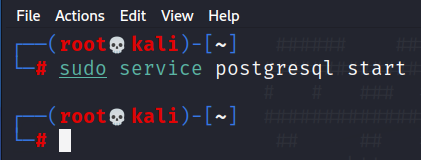
**Database not connected**

Metasploit uses PostgreSQL as its database, so it needs to be started.

Open a new terminal. At the prompt, type the following to start the PostgreSQL database.

**sudo service postgresql start**

Press enter.



With PostgreSQL up and running, we next need to create and initialize the msf database.

At the prompt, type the following to initialize the msf database.

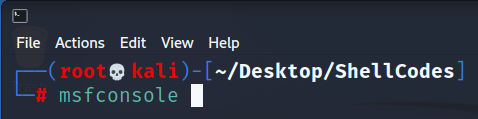
**sudo msfdb init**

****

Press enter.

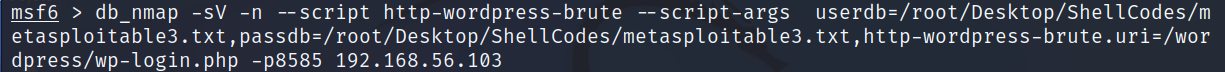
Close out the terminal. Close out your Metasploit terminal. Right-click on your working folder, and from the context menu, select Open a terminal here.

At the terminal prompt, type msfconsole.



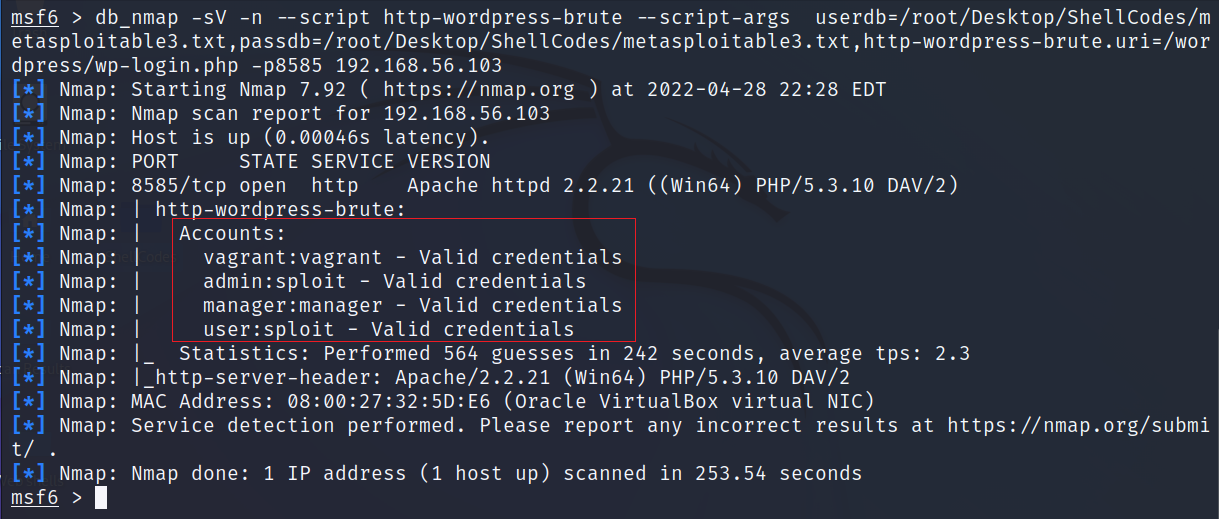
Press enter.

Use your up arrow to reload your last command at the Metasploit prompt.



Press enter.

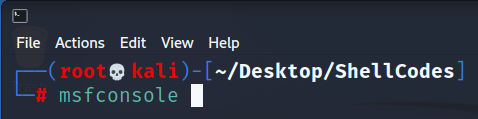
After a few minutes, the Nmap scan returns the following results finding four sets of credentials.



**Brute forcing WordPress using Metasploit**

Right-click on your working folder and select, Open Terminal from the context menu.

At the terminal prompt, type msfconsole.



Press enter.

Type in each of the following Metasploit commands one at a time, hitting enter between each command.

use auxiliary/scanner/http/wordpress\_xmlrpc\_login

set rhost 192.168.56.140

set rport 8585

set targeturi /wordpress

set user\_file /root/Desktop/ShellCodes/metasploitable3.txt

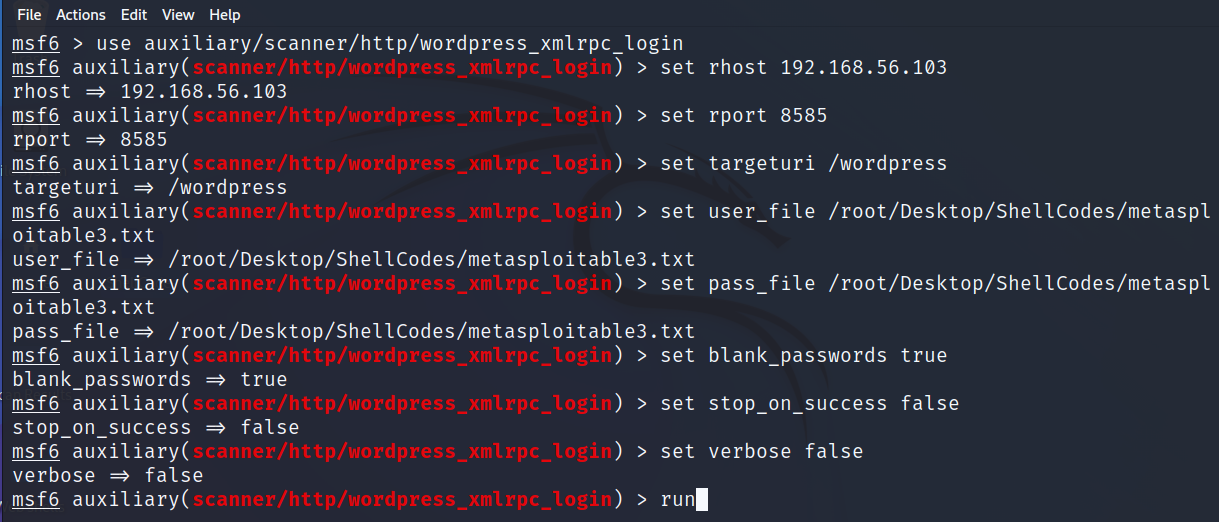
set pass\_file /root/Desktop/ShellCodes/metasploitable3.txt

set blank\_passwords true

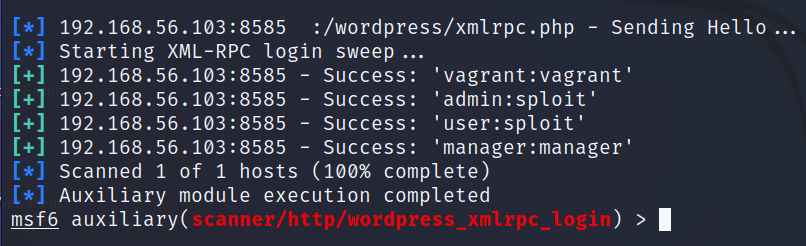
set stop\_on\_success false

set verbose false

run



After a short scan, Metasploit finds four sets of credentials.



**Brute forcing WordPress using Wpscan**

Right-click on your working folder and select, Open Terminal from the context menu.

At the prompt, type the following:

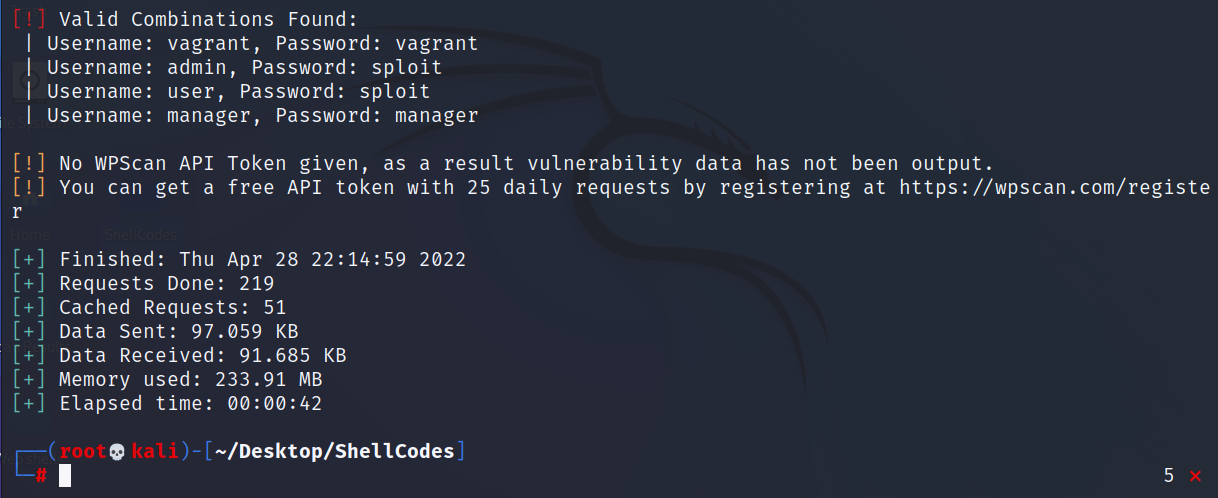
wpscan --url http://192.168.56.140:8585/wordpress/ --passwords /root/Desktop/ShellCodes/metasploitable3.txt

Press enter.

When wpscan starts for the first time, it will ask you if you want to update. I recommend allowing the update, but you will have to change your VirtualBox adapter for Kali to Nat network.

After the update, you’ll need to change it back to a Host-only adapter and restart the scan.

Wpscan found four sets of credentials.



Back at the WordPress login page, you can now login to WordPress using vagrant and vagrant.

Graphical user interface, application

Description automatically generated

You now have full administrative access to WordPress.

Graphical user interface, text, application

Description automatically generated

**Summary**

Having success at brute forcing our way into a web application such as WordPress is easy enough in a sterile lab environment, but roughly 50% of all exploits you will try will fail in the real world. Different versions of the operating system, different versioning of some needed files, patches, security updates, and many other issues make pentesting or hacking a website difficult. Therefore, you need to know more than just one method. You should always try the out-of-the-box default username and password for the application first.

There have many a few times when I surprised myself when the default username and password worked. If the application or the device comes out of the box with a default username and password, it can easily be found on the Internet using Shodan.

End of the lab!